

# ПРАВОВАЯ ИНФОРМАТИКА

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ

№ 3, 2026 г.

Выходит 4 раза в год

Зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций  
Свидетельство № 015372 от 01.11.1996 г.

Журнал входит в Перечень научных изданий ВАК,  
имеет рейтинг K1, по специальностям:

- 2.3.1. Системный анализ, управление и обработка информации  
(технические, физико-математические науки);  
5.1.2. Публично-правовые (государственно-правовые) науки  
(юридические науки).

## Главный редактор:

доктор юридических наук, профессор,  
кандидат технических наук

**Андрей Витальевич Морозов**

## Председатель редакционного совета:

доктор технических наук, профессор

**Михаил Юрьевич Сергин**

## Ответственный редактор,

### заместитель главного редактора:

кандидат юридических наук, учёный секретарь  
научно-технического совета

ФБУ НЦПИ при Минюсте России

**Мадина Олеговна Дубровина**

## Учредитель и издатель:

Федеральное бюджетное учреждение  
«Научный центр правовой информации  
при Министерстве юстиции  
Российской Федерации»

Адрес редакции:

125437, Москва, Михалковская ул., 65, корп.1

Телефон: +7 (495) 197-89-06 (доб. 248)

E-mail: it-pravo@scli.ru

Требования, предъявляемые к рукописям,  
размещены на сайте <http://uzulo.su/prav-inf>

Отпечатано в Отделении разработки информационного  
контента ФБУ НЦПИ при Минюсте России.

Печать цветная цифровая.

Подписано в печать 09.10.2026 г.

Общий тираж 100 экз. Цена свободная

# LEGAL INFORMATION

RESEARCH PEER-REVIEWED JOURNAL

2026, No.3

The journal is published quarterly.

Registered by the Federal Service for Supervision  
in the Sphere of Telecom, Information Technologies  
and Mass Communications  
Registration Certificate No. 015372 of the 1<sup>st</sup> of November 1996.

The journal is included in the list of scientific publications  
of the Higher Attestation Commission by specialty:

- 2.3.1. System analysis, management and processing Information  
(technical, physical and mathematical);  
5.1.2. Public-law (state-law) Science (Legal).

## Editor-in-Chief:

Dr.Sc. (Law), Professor,  
Ph.D. (Technology)

**Andrei Morozov**

## Chair of the Editorial Council:

Dr.Sc. (Technology), Professor

**Mikhail Sergin**

## Managing Editor, Deputy Editor-in-Chief:

Ph.D. (Law), Scholarly Secretary of the Research  
and Technology Board of the Scientific Centre  
for Legal Information (SCLI) under  
the Ministry of Justice of the Russian Federation

**Madina Dubrovina**

## Founder and publisher:

Federal State-Funded Institution  
“Scientific Centre for Legal Information  
under the Ministry of Justice of the  
Russian Federation” (SCLI)

Postal address:

Mikhalkovskaya str., bld. 65/1, 125 438, Moscow, Russia

Telephone: +7 (495) 197-89-06 (ext. 248)

E-mail: it-pravo@scli.ru

Guidelines for preparing manuscripts for publication can  
be found on the website <http://uzulo.su/prav-inf>

Printed by the Department of Information  
Content Development of the SCLI.

Printed in digital colour. Approved for print  
on the 9<sup>th</sup> of October, 2026.

Number of items printed: 100. Free price

## РЕДАКЦИОННЫЙ СОВЕТ

СЕРГИН Михаил Юрьевич  
БАТУРИН Юрий Михайлович  
БАБУРИН Сергей Николаевич  
ЕМЕЛИН Николай Михайлович  
ЗАПОЛЬСКИЙ Сергей Васильевич  
ИСАКОВ Владимир Борисович  
ТЮТЮННИК Вячеслав Михайлович  
УВАЙСОВ Сайгид Увайсович

председатель редакционного совета, доктор технических наук, профессор, г. Москва  
доктор юридических наук, член-корреспондент РАН, Герой России, г. Москва  
доктор юридических наук, профессор, г. Москва  
доктор технических наук, профессор, г. Москва  
доктор юридических наук, профессор, г. Москва  
доктор юридических наук, профессор, г. Москва  
доктор технических наук, профессор, г. Москва  
доктор технических наук, профессор, г. Москва

### Иностранные члены

КРУГЛИКОВ Сергей Владимирович  
ШАРШУН Виктор Александрович

доктор военных наук, кандидат технических наук, доцент, г. Минск, Республика Белоруссия  
кандидат юридических наук, доцент, г. Минск, Республика Белоруссия

## РЕДАКЦИОННАЯ КОЛЛЕГИЯ

### Технические науки

АЛЕКСЕЕВ Владимир Витальевич  
БУРЫЙ Алексей Сергеевич  
СКИБА Владимир Юрьевич  
СУХОВ Андрей Владимирович

доктор технических наук, профессор, г. Тамбов  
доктор технических наук, г. Москва  
доктор технических наук, профессор, г. Москва, пгт. Сириус  
доктор технических наук, профессор, г. Москва

### Юридические науки

ЗАХАРЦЕВ Сергей Иванович  
КАБАНОВ Павел Александрович  
КАРЦХИЯ Алесандр Амиранович  
ПОЛЯКОВА Татьяна Анатольевна  
АТАГИМОВА Эльмира Исамудиновна

доктор юридических наук, профессор, г. Москва  
доктор юридических наук, профессор, г. Казань  
доктор юридических наук, доцент, г. Москва  
доктор юридических наук, профессор, г. Москва  
кандидат юридических наук, доцент, г. Москва

---

## EDITORIAL COUNCIL

Mikhail SERGIN  
Iurii BATURIN  
  
Sergei BABURIN  
Nikolai EMELIN  
Sergei ZAPOL'SKII  
Vladimir ISAKOV  
Viacheslav TIUTIUNNIK  
Saigid UVAISOV

Chair of the Editorial Council, Dr.Sc. (Technology), Professor, Moscow  
Dr.Sc. (Law), Corresponding Member of the Russian Academy of Sciences,  
Hero of the Russian Federation, Moscow  
Dr.Sc. (Law), Professor, Moscow  
Dr.Sc. (Technology), Professor, Moscow  
Dr.Sc. (Law), Professor, Moscow  
Dr.Sc. (Law), Professor, Moscow  
Dr.Sc. (Technology), Professor, Tambov  
Dr.Sc. (Technology), Professor, Moscow

### Foreign members

Sergei KRUGLIKOV  
Viktor SHARSHUN

Dr.Sc. (Military), Ph.D. (Technology), Associate Professor, Minsk, Belarus  
Ph.D. (Technology), Associate Professor, Minsk, Belarus

## EDITORIAL BOARD

### Technology

Vladimir ALEKSEEV  
Alekssei BURYI  
Vladimir SKIBA  
Andrey SUKHOV

Dr.Sc. (Technology), Professor, Tambov  
Dr.Sc. (Technology), Professor, Moscow  
Dr.Sc. (Technology), Professor, Moscow  
Dr.Sc. (Technology), Professor, Moscow

### Law

Sergey ZAKHARTSEV  
Pavel KABANOV  
Aleksandr Kartschiya  
Tat'iana POLIAKOVA  
El'mira ATAGIMOVA

Dr.Sc. (Law), Professor, Moscow  
Dr.Sc. (Law), Professor, Kazan  
Dr.Sc. (Law), Professor, Moscow  
Dr.Sc. (Law), Professor, Moscow  
Ph.D. (Law), Associate Professor, Moscow

# СОДЕРЖАНИЕ

## Системный анализ, управление, искусственный интеллект и защита информации

|                                                                                                                                                                                       |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛИЗИРОВАННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ<br><i>Максимова Е.А.</i> .....                 | 7   |
| МЕТОДИКА ОЦЕНКИ КВАНТОВОЙ УСТОЙЧИВОСТИ БЛОКЧЕЙН-ПЛАТФОРМ НА ОСНОВЕ СЕТЕЙ ПЕТРИ<br><i>Ларина М.В., Скиба В.Ю.</i> .....                                                                | 17  |
| МЕТОД ИНТЕРПРЕТАЦИОННОГО ДИАГНОСТИРОВАНИЯ СОСТОЯНИЯ ЭЛЕМЕНТОВ БЛОКЧЕЙН-СИСТЕМ ПО РЕШЕНИЮ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ<br><i>Лисов Д.Н., Гнидко К.О.</i> .....                           | 29  |
| РАЗВИТИЕ ОТЕЧЕСТВЕННЫХ СИСТЕМ ИНФОРМАЦИОННО-ТЕЛЕМЕТРИЧЕСКОГО ОБЕСПЕЧЕНИЯ ОТРАБОТКИ СРЕДСТВ ВЫВЕДЕНИЯ В КОНТЕКСТЕ СЛОЖИВШИХСЯ ПРОИЗВОДСТВЕННЫХ ОТНОШЕНИЙ<br><i>Воронцов В.Л.</i> ..... | 41  |
| БАЗА ЗНАНИЙ В СИСТЕМЕ РАССЛЕДОВАНИЯ АВАРИЙ И ИНЦИДЕНТОВ НА ПРОИЗВОДСТВЕННЫХ ОБЪЕКТАХ<br><i>Маркарян А.О., Поляховская О.А., Якубовская Ю.А.</i> ...                                   | 51  |
| ПОДХОД К РЕАЛИЗАЦИИ БЕЗОПАСНОГО УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ ИНФРАСТРУКТУР<br><i>Морозов Ф.А.</i> .....                                                 | 60  |
| АНАЛИЗ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ МОНИТОРИНГА ОБСТАНОВКИ И ПРОГРАММНЫХ КОМПЛЕКСОВ МОДЕЛИРОВАНИЯ ПОСЛЕДСТВИЙ ЧС<br><i>Мураев Н.П., Карапузиков А.А.</i> .....                  | 70  |
| МЕТОДИКА ОПТИМИЗАЦИИ СЛОЖНОЙ ЧЕЛОВЕКО-МАШИННОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С УЧЁТОМ УГЛЕРОДНОЙ ИНТЕНСИВНОСТИ<br><i>Исаев Н.А.</i> .....  | 79  |
| ИНТЕРПРЕТАЦИОННАЯ МОДЕЛЬ НАБЛЮДЕНИЯ И ДИАГНОСТИРОВАНИЯ СОСТОЯНИЯ ЭЛЕМЕНТОВ БЛОКЧЕЙН-СИСТЕМ ПО РЕШЕНИЯМ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ<br><i>Лисов Д.Н.</i> .....                          | 88  |
| <b>Государственно-правовые науки</b>                                                                                                                                                  |     |
| К ЮБИЛЕЮ СОЗДАТЕЛЯ СВОДА ЗАКОНОВ СССР ТЕРЕБИЛОВА ВЛАДИМИРА ИВАНОВИЧА<br><i>Морозов А.В.</i> .....                                                                                     | 100 |
| СИСТЕМА ФИНАНСОВЫХ ОБЯЗАТЕЛЬСТВ КАК АЛГОРИТМ РАЗВИТИЯ ФИНАНСОВО-ПРАВОВЫХ ИНСТИТУТОВ<br><i>Васянина Е.Л.</i> .....                                                                     | 104 |

|                                                                                                                                                                                |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| О ПРАВОВЫХ ОСНОВАХ ДЕЯТЕЛЬНОСТИ АФФИЛИРОВАННЫХ АКЦИОНЕРНЫХ ОБЩЕСТВ В СОСТАВЕ ГОСУДАРСТВЕННЫХ КОРПОРАЦИЙ И КОМПАНИЙ<br><i>Запольский С.В.</i> .....                             | 112 |
| КИБЕРНЕТИЧЕСКИЙ ПОДХОД К ПОНИМАНИЮ ГОСУДАРСТВА (СПЕЦИАЛЬНАЯ ТЕОРИЯ СИНЕРГЕТИКИ)<br><i>Зырянов А.В.</i> .....                                                                   | 120 |
| АДМИНИСТРАТИВНО-ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ПРАВ ГРАЖДАН В ФИСКАЛЬНЫХ ПРАВООТНОШЕНИЯХ<br><i>Кобзарь-Фролова М.Н.</i> .....                                                       | 131 |
| ОБ ИНФОРМАЦИОННО-ПРАВОВОЙ ПРИРОДЕ ФИНАНСОВОГО КОНТРОЛЯ<br><i>Глазунова И.В., Запольский С.В.</i> .....                                                                         | 140 |
| СОСТОЯНИЕ ЗАКОННОСТИ В СФЕРЕ БЕЗОПАСНОСТИ ДЕТЕЙ И РОЛЬ ПРОКУРАТУРЫ В ЕГО ОБЕСПЕЧЕНИИ<br><i>Ережипалиев Д.И.</i> .....                                                          | 149 |
| ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ И РАЗВИТИЯ ТАКТИКИ НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ ПРОКУРАТУРЫ<br><i>Махьянова Р.М.</i> .....                                                                    | 157 |
| «ТЕХНОЛОГИИ ЗДРАВООХРАНЕНИЯ», «ТЕХНОЛОГИИ СБЕРЕЖЕНИЯ ЗДОРОВЬЯ», «МЕДИЦИНСКИЕ ТЕХНОЛОГИИ»: СООТНОШЕНИЕ ДЕФИНИЦИЙ В КОНТУРЕ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ<br><i>Рыбакова О.С.</i> ..... | 167 |
| ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПРОКУРОРСКОГО НАДЗОРА ЗА ИСПОЛНЕНИЕМ ЗАКОНОВ В СФЕРЕ ПРОФИЛАКТИКИ ДЕВИАНТНОГО ПОВЕДЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ<br><i>Рябокоть В.П.</i> .....               | 177 |
| ПРАВОВЫЕ ПРОБЛЕМЫ ИДЕНТИФИКАЦИИ ДЕСТРУКТИВНОЙ ИНФОРМАЦИИ В СЕТИ «ИНТЕРНЕТ»<br><i>Чудесенко А.В.</i> .....                                                                      | 185 |
| <b>Регуляторная информатика</b>                                                                                                                                                |     |
| ЦИФРОВЫЕ ЛОГИСТИЧЕСКИЕ ПЛАТФОРМЫ И АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ<br><i>Сморчкова Л.Н.</i> .....                                                                       | 192 |
| ЦИФРОВЫЕ ФИНАНСОВЫЕ АКТИВЫ: РЕГУЛИРОВАНИЕ УЗЛОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ<br><i>Метельков А.Н.</i> .....                                                                          | 199 |
| ОБОСНОВАННОСТЬ ЭКСПЕРТНОЙ ОЦЕНКИ ПРОГРАММ И МЕТОДИК ИСПЫТАНИЙ<br><i>Шелестович О.А., Свистунов А.В.</i> .....                                                                  | 208 |
| ЦИФРОВОЙ АВАТАР ПРЕПОДАВАТЕЛЯ КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ<br><i>Зуева А.С.</i> .....                                                                                    | 219 |

|                                                                                                                                                                                                     |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <b>НЕКОММЕРЧЕСКИЕ ОРГАНИЗАЦИИ В ЦИФРОВОЙ<br/>МОДЕЛИ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ<br/>И ИСПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ</b><br><i>Дубровина М.О.</i> .....                                                          | 228 |
| <b>ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ<br/>ПРОГРАММ ФИЗИЧЕСКОЙ ПОДГОТОВКИ КУРСАНТОВ<br/>ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МЧС РОССИИ</b><br><i>Кокшаров Е.В., Гареев Д.Р.</i> .....                        | 240 |
| <b>НОРМАТИВНО-ОРИЕНТИРОВАННЫЙ МЕТОД<br/>ОБОСНОВАНИЯ РЕШЕНИЙ ОБ АВТОМАТИЗАЦИИ<br/>ПРОЦЕССОВ ДЕЯТЕЛЬНОСТИ</b><br><i>Свистунов А.В.</i> .....                                                          | 248 |
| <b>ПРИНЦИП ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В СФЕРЕ<br/>ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:<br/>ТЕОРЕТИКО-ПРАВОВЫЕ АСПЕКТЫ</b><br><i>Дубень А.К.</i> .....                                             | 262 |
| <b>ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ<br/>ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br/>ПРИ ВЗАИМОДЕЙСТВИИ ГОСУДАРСТВЕННЫХ<br/>ИНФОРМАЦИОННЫХ СИСТЕМ И КРЕДИТНЫХ<br/>ОРГАНИЗАЦИЙ</b><br><i>Иванов Н.Ю.</i> ..... | 268 |
| <b>СТАНОВЛЕНИЕ И РАЗВИТИЕ ЦИФРОВОГО<br/>ПРОСТРАНСТВА КАК ОБЪЕКТА ПРАВОВОГО<br/>РЕГУЛИРОВАНИЯ</b><br><i>Маскайкина Е.А.</i> .....                                                                    | 277 |
| <b>ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ<br/>КАК ОПОРНАЯ ИНФРАСТРУКТУРА НАЦИОНАЛЬНОЙ<br/>ПЛАТЁЖНОЙ СИСТЕМЫ: ПРАВОВОЙ РЕЖИМ<br/>НЕДОСТУПНОСТИ</b><br><i>Лобанов Н.А.</i> .....                      | 285 |
| <b>ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА<br/>В ОБЕСПЕЧЕНИИ ПОЖАРНОЙ БЕЗОПАСНОСТИ</b><br><i>Попова С.В.</i> .....                                                                                     | 295 |
| <b>ПРАВОВЫЕ МЕХАНИЗМЫ СНИЖЕНИЯ<br/>РИСКОВ НЕКАЧЕСТВЕННОЙ ИНФОРМАЦИИ В<br/>ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ</b><br><i>Олифиренко А.А.</i> .....                                               | 302 |
| <b>ИНТЕЛЛЕКТУАЛЬНЫЙ ПОМОЩНИК ДЛЯ ОБУЧЕНИЯ<br/>НАСЕЛЕНИЯ АЛГОРИТМАМ ОКАЗАНИЯ ПЕРВОЙ<br/>ПОМОЩИ</b><br><i>Васильев Р.В.</i> .....                                                                     | 312 |
| <b>ЦИФРОВИЗАЦИЯ ПРОЦЕССОВ НАУЧНОЙ КАРЬЕРЫ:<br/>ТРАНСФОРМАЦИЯ РОЛИ УНИВЕРСИТЕТОВ<br/>В СТРАНАХ ШОС</b><br><i>Башмакова В.И.</i> .....                                                                | 320 |

# CONTENTS

## System analysis, management, artificial intelligence, and information protection

### AN INFORMATION SECURITY ADVERSARY MODEL FOR INTELLIGENT CYBER-PHYSICAL SYSTEMS IN CRITICAL INFORMATION INFRASTRUCTURE

*Maksimova E.A.* ..... 7

### METHODOLOGY FOR ASSESSING THE QUANTUM RESILIENCE OF BLOCKCHAIN PLATFORMS BASED ON PETRI NETS

*Larina M.V., Skiba V.Yu.* ..... 17

### A METHOD FOR INTERPRETATIVE DIAGNOSIS OF THE STATE OF BLOCKCHAIN SYSTEM COMPONENTS USING MACHINE LEARNING MODEL SOLUTIONS

*Lisov D.N., Gnidko K.O.* ..... 29

### DEVELOPMENT OF DOMESTIC INFORMATION AND TELEMETRY SUPPORT SYSTEMS FOR LAUNCH VEHICLE IN THE CONTEXT OF THE EXISTING PRODUCTION RELATIONS

*Vorontsov V.L.* ..... 41

### KNOWLEDGE BASE IN THE SYSTEM OF INVESTIGATING ACCIDENTS AND INCIDENTS AT INDUSTRIAL FACILITIES

*Markarian A.O., Polyakhovskaya O.A., Yakubovskaya Yu.A.* . 51

### A SECURE REMOTE ADMINISTRATION APPROACH FOR DISTRIBUTED COMPUTING INFRASTRUCTURES

*Morozov F.A.* ..... 60

### ANALYSIS OF INFORMATION AND ANALYTICAL SYSTEMS FOR MONITORING THE SITUATION AND SOFTWARE COMPLEXES FOR MODELING THE CONSEQUENCES OF EMERGENCIES

*Muraev N.P., Karapuzikov A.A.* ..... 70

### A METHODOLOGY FOR OPTIMIZING A COMPLEX HUMAN-MACHINE DECISION SUPPORT SYSTEM IN INFORMATION SECURITY CONSIDERING CARBON INTENSITY

*Isaev N.A.* ..... 79

### AN INTERPRETATIVE MODEL FOR MONITORING AND DIAGNOSING THE STATUS OF BLOCKCHAIN SYSTEM COMPONENTS USING MACHINE LEARNING MODELS

*Lisov D.N.* ..... 88

## Constitutional law

### TO THE ANNIVERSARY OF THE CREATOR OF THE CODE OF LAWS OF THE USSR, VLADIMIR IVANOVICH TEREBILOV

*Morozov A.V.* ..... 100

### THE SYSTEM OF FINANCIAL OBLIGATIONS AS AN ALGORITHM FOR THE DEVELOPMENT OF FINANCIAL AND LEGAL INSTITUTIONS

*Vasyanina E.L.* ..... 104

### ON THE LEGAL BASIS FOR THE ACTIVITIES OF AFFILIATED JOINT-STOCK COMPANIES AS PART OF STATE CORPORATIONS AND COMPANIES

*Zapolsky S.V.* ..... 112

### CYBERNETIC APPROACH TO UNDERSTANDING THE STATE (SPECIAL THEORY OF SYNERGETICS)

*Zyryanov A.V.* ..... 120

### ADMINISTRATIVE AND LEGAL MECHANISMS FOR PROTECTING THE RIGHTS OF CITIZENS IN FISCAL LEGAL RELATIONS

*Kobzar-Frolova M.N.* ..... 131

### ON THE INFORMATIONAL AND LEGAL NATURE OF FINANCIAL CONTROL

*Glazunova I.V., Zapolsky S.V.* ..... 140

### THE STATE OF LEGALITY IN THE SPHERE OF CHILD SAFETY AND THE ROLE OF THE PROSECUTOR'S OFFICE IN ITS ENSURING

*Erezhipaliev D.I.* ..... 149

### PROBLEMS OF USING AND DEVELOPING SUPERVISORY TACTICS IN THE PROSECUTOR'S OFFICE

*Makh'ianova R.M.* ..... 157

### "HEALTH TECHNOLOGIES", "HEALTHCARE TECHNOLOGIES", "MEDICAL TECHNOLOGIES": THE RELATIONSHIP OF DEFINITIONS IN THE CONTOUR OF LEGAL REGULATION

*Rybakova O.S.* ..... 167

### FEATURES OF ORGANIZING PROSECUTORIAL SUPERVISION OVER THE IMPLEMENTATION OF LAWS IN THE FIELD OF PREVENTING DEVIANT BEHAVIOR AMONG MINORS

*Ryabokon V.P.* ..... 177

### LEGAL PROBLEMS OF IDENTIFYING DESTRUCTIVE INFORMATION ON THE INTERNET

*Chudesenko A.V.* ..... 185

## Regulatory informatics

### DIGITAL LOGISTICS PLATFORMS AND ADMINISTRATIVE AND LEGAL REGULATION

*Smorchkova L.N.* ..... 192

### DIGITAL FINANCIAL ASSETS: REGULATION OF INFORMATION SYSTEM NODES

*Metel'kov A.N.* ..... 199

### VALIDITY OF EXPERT ASSESSMENT OF TEST PROGRAMS AND PROCEDURES

*Shelestovich O.A., Svistunov A.V.* ..... 208

### DIGITAL AVATAR OF A TEACHER AS AN OBJECT OF LEGAL REGULATION

*Zueva A.S.* ..... 219

### NON-PROFIT ORGANIZATIONS WITHIN A DIGITAL MODEL FOR COMPLIANCE WITH REQUIREMENTS AND THE PERFORMANCE OF OBLIGATIONS

*Dubrovina M.O.* ..... 228

### INFORMATION AND LEGAL SUPPORT FOR PHYSICAL TRAINING PROGRAMS FOR CADETS IN EDUCATIONAL ORGANIZATIONS OF THE EMERCOM OF RUSSIA

*Koksharov E.V., Gareev D.R.* ..... 240

|                                                                                                                                                                                         |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <b>A NORMATIVELY ORIENTED METHOD<br/>FOR SUBSTANTIATING DECISIONS<br/>ON THE AUTOMATION OF ACTIVITY PROCESSES</b><br><i>Svistunov A.V.</i> .....                                        | 248 |
| <b>THE PRINCIPLE OF INFORMATION RELIABILITY<br/>IN THE FIELD OF INFORMATION SECURITY:<br/>THEORETICAL AND LEGAL ASPECTS</b><br><i>Duben A.K.</i> .....                                  | 262 |
| <b>ORGANIZATIONAL AND LEGAL SUPPORT<br/>FOR INFORMATION SECURITY IN THE INTERACTION<br/>BETWEEN STATE INFORMATION SYSTEMS<br/>AND CREDIT ORGANIZATIONS</b><br><i>Ivanov N.Yu.</i> ..... | 268 |
| <b>FORMATION AND DEVELOPMENT OF DIGITAL SPACE<br/>AS AN OBJECT OF LEGAL REGULATION</b><br><i>Maskaikina E.A.</i> .....                                                                  | 277 |
| <b>STATE INFORMATION SYSTEMS AS THE SUPPORTING<br/>INFRASTRUCTURE OF THE NATIONAL PAYMENT SYSTEM:<br/>THE LEGAL REGIME OF UNAVAILABILITY</b><br><i>Lobanov N.A.</i> .....               | 285 |
| <b>THE USE OF ARTIFICIAL INTELLIGENCE IN ENSURING<br/>FIRE SAFETY</b><br><i>Popova S.V.</i> .....                                                                                       | 295 |
| <b>LEGAL MECHANISMS FOR REDUCING RISKS<br/>OF LOW-QUALITY INFORMATION IN GOVERNMENT<br/>INFORMATION SYSTEMS</b><br><i>Olifrenko A.A.</i> .....                                          | 302 |
| <b>INTELLIGENT ASSISTANT FOR TEACHING THE GENERAL<br/>PUBLIC FIRST-AID PROCEDURES</b><br><i>Vasilyev R.V.</i> .....                                                                     | 312 |
| <b>DIGITALIZATION OF ACADEMIC CAREER PROCESSES:<br/>TRANSFORMING THE ROLE OF UNIVERSITIES<br/>IN THE SCO COUNTRIES</b><br><i>Bashmakova V.I.</i> .....                                  | 320 |



# МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛИЗИРОВАННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Максимова Е.А.<sup>1</sup>

**Ключевые слова:** искусственный интеллект, деструктивные воздействия, функциональный агент, инфраструктурный деструктивизм, каскадные последствия, автономность, инфраструктурный риск, регулятивный подход, межобъектные зависимости, источник воздействия, деструктивный эффект.

## Аннотация

**Цель работы:** развитие модели нарушителя информационной безопасности применительно к интеллектуализированным киберфизическим системам критической информационной инфраструктуры с учетом автономных программно-алгоритмических компонентов, межобъектных зависимостей и каскадного распространения деструктивных эффектов.

**Методы исследования:** системный анализ, структурно-функциональное и теоретико-множественное моделирование, классификация источников и сценариев деструктивных воздействий, элементы риск-ориентированного подхода.

**Результаты исследования:** предложена расширенная модель нарушителя информационной безопасности интеллектуализированных киберфизических систем критической информационной инфраструктуры, учитывающая автономность и адаптивность интеллектуальных компонентов, динамику межсистемных связей и возможность каскадного распространения нарушений. Определены условия перехода системы искусственного интеллекта в функционально-субъектное состояние; выделены антропогенные, программно-алгоритмические, инфраструктурно-технологические и гибридные категории источников и агентов воздействия. Сформулированы признаки инфраструктурно-динамического характера угроз, при которых деструктивный эффект возникает в результате взаимодействия человека, алгоритмов, данных, технических компонентов и текущего состояния инфраструктуры. Формализованы сценарии формирования деструктивного эффекта. Предложена структура показателей инфраструктурного риска, учитывающая автономность, адаптивность и каскадное распространение последствий. Обоснована возможность применения разработанной модели для раннего обнаружения и прогнозирования угроз, локализации нарушений, предупреждения каскадной деградаци и выбора механизмов реконфигурации и самовосстановления интеллектуализированных киберфизических систем. Полученные результаты могут применяться при моделировании угроз и обосновании мер защиты интеллектуализированных объектов КИИ.

DOI: 10.24412/1994-1404-2026-3-7-16

## Введение

В сфере информационной безопасности Российской Федерации (ИБ) за последние десятилетия сформировалась устойчивая концептуальная и методологическая база, определяющая объект защиты, источники угроз, модель нарушителя ИБ (далее — Модель), состав мер защиты и порядок оценки рисков. Данный подход закреплён в документах и регламентах в области защиты информации, в том числе рассматривающих

вопросы обеспечения безопасности критической информационной инфраструктуры Российской Федерации<sup>2</sup> (КИИ) [1].

<sup>2</sup> Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации. 2017. № 31. Ст. 4736.

<sup>1</sup> **Максимова Елена Александровна**, доктор технических наук, доцент, главный инженер-исследователь, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», пгт Сириус, Российская Федерация. ORCID 0000-0001-8788-4256.

E-mail: [maksimova.ea@talantiuspeh.ru](mailto:maksimova.ea@talantiuspeh.ru)

В контексте регулятивного (классического) подхода существующие Модели преимущественно описывают характеристики физического лица или группы лиц<sup>3</sup> [2, 3]. При этом автономные программно-алгоритмические компоненты, межобъектные зависимости и способность инфраструктуры к каскадному усилению последствий либо рассматриваются как внешние условия реализации угроз, либо не включаются в структуру Модели. Это затрудняет описание сценариев, в которых источник воздействия, непосредственный агент и механизм распространения деструктивного эффекта контекстно различимы.

Вместе с тем применение классической теории ИБ к КИИ не всегда является достаточным. В КИИ это связано с ее специфическими свойствами как сложной системы [4, 5]. Кроме того, в качестве объектов КИИ сегодня активно рассматриваются киберфизические системы (КФС) [6—11], в интеллектуализированном состоянии способные выступать в роли как объекта защиты, так и субъекта нападения (агента воздействия).

Под интеллектуализированной киберфизической системой (ИКФС) в настоящем исследовании понимается совокупность взаимосвязанных информационных, вычислительных, коммуникационных и физических компонентов, в которой функции анализа состояния, прогнозирования, принятия решений или управления частично либо полностью реализуются с применением методов искусственного интеллекта. В составе ИКФС система искусственного интеллекта (СИИ) может выступать программно-алгоритмическим компонентом, реализующим функции анализа, прогнозирования, принятия решений или управления [12].

В данном исследовании ИКФС будем рассматривать как целостный объект или совокупность взаимосвязанных объектов КИИ, а СИИ — как её интеллектуальный компонент, потенциально способный приобретать свойства функционального агента воздействия (далее — ФАВ).

Инфраструктурный деструктивизм (далее — ИнД) будем рассматривать как способность сложной информационной инфраструктуры порождать, распространять и усиливать деградационные состояния за счёт собственных связей, архитектуры, режимов взаимодействия и автономных компонентов. В отличие от классической модели «нарушитель — уязвимость — атака — ущерб» ИнД позволяет выполнить переход к модели, в которой учитываются не только субъектные действия, но и внутренние свойства инфраструктуры как источника деструктивной динамики<sup>4</sup> [13, 14].

Классическое понимание нарушителя ИБ основывается на представлении о физическом лице или ло-

гическом объекте, случайно или преднамеренно совершившем действие, следствием которого является нарушение ИБ организации<sup>5</sup>. В методических документах ФСТЭК России при оценке угроз ИБ акцент сделан на антропогенных источниках угроз. Данный подход является нормативно значимым и практически необходимым, однако применительно к ИКФС, он нуждается в развитии. Это обоснованно, так как он не в полной мере учитывает случаи, когда непосредственный агент воздействия имеет программно-алгоритмическую природу, а деструктивный эффект — инфраструктурный, распределённый или каскадный генезис. В рамках настоящего исследования расширяется не нормативное понятие актуального нарушителя, а состав элементов, учитываемых при построении его модели. Наряду с антропогенным источником угрозы рассматриваются ФАВ, механизм реализации воздействия и инфраструктурное распространение последствий. Такой подход не предполагает признания СИИ самостоятельным субъектом юридической ответственности.

### **Классификация деструктивных воздействий на элементы КИИ**

Для уточнения Модели классифицируем деструктивные воздействия в зависимости от их генезиса и влияния на межобъектные связи по следующим сценариям.

Сценарий 1 соответствует традиционной Модели и связан с проявлением ИнД вследствие целенаправленной деятельности субъекта, которому присваивается роль злоумышленника прямого воздействия<sup>6—8</sup>.

Сценарий 2 также частично учитывается действующими методическими подходами и связан с проявлением ИнД вследствие ошибочных действий субъекта, рассматриваемого в качестве нарушителя непреднамеренного воздействия<sup>2, 5, 6, 7</sup>.

Сценарий 3 связан с проявлением ИнД вследствие межобъектного взаимодействия. Реализуемые в ходе данного сценария процессы соответствуют представлениям о каскадных отказах, нормальных авариях, функциональном резонансе и взаимозависимости объектов критических инфраструктур.

Сценарий 4 возможен в условиях КИИ, где используемые в КФС СИИ выполняют функции анализа, прогнозирования, принятия решений и формирования управляющих воздействий. При достижении определённого уровня автономности и доступа к критически

<sup>3</sup> ФСТЭК России. Методика оценки угроз безопасности информации. Утв. ФСТЭК России 05.02.2021.

<sup>4</sup> Максимова Е.А. Модели и методы оценки информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генезиса : дис. ... докт. тех. наук: 2.3.6 / Максимова Елена Александровна, 2022. 448 с. EDN: OHNDPO.

<sup>5</sup> ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М. : Стандартинформ, 2009.

<sup>6</sup> ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил по применению мер обеспечения информационной безопасности. М. : Стандартинформ, 2021.

<sup>7</sup> ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М. : Стандартинформ, 2011.



значимым функциям такие системы приобретают свойства ФАВ на КИИ. В зависимости от происхождения целевой функции, режима эксплуатации и характера последствий СИИ может рассматриваться как инструмент антропогенного нарушителя, скомпрометированный логический компонент, источник непреднамеренного алгоритмического воздействия либо элемент гибридного распределённого сценария нарушения ИБ. Таким образом данный сценарий связан с автономным алгоритмическим воздействием, включая действия СИИ. То есть СИИ может рассматриваться как автономный агент управления или как катализатор межобъектного деструктивизма<sup>8, 9</sup> [13].

Предложенная система сценариев обосновывает выход за пределы классической теории ИБ и описывает внутреннюю способность сложной системы порождать условия саморазрушения через собственные связи, алгоритмы, архитектуру и режимы взаимодействия.

С учетом предложенных сценариев, деструктивные воздействия на элементы КИИ можно разделить на три класса.

Класс 1: прямые деструктивные воздействия на объекты КИИ и/или на межобъектные связи. Для данного класса применимы действующие процедуры моделирования угроз, оценки возможностей нарушителя, категорирования объектов и выбора мер защиты<sup>3, 10</sup>.

Класс 2: косвенные антропогенно обусловленные, как преднамеренные, так и непреднамеренные воздействия на объекты КИИ<sup>12</sup> [15]. Нарушитель выступает в том числе и как источник условий, порождающих уязвимости, ошибки проектирования, дефекты программного кода, конфигурационные нарушения или эксплуатационные несогласованности<sup>5, 6, 11, 12</sup>.

В данных ситуациях ИКФС может рассматриваться как объект КИИ, то есть как объект защиты.

Класс 3: косвенные воздействия нарушителя на объекты КИИ инфраструктурного генезиса технологического субъектного типа. Нарушитель является создателем технологического субъекта, способного самостоятельно реализовать деструктивные воздействия инфраструктурного генезиса.

По сути дела, на уровне деструктивных воздействий класса 3 возникает много вопросов, связанных с деятельностью ИКФС. Именно третий класс представляет наибольший научный интерес, поскольку он выходит

за пределы классической Модели. Если интеллектуальному компоненту ИКФС переданы функции лица, принимающего решение, то фактически она приобретает свойства функционального субъекта воздействия. При этом, оставаясь программным продуктом, СИИ в данном случае может содержать ошибки, алгоритмические погрешности и иные дефекты, способные привести к деструктивному результату<sup>3, 13, 14</sup>.

### **Переход программной системы из объектного в функционально-агентное состояние**

Включение СИИ в контуры управления КИИ требует рассмотрения проблемы перехода программной системы в функционально-агентное состояние. В классическом понимании программная система является объектом защиты, инструментом обработки данных или средством автоматизации. Однако при передаче ей функций принятия решений она приобретает признаки функциональной агентности<sup>12, 13, 15, 16, 17—20</sup>.

Рассмотрение этого перехода возможно на философском, программно-аппаратном, техническом, формально-математическом, этическом и нормативно-правовом уровнях. Философский уровень позволяет осмыслить природу субъектности, агентности и автономности программных систем. Технический — описывает механизмы реализации управляющих функций. Формально-математический — необходим для моделирования состояний, переходов и последствий решений. Этический и нормативно-правовой — связаны с вопросами ответственности, контроля и допустимых границ автономности<sup>12, 13</sup>. Системообразующим в данном случае будет уровень философского познания, через который возможно принятие сущностей процессов перехода программной системы из объектного в субъектное состояние.

Согласно ГОСТ<sup>4</sup>, нарушитель ИБ организации — это физическое лицо или логический объект, случайно или преднамеренно совершивший действия, следствием которых является нарушение ИБ организации. В данном определении уже содержится возможность его рассмотрения как логического объекта. В это же время в Методике нарушителя ИБ рассматриваются как антропогенные источники угроз, то есть лица или группы лиц<sup>6</sup>.

Таким образом, с одной стороны, ГОСТ<sup>4</sup> допускает рассмотрение логического объекта в качестве нарушителя. С другой стороны, Методика<sup>2</sup> конкретизирует актуального нарушителя преимущественно через

<sup>8</sup> ISO/IEC 23894:2023. Information technology — Artificial intelligence — Guidance on risk management. Geneva: ISO, 2023.

<sup>9</sup> ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system. Geneva: ISO, 2023.

<sup>10</sup> Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

<sup>11</sup> ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. М. : Стандартинформ, 2016.

<sup>12</sup> ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. М. : Стандартинформ, 2016.

<sup>13</sup> ISO/IEC 23894:2023. Information technology — Artificial intelligence — Guidance on risk management. Geneva: ISO, 2023.

<sup>14</sup> ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system. Geneva: ISO, 2023.

<sup>15</sup> ПНСТ 1046-2026. Искусственный интеллект в критической информационной инфраструктуре. Общие положения.

<sup>16</sup> ГОСТ Р 59276-2020. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения. М. : Стандартинформ, 2020.

<sup>17</sup> ГОСТ Р 59921.0-2022. Системы искусственного интеллекта. Часть 0. Основные положения. М. : Стандартинформ, 2022.

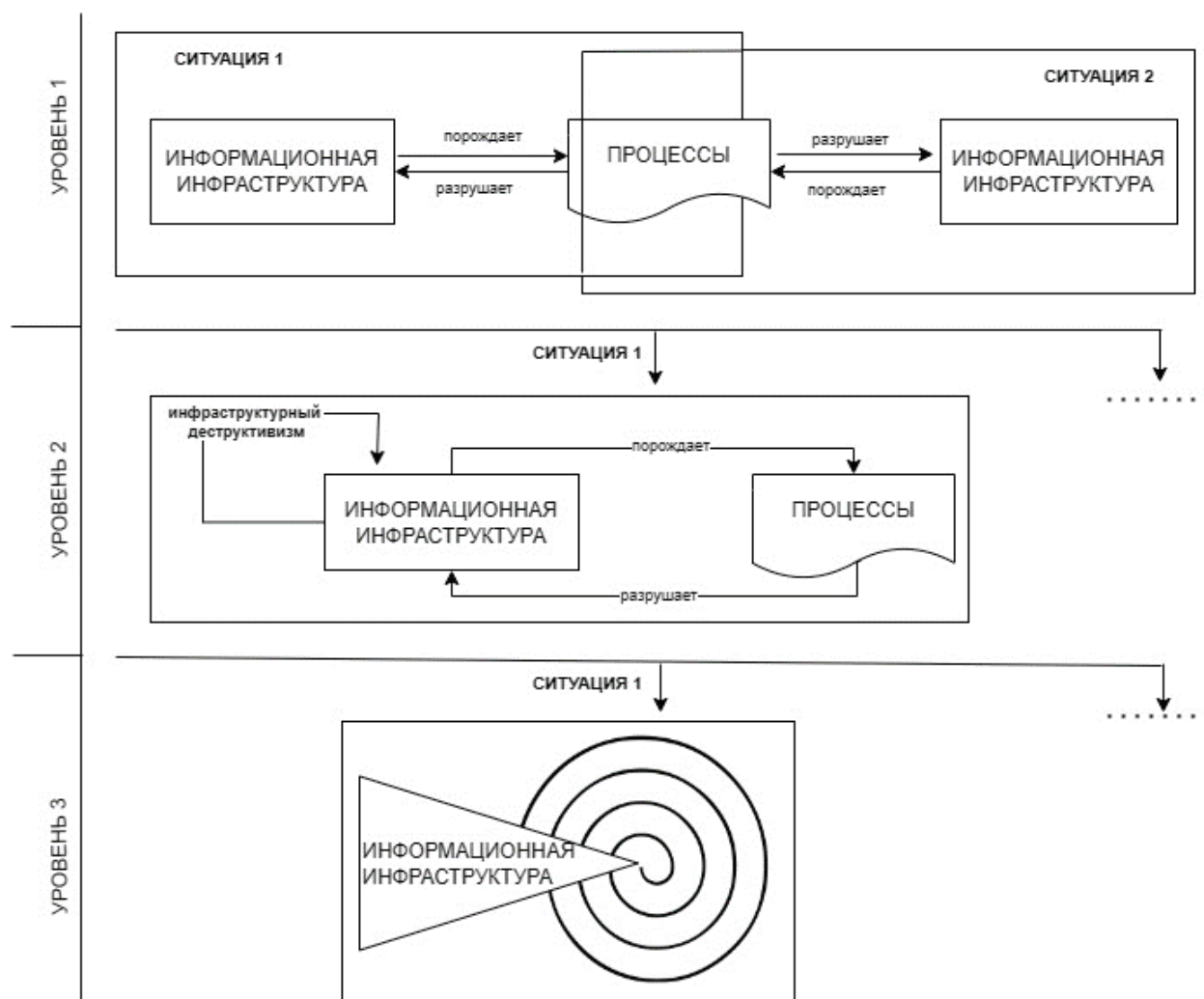


Рис. 1. Трехуровневая модель детализации развития инфраструктурного деструктивизма

физическое лицо или группу лиц. В контексте ИнД это значимо, поскольку ФАВ может быть логическим объектом, функционально реализующим субъектное воздействие на инфраструктуру.

В классической теории нарушитель и объект информатизации являются различными сущностями. В теории ИнД нарушитель и объект воздействия могут частично совпадать, а деструктивный эффект является результатом не внешней атаки, а следствием внутренних связей, алгоритмов и режимов функционирования. Данное явление представимо в виде трехуровневой модели детализации процесса развития ИнД в информационной инфраструктуре (рис. 1).

На первом уровне (рис. 1) отражается взаимное влияние информационной инфраструктуры и порождаемых ею процессов. На втором уровне показано формирование контура положительной обратной связи, в котором процессы, сформированные инфраструктурой, изменяют состояние её компонентов и связей. На третьем уровне представлено накопление и усиление деструктивных изменений, приводящее к переходу инфраструктуры в область преддеструктивных или деструктивных состояний.

### Ограничения субъектной парадигмы в контексте инфраструктурного деструктивизма

Описанную ситуацию можно обозначить как кризис субъектной парадигмы. С философской точки зрения субъектность традиционно связывается с активностью, намерением, рефлексией и способностью быть источником действия. Однако в условиях распределённых, автоматизированных и интеллектуализированных инфраструктур деструктивный эффект может возникать без явно выраженного субъекта-инициатора. В этом случае субъект перестаёт быть единственным и обязательным центральным элементом объяснения нарушения.

В традиционной Модели ключевым является вопрос: кто совершил деструктивное воздействие? В инфраструктурной Модели центр внимания смещается от субъекта к структуре, от намерения к зависимости, от события к процессу, от единичного воздействия к динамике распространения последствий.

В КИИ КФС представляют собой совокупность взаимозависимых компонентов. Поэтому нарушение в одном объекте может повлиять на другие объекты и на инфраструктуру в целом. ИнД фиксирует эту

особенность и описывает деструктивность не только как результат субъектного воздействия, но и как системное свойство инфраструктуры, способной порождать, распространять и усиливать деградационные состояния. Таким образом, ИнД можно рассматривать как методологический ответ на кризис субъектной парадигмы в сфере обеспечения безопасности КИИ.

Важно также отметить, что использование в КИИ СИИ дополнительно размывает и усложняет классическое понимание субъекта. СИИ может не обладать субъектностью в человеческом смысле, но при этом она способна принимать решения, инициировать действия и др. В результате возникает ситуация, при которой ФАВ является одновременно объектом защиты, инструментом управления и активным агентом воздействия на инфраструктуру.

Кроме того, если интеллектуализированный компонент КФС, действуя в соответствии с заданным алгоритмом и текущими параметрами среды, перераспределяет нагрузку таким образом, что это приводит к каскадной деградации, деструктивный эффект не может быть полностью объяснён намерением разработчика, ошибкой оператора или отказом отдельного объекта. В этом случае Модель должна учитывать также способность системы к автономному изменению состояния. Деструктивный эффект при этом будет возникать на пересечении данных, алгоритма, архитектуры, текущего состояния инфраструктуры и межобъектных зависимостей<sup>12</sup>.

Таким образом, из-за ограниченности традиционной субъектной парадигмы, предлагаемый инфраструктурно-динамический подход рассматривает нарушителя как элемент распределённого процесса воздействия. В рамках данного подхода деструктивность определяется не только намерением конкретного субъекта, но и результатом межфакторного взаимодействия внутри ИКФС.

#### **Интеллектуализированная киберфизическая система как функциональный агент воздействия на объекты КИИ**

Теория ИнД предполагает возможность существования искусственного функционального субъекта, самостоятельно принимающего решения на инфраструктурном уровне. В качестве такого субъекта может выступать СИИ<sup>12-16</sup>.

В контексте КИИ возникает вопрос: возможно ли рассматривать ИКФС в качестве объекта КИИ? При ответе на данный вопрос выделим три ситуации.

1) ИКФС идентифицирована как объект КИИ и подлежит защите в соответствии с действующей нормативно-правовой и методической базой<sup>1,2</sup>;

2) ИКФС выступает субъектом деструктивного воздействия на объекты КИИ;

3) ИКФС, первоначально рассматриваемая как объект КИИ, переходит в состояние функционального субъекта воздействия.

В ситуации 1 ИКФС рассматривается как компонент инфраструктуры, к которому применяются регулятив-

ные требования. Ситуации 2 и 3 методологически сложнее, так как ФАВ как субъект деструктивного воздействия, в настоящее время недостаточно формализован. Здесь возникает вопрос: можно ли рассматривать ФАВ как одну из категорий актуального нарушителя?

В соответствии с Методикой<sup>2</sup>, ИКФС не может быть напрямую отнесена к актуальным нарушителям, поскольку она не является физическим лицом или группой лиц. Однако если рассматривать ФАВ как антропогенно созданного логического объекта, функционально способного воздействовать на информационные ресурсы и компоненты систем и сетей, то появляется основание для расширения интерпретации Модели. В такой трактовке ФАВ может рассматриваться как функциональный субъект инфраструктурного воздействия.

В расширенной Модели источник деструктивного воздействия не всегда совпадает с его непосредственным функциональным агентом. В инфраструктурных сценариях деструктивный эффект может усиливаться и распространяться межобъектными связями уже после окончания воздействия.

Т.о., в расширенной Модели целесообразно разделять актуального нарушителя в нормативном смысле и ФАВ. Роль актуального нарушителя сохраняется за физическим лицом или группой лиц, выступающих антропогенным источником угрозы. Созданный, построенный либо скомпрометированный ими логический объект, включая интеллектуальный компонент ИКФС, может рассматриваться как функциональный агент, непосредственно реализующий, адаптирующий или усиливающий воздействие на объекты КИИ. Такое разграничение позволяет включить СИИ в структуру Модели, не наделяя техническую систему правосубъектностью.

#### **Формализация расширенной модели нарушителя информационной безопасности КИИ**

Предлагаемая формализация носит концептуальный характер и предназначена для определения состава и взаимосвязи параметров Модели.

В общем виде формализация расширенной Модели в КИИ, с учетом эффектов ИнД, представима в виде:

$$M_{\pi} = \langle \text{Src}, G, \text{Acc}, \text{Res}, \text{Act}, \text{Aut}, \text{Adp}, \text{Otar}, \text{Ch}, \text{Obs}, \text{Cas}, \text{Rec} \rangle, \quad (1)$$

где Src — источник воздействия; G — цели или функциональные приоритеты; Acc — уровень доступа; Res — доступные ресурсы; Act — множество возможных действий; Aut — степень автономности; Adp — способность адаптировать стратегию поведения; Otar — множество целевых объектов; Ch — каналы воздействия; Obs — доступная агенту информация о состоянии инфраструктуры; Cas — потенциал каскадного распространения последствий; Rec — способность к реконфигурации и продолжению воздействия при изменении среды.

Важно отметить, что именно параметры, определяющие способность к адаптивному и автономному поведению, отличают предлагаемую модель от традиционных Моделей.

Модель (1) применяется совместно с моделью КИИ;

$$KII = \langle O, L, S, Act, V, T, R, C, D, E \rangle, \quad (2)$$

где  $O = \{o_1, o_2, \dots, o_n\}$  — множество объектов КИИ;  $L = \{l_{ij}\}$  — множество межобъектных связей;  $S = \{s_1, s_2, \dots, s_m\}$  — множество антропогенных субъектов и функциональных агентов воздействия;  $Act = \{a_1, a_2, \dots, a_k\}$  — множество действий и воздействий, способных изменять состояния объектов и связей КИИ;  $V = \{v_1, v_2, \dots, v_p\}$  — множество уязвимостей, дефектов, ошибок конфигурации, архитектурных и алгоритмических несогласованностей;  $T = \{t_1, t_2, \dots, t_i\}$  — множество угроз ИБ;  $R = \{r_1, r_2, \dots, r_q\}$  — множество негативных последствий;  $C = \{c_1, c_2, \dots, c_z\}$  — множество ограничений;  $D = \{d_1, d_2, \dots, d_w\}$  — множество деструктивных состояний инфраструктуры;  $E = \{e_1, e_2, \dots, e_u\}$  — множество условий функционирования инфраструктуры.

С точки зрения регулятивного подхода событие ИБ обычно описывается через воздействие субъекта  $s_i$  на объект защиты  $o_j$  через реализуемое им воздействие  $a_k$ :

$$s_i \rightarrow a_k \rightarrow o_j \rightarrow r_q, \quad (3)$$

где  $r_q$  — негативное последствие нарушения ИБ.

В контексте ИнД схема (3) может быть расширена:

$$\langle s_i, a_k, o_j, l_{ij}, v_p, c_z \rangle \rightarrow d_w \rightarrow r_q. \quad (4)$$

Здесь удобно рассмотреть показатель деструктивности  $I_D(t)$ :

$$I_D(t) = F(O(t), L(t), S(t), Act(t), V(t), C(t), E(t)), \quad (5)$$

где  $E(t)$  — внешние и внутренние условия функционирования инфраструктуры.

Инфраструктура переходит из нормального состояния в деструктивное, если:

$$I_D(t) > \delta \Rightarrow KII(t) \in \Omega_D, \quad (6)$$

где  $\delta$  — допустимый порог;  $\Omega_D$  — область деструктивных состояний КИИ.

В области функционирования инфраструктуры можно выделить области:

- 1) нормального функционирования —  $\Omega_N$ ,
- 2) преддеструктивных состояний —  $\Omega_P$ ,
- 3) деструктивных состояний —  $\Omega_D$ ,
- 4) восстановления —  $\Omega_R$ .

Переходы между ними определяют динамику состояний КИИ:

$$\Omega_N \rightarrow \Omega_P \rightarrow \Omega_D \rightarrow \Omega_R \rightarrow \Omega_N.$$

Важно отметить, что в сложноструктурированной инфраструктуре данные переходы не всегда являются линейными.

В контексте ИнД можно ввести показатель  $R_I$  — инфраструктурный риск, связанный с участием СИИ в развитии управляющих решений на уровне КИИ:

$$R_I = P(T) \times U \times K_I \times K_c \times K_r, \quad (7)$$

где  $P(T)$  — вероятность реализации угрозы;  $U$  — величина потенциального ущерба;  $K_I$  — коэффициент межобъектной связности;  $K_c$  — коэффициент критичности затронутых функций;  $K_r$  — коэффициент каскадного распространения последствий.

Данный показатель характеризует инфраструктурную составляющую риска и позволяет учитывать факторы межобъектной связности, критичности функций и каскадного распространения последствий, которые могут не отражаться в локальной объектно-ориентированной оценке риска.

Для случаев, связанных с применением СИИ, модель (7) должна быть дополнена коэффициентом алгоритмической автономности  $K_{ai}$  и коэффициентом доверия к данным  $K_{data}$ :

$$R_{AI} = P(T_{AI}) \times U \times K_I \times K_c \times K_r \times K_{aut} \times K_{adp} \times K_d,$$

где  $R_{AI}$  — риск, связанный с включенностью ИКФС в управленческие функции на уровне КИИ;  $P(T_{AI})$  — вероятность реализации угрозы или ошибочного алгоритмического воздействия, связанного с ИКФС;  $K_{aut}$  — коэффициент автономности СИИ;  $K_{adp}$  — коэффициент адаптивности СИИ, характеризующий её способность изменять стратегию поведения в зависимости от данных и состояния инфраструктуры;  $K_d$  — коэффициент риска. Увеличение  $K_d$  соответствует увеличению риска, связанного со снижением качества данных.

Предложенные показатели имеют концептуальный характер. Значения порогов автономности, адаптивности и доступа, а также коэффициентов связности, критичности и каскадного распространения должны определяться применительно к архитектуре конкретной ИКФС. Практическое использование модели предполагает предварительную нормализацию и калибровку коэффициентов.

Интересна ситуация, в которой СИИ, входящая в состав ИКФС, приобретает свойства ФАВ, т. е. становится потенциальным нарушителем ИБ. В данном случае воздействие ИКФС на КИИ можно представить в виде:

$$Y_{AI}(t) = \Phi_{AI}(X(t), G, H, C_{AI}), \quad (8)$$

где  $Y_{AI}(t)$  — управляющее воздействие, сформированное СИИ в момент времени  $t$ ;  $X(t)$  — входные данные;  $G$  — целевая функция;  $H$  — накопленная история обучения и эксплуатации;  $C_{AI}$  — ограничения, правила безопасного функционирования и допустимые режимы принятия решений.

При этом переход ИКФС в функционально-субъектное состояние может быть задан условием:



$$a_{AI} \in S_{FAV} \text{ если } Aut > \alpha \wedge Acc \geq \beta \wedge Adp \geq \eta \wedge \gamma, \quad (9)$$

где  $a_{AI}$  — СИИ, рассматриваемая как потенциальный ФАВ;  $S_{FAV}$  — множество ФАВ;  $\alpha$  — порог автономности;  $\beta$  — порог доступа к критически значимым функциям;  $\eta$  — порог адаптивности;  $\gamma$  — минимально значимое изменение состояния КИИ, вызванное решением СИИ.

Таким образом, СИИ приобретает свойства ФАВ, если обладает достаточным уровнем автономности и адаптивности, имеет доступ к значимым функциям или объектам КИИ и способна формировать решения, вызывающие существенное изменение состояния инфраструктуры.

Для описания ФАВ, как потенциального нарушителя для объектов КИИ, определим следующие виды сценариев воздействия:

$sc_1$  — прямое преднамеренное воздействие субъекта;  
 $sc_2$  — непреднамеренное ошибочное воздействие субъекта;  
 $sc_3$  — межобъектное инфраструктурное воздействие;  
 $sc_4$  — автономное или полуавтономное алгоритмическое воздействие ФАВ.

Для каждого сценария можно задать обобщенную функцию деструктивного эффекта:

$$D\_sc[i] = F\_sc[i](S, O, L, Act, V, C, E), \quad (10)$$

где  $D\_sc[i]$  — деструктивный эффект в рамках сценария  $sc[i]$ ,  $i=1,4$ ;  $F\_sc[i]$  — функция преобразования исходных условий и воздействий в деструктивный результат. Модели реализации обозначенных видов сценариев представлены в таблице 1.

Таблица 1

**Модели реализации сценариев деструктивного воздействия на объекты КИИ**

| СЦЕНАРИЙ | МОДЕЛЬ                                           | ПОЯСНЕНИЯ                                                                                                                                                                               |
|----------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| $sc_1$   | $D\_sc_1 = F_1(S\_h \cup S\_g, A, O, V)$         | $S\_h$ — физическое лицо                                                                                                                                                                |
| $sc_2$   | $D\_sc_2 = F_2(S\_h \cup S\_g, A\_err, O, V, C)$ | $A\_err$ — множество ошибочных действий, включая ошибки эксплуатации, проектирования, настройки, сопровождения или управления.<br>$S\_g$ — группа лиц                                   |
| $sc_3$   | $D\_sc_3 = F_3(O, L, V, C, E)$                   | —                                                                                                                                                                                       |
| $sc_4$   | $D\_sc_4 = F_4(S\_I, X, M_{AI}, G, Y, O, L, C)$  | $S\_I$ — логический объект, выполняющий функции агента воздействия.<br>$X$ — входные данные СИИ.<br>$G$ — целевая функция.<br>$Y$ — сформированное решение или управляющее воздействие. |

Таким образом, ИнД может быть формально представлен как динамическое состояние, при котором возможно превышение допустимого порога деструктивности:

$$F(O(t), L(t), S(t), A(t), V(t), C(t), E(t)) > \delta. \quad (11)$$

Данное условие определяет отличие ИнД от классического нарушения ИБ, так как в инфраструктурной модели нарушение может быть результатом сложной динамики инфраструктуры.

Модель является исходной основой для разработки технологии самовосстановления КФС. Она позволяет учитывать факторы инфраструктурной динамики, которые могут не отражаться в объектно-ориентированной оценке рисков ИБ.

### Модель актуального нарушителя КИИ с учетом интеллектуализированных киберфизических систем

Для построения Модели в КИИ с учетом ИКФС целесообразно сохранить общую логику Методики<sup>2</sup>, но дополнить её параметрами, отражающими алгоритмическую и инфраструктурную природу воздействия. В частности, к исходным данным здесь должны также относиться сведения о функциях ФА, границах её автономности, типах принимаемых решений, источниках данных, архитектуре модели, режимах обучения, процедурах валидации и связях с объектами КИИ<sup>12-16</sup>.

Если ФАВ разрабатывается внешним исполнителем, то Модель может быть многокомпонентной. Конкретная структура при этом будет зависеть от сложности инфраструктуры субъекта КИИ, количества задач, решаемых с помощью интеллектуальных систем, уровня автономности ФА, квалификации разработчиков и характера интеграции в контуры управления.

Особое значение имеет вопрос целеполагания. В Методике<sup>2</sup> нарушители признаются актуальными, если возможные цели реализации угроз могут привести к негативным последствиям и соответствующим рискам. В отношении физического лица цель может быть связана с намерением, мотивом или интересом. В отношении ФАВ цель должна пониматься функционально.

В этой связи можно выделить целевые уровни субъектов деструктивного воздействия:

1) субъект-разработчик или оператор ФАВ, выступающий как нарушитель или злоумышленник в классическом смысле.

2) сам ФАВ как функциональный субъект воздействия, выступающий как непреднамеренный нарушитель, как инструмент злоумышленника или как автономный агент, реализующий деструктивный сценарий в пределах заданных алгоритмических правил. Здесь ФАВ может совмещать роли, так как его поведение может быть результатом наложения целевой функции, ошибочных данных, внешних команд и текущего состояния инфраструктуры. Поэтому для ФАВ возможны

состояния: цель непреднамеренного нарушения, цель злоумышленного использования или комбинированная цель, при которой один и тот же алгоритмический процесс приводит к разным типам деструктивных эффектов.

Так как при рассмотрении уровней возможностей ФАВ должны учитываться не только доступ и ресурсы, но и степень автономности, масштаб управляющих полномочий, качество данных, возможность самообучения, уровень интеграции с объектами КИИ, доступ к критическим функциям и наличие ограничителей безопасного поведения, то можно утверждать о необходимости адаптации и расширении уровней возможностей нарушителя, представленных в Методике<sup>2</sup>, при рассмотрении ИКФС.

### **Заключение**

В исследовании представлены взаимосвязанные классификации: по природе источника или функционального агента; по характеру воздействия; по сценарию формирования деструктивного эффекта. Представлены классификации источников и агентов, гибридных структур, видов воздействий, сценариев.

В работе предложено расширение Модели применительно к ИКФС КИИ. Показано, что в таких системах исходный источник деструктивного воздействия и функциональный агент могут различаться. Кроме

того, обосновано, что результаты воздействий могут формироваться за счёт межобъектных зависимостей, автономных алгоритмических решений и каскадной динамики инфраструктуры.

Представлены отличия между антропогенными, программно-алгоритмическими, инфраструктурно-технологическими и гибридными категориями источников и агентов воздействия. В качестве условий, при которых СИИ, входящая в состав ИКФС, приобретает свойства ФАВ определены достижения порогового уровня автономности и адаптивности, наличие доступа к функциям управления, способность самостоятельно формировать и реализовывать действия, изменяющие состояния объектов КИИ.

Формализованы сценарии формирования деструктивного эффекта. С учетом каскадного усиления последствий, автономности и адаптивности программно-алгоритмических компонентов описана структура оценки инфраструктурного риска.

Полученные в ходе исследования результаты возможно использовать при разработке моделей угроз, уточнении характеристик актуальных нарушителей, выявлении ФАВ и обосновании мер защиты интеллектуализированных объектов КИИ. Развитие предложенной тематики можно направить на апробацию модели на типовых архитектурах киберфизических систем и исследование процессов самовосстановления ИКФС в условиях ИнД.

*Исследование выполнено за счет гранта Российского научного фонда № 25-11-20037 «Технология самовосстановления киберфизических систем национальной критической информационной инфраструктуры в условиях беспрецедентного роста угроз безопасности на основе искусственного интеллекта» (руководитель — д.т.н. Петренко С.А.).*

### **Литература**

1. Яковлев А.В., Пеливан М.А. Предметно-смысловые ограничения при моделировании компьютерного противоборства // Правовая информатика. 2024. № 3. С. 86—95. DOI: 10.24682/1994-1404-2024-3-86-95. EDN: JYEUHQ.
2. Чечулин А.А. Моделирование нарушителя, инфраструктуры и атак в системах информационной безопасности // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2024. № 2. С. 70—79. DOI: 10.61260/2218-130X-2024-2-70-79. EDN: VHHYHE.
3. Трещев И.А., Монастырская Е.И. Событийная формальная модель поведения злоумышленника // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2024. № 1 (73). С. 42—46. EDN: IZQRGT.
4. Nickolov E. Critical Information Infrastructure Protection Analysis Evaluation and Expectations // Information and Security. An International Journal, vol. 17, 2005, pp. 105—119. URL: [https://www.researchgate.net/publication/228343373\\_Critical\\_Information\\_Infrastructure\\_Protection\\_Analysis\\_Evaluation\\_and\\_Expectations](https://www.researchgate.net/publication/228343373_Critical_Information_Infrastructure_Protection_Analysis_Evaluation_and_Expectations)
5. Sunyaev A. (2024). Critical Information Infrastructures. In: Internet Computing. Springer, Cham. DOI: 10.1007/978-3-031-61014-1\_11.
6. Балябин А.А., Петренко С.А. Метод обеспечения киберустойчивости платформ управления киберфизическими объектами на основе кибериммунитета // Защита информации. Инсайд. 2025. № 6 (126). С. 21—29. EDN: ZZTXGC.
7. Соболев Н.В. Систематизация атак с нулевой динамикой для различных типов киберфизических систем // Проблемы информационной безопасности. Компьютерные системы. 2026. № S2 (70). С. 81—95. DOI: 10.66424/2071-8217-2026-S2-8. EDN: KDDCBB.



8. Кравец А.Г., Сальникова Н.А., Долгова Е.П. Анализ методов решения проблем управления киберфизическими системами // Математические методы в технологиях и технике. 2025. № 3. С. 102—106. EDN: VQPCFW.
9. Петренко С.А. Кибериммунология. СПб. : Афина, 2021. 239 с. ISBN 978-5-9909868-7-9. EDN: ARCUWY.
10. Furrer F.J. (2022). Cyber-Physical Systems. In: Safety and Security of Cyber-Physical Systems. Springer Vieweg, Wiesbaden. DOI: 10.1007/978-3-658-37182-1\_2.
11. Paul P.K., Chatterjee R., Kayyali M., Das N. (2025). Cyber-Physical Systems: Its Foundation, Emergence, Possible Applications, and Issues with Reference to the Education Sector. In: Choudhury A., Kaushik K., Kumar V., Singh B.K. (eds), Cyber-Physical Systems Security. Studies in Big Data, vol. 154. Springer, Singapore. DOI: 10.1007/978-981-97-5734-3\_1.
12. Привалов А.Н., Богомолов А.В., Ларкин Е.В. Моделирование надежности программных компонентов киберфизических систем // Программные продукты и системы. 2025. № 1. С. 47—54. DOI: 10.15827/0236-235X.149.047-054. EDN: KSYSDN.
13. Максимова Е.А. Методы выявления и идентификации источников деструктивных воздействий инфраструктурного генеза // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 2. С. 86—99. EDN: KTYQJE.
14. Romashkina N.P., Markov A.S., Stefanovich D.V. Information Technologies and International Security. Moscow : IMEMO, 2023. 111 p. URL: <https://www.imemo.ru/publications/info/information-technologies->
15. Максимова Е.А., Садовникова Н.П. Межсубъектное взаимодействие как источник деструктивных воздействий на субъекте критической информационной инфраструктуры // Прикаспийский журнал: управление и высокие технологии. 2021. № 2 (54). С. 71—80. DOI: 10.21672/2074-1707.2021.53.1.071-0800. EDN: MJJRWJ.

**SECTION:**

*SYSTEM ANALYSIS, MANAGEMENT, ARTIFICIAL INTELLIGENCE, AND INFORMATION PROTECTION*

# **AN INFORMATION SECURITY ADVERSARY MODEL FOR INTELLIGENT CYBER-PHYSICAL SYSTEMS IN CRITICAL INFORMATION INFRASTRUCTURE**

**Maksimova E.A.**<sup>18</sup>

**Keywords:** *artificial intelligence, destructive impacts, functional agent, infrastructure destructivism, cascading consequences, autonomy, infrastructure risk, regulatory approach, inter-object dependencies, source of impact, destructive effect.*

## **Abstract**

**Purpose of work:** *development of a model of an information security adversary in relation to intelligent cyber-physical systems of critical information infrastructure, taking into account autonomous software and algorithmic components, inter-object dependencies, and the cascading propagation of destructive effects.*

**Research methods:** *system analysis, structural-functional and set-theoretic modeling, classification of sources and scenarios of destructive impacts, elements of a risk-based approach.*

**Results of the study:** *An extended model of an information security threat actor targeting intelligent cyber-physical systems within critical information infrastructure is proposed; the model accounts for the autonomy and adaptability of intelligent components, the dynamics of inter-system connections, and the potential for the cascading propagation of security breaches. Conditions for an artificial intelligence system to transition into a “functional-agent” state are defined, and categories of impact sources and agents — classified as anthropogenic, software-algorithmic, infrastructural-technological, and hybrid — are identified. Characteristics of infrastructure-dynamic threats are formulated, wherein a destructive effect arises from the interaction between humans, algorithms, data, technical components, and the infrastructure’s current state. Scenarios leading to such destructive effects are formalized. A framework of infrastructure risk indicators is proposed, incorporating factors such as autonomy, adaptability, and the cascading propagation of consequences. The applicability of the developed model is substantiated for early threat detection and forecasting, breach containment, the prevention of cascading degradation, and the selection of reconfiguration and self-healing mechanisms for intelligent cyber-physical systems. The results obtained can be utilized in threat modeling and in justifying protection measures for intelligent CII assets.*

---

<sup>18</sup> **Elena A. Maksimova**, Dr.Sc. (Technology), Chief Research Engineer, Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sirius urban-type settlement, Russian Federation. ORCID: 0000-0001-8788-4256.  
E-mail: [maksimova.ea@talantiuspeh.ru](mailto:maksimova.ea@talantiuspeh.ru)

## References

1. Iakovlev A.V., Pelivan M.A. Predmetno-smyslovye ogranicheniia pri modelirovanii komp'uternogo protivoborstva // Pravovaia informatika. 2024. No. 3. S. 86—95. DOI: 10.24682/1994-1404-2024-3-86-95. EDN: JYEUMQ.
2. Chechulin A.A. Modelirovanie narushitel'ia, infrastruktury i atak v sistemakh informatsionnoi bezopasnosti // Nauchno-analiticheskii zhurnal "Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoi protivopozharnoi sluzhby MChS Rossii". 2024. No. 2. S. 70—79. DOI: 10.61260/2218-130X-2024-2-70-79. EDN: VHHYHE.
3. Treshchev I.A., Monastyraia E.I. Sobytiinaia formal'naia model' povedeniia zloumyshlennika // Uchenye zapiski Komsomol'skogo-na-Amure gosudarstvennogo tekhnicheskogo universiteta. 2024. No. 1 (73). S. 42—46. EDN: IZQRGT.
4. Nickolov E. Critical Information Infrastructure Protection Analysis Evaluation and Expectations // Information and Security. An International Journal, vol. 17, 2005, pp. 105—119. URL: [https://www.researchgate.net/publication/228343373\\_Critical\\_Information\\_Infrastructure\\_Protection\\_Analysis\\_Evaluation\\_and\\_Expectations](https://www.researchgate.net/publication/228343373_Critical_Information_Infrastructure_Protection_Analysis_Evaluation_and_Expectations)
5. Sunyaev A. (2024). Critical Information Infrastructures. In: Internet Computing. Springer, Cham. DOI: 10.1007/978-3-031-61014-1\_11.
6. Baliabin A.A., Petrenko S.A. Metod obespecheniia kiberustoichivosti platform upravleniia kiberfizicheskimi ob"ektami na osnove kiberimmuniteta // Zashchita informatsii. Insaid. 2025. No. 6 (126). S. 21—29. EDN: ZZTXGC.
7. Sobolev N.V. Sistematizatsiia atak s nulevoi dinamikoi dlia razlichnykh tipov kiberfizicheskikh sistem // Problemy informatsionnoi bezopasnosti. Komp'uternye sistemy. 2026. No. S2 (70). S. 81—95. DOI: 10.66424/2071-8217-2026-S2-8. EDN: KDDCBB.
8. Kravets A.G., Sal'nikova N.A., Dolgova E.P. Analiz metodov resheniia problem upravleniia kiberfizicheskimi sistemami // Matematicheskie metody v tekhnologiiakh i tekhnike. 2025. No. 3. S. 102—106. EDN: VQPCFW.
9. Petrenko S.A. Kiberimmunologiya. SPb. : Afina, 2021. 239 s. ISBN 978-5-9909868-7-9. EDN: ARCUWY.
10. Furrer F.J. (2022). Cyber-Physical Systems. In: Safety and Security of Cyber-Physical Systems. Springer Vieweg, Wiesbaden. DOI: 10.1007/978-3-658-37182-1\_2.
11. Paul P.K., Chatterjee R., Kayyali M., Das N. (2025). Cyber-Physical Systems: Its Foundation, Emergence, Possible Applications, and Issues with Reference to the Education Sector. In: Choudhury A., Kaushik K., Kumar V., Singh B.K. (eds), Cyber-Physical Systems Security. Studies in Big Data, vol. 154. Springer, Singapore. DOI: 10.1007/978-981-97-5734-3\_1.
12. Privalov A.N., Bogomolov A.V., Larkin E.V. Modelirovanie nadezhnosti programmnykh komponentov kiberfizicheskikh sistem // Programmnye produkty i sistemy. 2025. No. 1. S. 47—54. DOI: 10.15827/0236-235X.149.047-054. EDN: KSYSDN.
13. Maksimova E.A. Metody vyivleniia i identifikatsii istochnikov destruktivnykh vozddeistvii infrastrukturnogo geneza // Elektronnyi setevoi politematicheskii zhurnal "Nauchnye trudy KubGTU". 2022. No. 2. S. 86—99. EDN: KTYQJE.
14. Romashkina N.P., Markov A.S., Stefanovich D.V. Information Technologies and International Security. Moscow : IMEMO, 2023. 111 p. URL: <https://www.imemo.ru/publications/info/information-technologies->
15. Maksimova E.A., Sadovnikova N.P. Mezhsob"ektnoe vzaimodeistvie kak istochnik destruktivnykh vozddeistvii na sub"ekte kriticheskoi informatsionnoi infrastruktury // Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii. 2021. No. 2 (54). S. 71—80. DOI: 10.21672/2074-1707.2021.53.1.071-0800. EDN: MJJRWJ.



# МЕТОДИКА ОЦЕНКИ КВАНТОВОЙ УСТОЙЧИВОСТИ БЛОКЧЕЙН-ПЛАТФОРМ НА ОСНОВЕ СЕТЕЙ ПЕТРИ

Ларина М.В.<sup>1</sup>, Скиба В.Ю.<sup>2</sup>

**Ключевые слова:** квантовые угрозы, консенсус, критическая информационная инфраструктура, оценка рисков, постквантовая криптография, формализация атак, цифровые платформы, Proof-of-Stake, Proof-of-Work.

## Аннотация

**Цель работы** состоит в разработке методики оценки квантовой устойчивости блокчейн-платформ на основе математического аппарата сетей Петри, предназначенной для моделирования сценариев квантовых атак и выявления критических состояний функционирования распределенной системы.

**Методы исследования:** анализ устойчивости механизмов консенсуса Proof-of-Work и Proof-of-Stake, формализация атак и сценариев нарушений в терминах сетей Петри, оценка влияния криптографических, сетевых и вычислительных параметров на вероятность реализации угроз.

**Результаты исследования:** предложена модель, учитывающая зависимости между состояниями системы, параметрами переходов и вероятностями успешного выполнения атак. На основе данного подхода разработан программный комплекс для моделирования и сравнительного анализа сценариев безопасности блокчейн-платформ.

**Научная новизна:** методика оценки квантовой устойчивости блокчейн-платформ объединяет в единой модели криптографические, вычислительные и сетевые параметры, а также сценарный анализ устойчивости механизмов консенсуса Proof-of-Work и Proof-of-Stake. Формализация в терминах сетей Петри связывает логическую последовательность этапов атаки с количественными условиями их прохождения и позволяет выявлять критические состояния системы, оценивать вероятность реализации атак и учитывать взаимосвязь между криптографическими механизмами и структурой сети.

**Практическая значимость:** предложенная методика может быть использована при создании квантово-устойчивых блокчейн-экосистем и систем защиты критической информационной инфраструктуры.

DOI: 10.24412/1994-1404-2026-3-17-28

## Введение

Развитие квантовых вычислений является одним из факторов, способных значительно изменить существующие подходы к обеспечению информационной безопасности. Создание квантовых вычислительных систем с достаточным количеством логических кубитов потенциально позволит решать ряд математических задач эффективнее классических вычислительных систем. Проблема особенно актуальна для криптографических механизмов, поскольку стойкость широко используемых алгоритмов с открытым ключом

основана на вычислительной сложности задач, которые могут эффективно решаться с применением квантовых алгоритмов.

Вопрос перехода к постквантовой криптографии в настоящее время рассматривается на уровне международных организаций и национальных органов стандартизации. Национальный институт стандартов и технологий США (NIST) в августе 2024 года утвердил первые три федеральных стандарта постквантовой криптографии: FIPS 203 для механизма установления

<sup>1</sup> Ларина Мария Васильевна, лаборант-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус»», пгт Сириус, Краснодарский край, Российская Федерация. ORCID: 0009-0009-7826-0180.

E-mail: larina.mv@talantiuspeh.ru

<sup>2</sup> Скиба Владимир Юрьевич, доктор технических наук, старший научный сотрудник, главный инженер-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус»», пгт Сириус, Краснодарский край, Российская Федерация, профессор кафедры ИБМ-6 ФГАОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», г. Москва, Российская Федерация, профессор кафедры № 2 «Автоматика» национального исследовательского ядерного университета «МИФИ», г. Москва, Российская Федерация. ORCID: 0000-0002-9805-7800.

E-mail: skiba.vy@talantiuspeh.ru

ключей ML-KEM, FIPS 204 для цифровой подписи ML-DSA и FIPS 205 для цифровой подписи SLH-DSA. В NIST отмечается, что данные стандарты предназначены для защиты от будущих атак с использованием квантовых компьютеров и являются основой перехода к криптографическим механизмам, устойчивым к квантовым угрозам<sup>3</sup>.

Необходимость заблаговременной подготовки к такому переходу отмечается и Европейским агентством по кибербезопасности (ENISA). В материалах ENISA подчеркивается, что переход к постквантовой криптографии не ограничивается выбором новых алгоритмов и их стандартизацией: требуется адаптация существующих протоколов и информационных систем, а сам процесс миграции может занимать значительное время<sup>4</sup>. При этом организация отдельно указывает на необходимость уже на современном этапе учитывать угрозы, связанные с квантовыми вычислениями, несмотря на то что полномасштабные квантовые вычислительные системы, способные практически взламывать широко используемые криптографические схемы, пока не получили широкого распространения.

В соответствии с Концепцией обеспечения устойчивости цифровых платформ и блокчейн-экосистем в условиях появления квантовых угроз [1] особую значимость проблема приобретает для блокчейн-экосистем, поскольку криптографические механизмы являются одним из фундаментальных элементов их архитектуры. Согласно определению NIST, блокчейн представляет собой распределенный цифровой реестр криптографически подписанных транзакций, объединенных в блоки, причем каждый блок криптографически связан с предыдущим после проверки и принятия соответствующего решения механизмом консенсуса<sup>5</sup>. Таким образом, обеспечение целостности реестра и подтверждение прав участников непосредственно связаны с криптографическими механизмами и протоколами распределенного консенсуса. В NISTIR 8202 отмечается, что существенной составляющей блокчейн-технологий являются механизмы консенсу-

са, определяющие порядок формирования новых блоков и разрешения конфликтов между участниками распределенной сети. В документе рассматриваются различные модели консенсуса, в том числе Proof-of-Work (PoW) и Proof-of-Stake (PoS), отличающиеся ресурсом, определяющим возможность участника влиять на формирование состояния распределенного реестра.

Следовательно, квантовая угроза для блокчейн-экосистем не сводится исключительно к возможности компрометации используемого криптографического алгоритма. Изменение соотношения вычислительных возможностей участников сети, компрометация ключей и нарушение механизмов подтверждения транзакций могут иметь последствия для целостности распределенного реестра. Для платформ с PoW существенное значение приобретает изменение соотношения вычислительных ресурсов участников, тогда как для PoS критическим параметром является доля контролируемого стейка. При этом успешная атака может включать несколько последовательных этапов, например получение необходимого количества идентичностей, достижение требуемой доли ресурса консенсуса, создание конкурирующей ветви цепочки и последующую реализацию двойного расходования.

Дополнительную сложность представляет необходимость учитывать не только возможность наступления отдельного события, но и взаимосвязь последовательных этапов атаки. Например, достижение нарушителем определенной доли вычислительных ресурсов в PoW или доли стейка в PoS само по себе не характеризует итоговый риск в полном объеме. Необходимо дополнительно учитывать количество подтверждений транзакции, вероятность формирования конкурирующей цепочки, временные ограничения, механизмы обнаружения конфликта и экономические последствия реализации атаки. Методы количественной оценки квантовой устойчивости блокчейн-платформ рассматривались в [2]. Однако существующие подходы могут быть дополнены формализацией последовательности реализации угрозы с использованием сетей Петри<sup>6</sup>, позволяющих описывать состояния системы, события и условия перехода между состояниями. Применение данного математического аппарата дает возможность представить сценарий атаки как последовательность взаимосвязанных состояний и формально определить условия достижения конечного состояния.

Данная статья является продолжением работ [3, 4], посвященных классификации информационных систем в условиях развития квантовых информационных технологий и стратификации угроз безопасности инфор-

<sup>3</sup> Федеральные стандарты NIST:

FIPS 203. Federal Information Processing Standards Publication. Module-Lattice-Based Key-Encapsulation Mechanism Standard. Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD 20899-8900. Published August 13, 2024. DOI: 10.6028/NIST.FIPS.203.

FIPS 204. Federal Information Processing Standards Publication. Module-Lattice-Based Digital Signature Standard. Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD 20899-8900. Published August 13, 2024. DOI: 10.6028/NIST.FIPS.204.

FIPS 205. Federal Information Processing Standards Publication. Stateless Hash-Based Digital Signature Standard. Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD 20899-8900. Published August 13, 2024. DOI: 10.6028/NIST.FIPS.205.

<sup>4</sup> European Union Agency for Cybersecurity. Post-Quantum Cryptography: Current State and Quantum Mitigation. Heraklion: ENISA, 2021.

<sup>5</sup> Yaga D., Mell P., Roby N., Scarfone K. Blockchain Technology Overview: NISTIR 8202. Gaithersburg, MD: National Institute of Standards and Technology, 2018. 57 p. DOI: 10.6028/NIST.IR.8202.

<sup>6</sup> Например, использование обычных и цветных сетей Петри для анализа блокчейн-систем рассматривалось в работах: Pinna A., Tonelli R., Orrù M., Marchesi M. A Petri Nets Model for Blockchain Analysis // The Computer Journal. 2018. Vol. 61. No. 9. P. 1374—1388. DOI: 10.1093/comjnl/bxy001; Liu Z., Liu J. Formal Verification of Blockchain Smart Contract Based on Colored Petri Net Models // 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). Milwaukee, WI, USA: IEEE, 2019. P. 555—560. DOI: 10.1109/COMPSAC.2019.10265.



мации в них, а также работы [5], в которой предложена модель цифровой платформы для анализа её устойчивости к квантовым угрозам. В отличие от подхода, ориентированного исключительно на оценку стойкости отдельных криптографических механизмов, в данной работе предлагаемая методика рассматривает с использованием сетей Петри<sup>7</sup> развитие атаки как совокупность взаимосвязанных событий и позволяет учитывать вероятность успешного прохождения отдельных этапов, параметры механизма консенсуса PoW и PoS и применяемые защитные меры.

### Математическая постановка задачи

В рамках предлагаемого подхода блокчейн-экосистема задается вектором параметров  $\Theta$ , характеризующим тип консенсуса, применяемые политики безопасности, сеть и количество ее участников. Сценарий атаки рассматривается как последовательность событий, которая при фиксированном наборе параметров  $\Theta$  может привести к нарушению заданного свойства безопасности. В качестве конечного события могут выступать компрометация ключа, несанкционированный вывод активов, получение контроля над критической долей ресурса консенсуса или успешное двойное расходование.

Для формального представления сценария используется сеть Петри:

$$N = \{P, T, I, O, \mu^0\},$$

где  $P$  — конечное множество позиций;

$T$  — множество переходов;

$I$  и  $O$  — входная и выходная функции;

$\mu^0$  — начальная маркировка.

Позиции интерпретируются как состояния моделируемого сценария, а переходы — как события, изменяющие состояние системы. Наличие фишки в позиции означает достижение соответствующего состояния. Переход разрешен, если выполнены необходимые условия и на входных позициях присутствуют требуемые фишки.

Такое представление позволяет отделить количественную часть оценки от логики развития атаки. Вероятностная модель определяет значения показателей, используемых в условиях переходов, а сеть Петри фиксирует допустимую последовательность событий.

В этом случае можно сформировать четыре типа сценариев:

1. PoW\_1 — компрометация ключей в блокчейн-платформе с консенсусом PoW;
2. PoS\_1 — компрометация ключей в блокчейн-платформе с консенсусом PoS;
3. PoW\_2 — составная атака «Сивилла — 51% или двойная трата» для PoW;
4. PoS\_2 — составная атака «Сивилла — 51% или двойная трата» для PoS.

Сценарии первого и второго типа ориентированы на анализ криптографического звена, а сценарии третьего и четвертого типа описывают развитие составной атаки на уровне консенсуса. Такое разделение позволяет исследовать как локальную уязвимость отдельного механизма защиты, так и ее возможные последствия для функционирования распределенного реестра.

Таким образом, выделены можно выделить следующие задачи:

1. для выбранных сценариев атак на блокчейн-экосистемы построить сети Петри  $N(\Theta)$  и отображение параметров  $\Theta$  на структуру сети и на условия переходов;
2. определить набор показателей устойчивости  $U(N, \Theta)$  при реализации сценариев атак при заданных условиях;
3. реализовать уравнения динамики сети Петри и построение множества достижимых состояний;
4. разработать методику оценки  $U(N, \Theta)$ .

### Методика оценки сценариев компрометации ключей

Учитывая, что криптографические механизмы (цифровые подписи, процедуры управления ключами и т. д.) являются фундаментальными компонентами блокчейн-экосистем и используются для подтверждения прав на совершение транзакций, получение злоумышленником приватного ключа или достаточного количества ключей в пороговой схеме позволяет сформировать корректную с точки зрения протокола транзакцию от имени владельца скомпрометированного ключа.

В отличие от сценариев двойной траты, рассматриваемая атака не предполагает непосредственного нарушения механизма консенсуса. Злоумышленнику не требуется изменять состояние распределенного реестра путем формирования альтернативной цепи или получать контроль над большей частью вычислительных либо стейкинг-ресурсов сети. Достаточно пройти предусмотренные платформой процедуры авторизации и подписания операции. Для блокчейн-экосистем с механизмами консенсуса PoW и PoS базовая логика развития атаки совпадает, а различия учитываются параметрами модели, связанными с особенностями соответствующего участника сети. Устойчивость блокчейн-экосистем при этом определяется не только механизмом консенсуса, но и криптографической стойкостью используемых примитивов [6].

В модели сценарий представляется с помощью сети Петри (Рис. 1). Начальное состояние соответствует отсутствию атаки (p1). Далее последовательно моделируются компрометация ключа (p2), формирование и подписание транзакции (p3 и p4), проверка баланса (p5), проверка адреса назначения (p6) и ожидание исполнения операции (p7). При срабатывании защитного механизма переход осуществляется в состояние блокирования (p8 и p11), а при успешном прохождении всех проверок — в состояние исполнения транзакции (p9 и p10).

<sup>7</sup> Pinna, A. A Petri Nets Model for Blockchain Analysis / A. Pinna, R. Tonelli, M. Orrù, M. Marchesi // IEEE Access. 2017. DOI: 10.1109/ACCESS.2017.2749606.



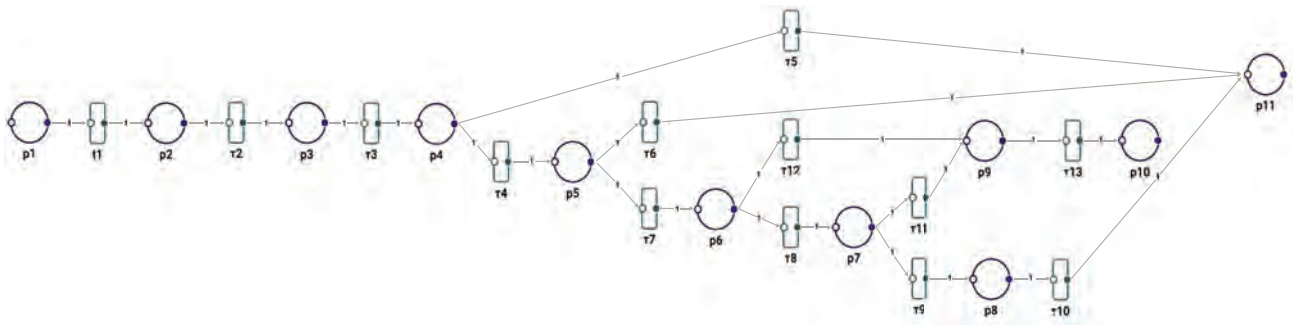


Рис. 1. Сеть Петри для сценария компрометации ключей

Возникновение криптографически значимых квантовых вычислений связано, в частности, с возможностью применения квантовых алгоритмов криптоанализа, включая алгоритм Шора [7—9]. В предлагаемой модели влияние квантовых вычислений учитывается посредством коэффициента квантового ускорения  $K$ .

Переход к состоянию компрометации определяет условием  $P_{raw} > 0$ .

После формирования транзакции проверяется достаточность баланса:

$$V_{attack} \leq B,$$

где  $V_{attack}$  — сумма вывода,  $B$  — баланс счета.

При использовании списка разрешенных адресов транзакция также должна быть направлена на адрес, включенный в *allowlist*. При наличии задержки вывода операция может быть обнаружена и заблокирована до исполнения. Такая последовательность соответствует общей логике оценки угроз, включающей анализ способа реализации, возможностей нарушителя и последствий атаки.

Для количественной оценки используются базовая вероятность компрометации ключа  $p_{base}$ , длина ключа  $key\_bits$ , горизонт наблюдения  $t_{obs}$ , срок действия ключа  $t_{valid}$ , коэффициент квантового ускорения  $K$ , параметры схемы подписания и коэффициенты эффективности защитных механизмов.

Тогда долю периода риска можно определить как:

$$m_T = \frac{\min(t_{valid}, t_{obs})}{t_{obs}}.$$

Для учета длины ключа используется нормированный коэффициент:

$$f_{key} = \min(1, \max(0, \frac{key\_bits}{256})).$$

Для параметризации влияния длины ключа на вероятность его компрометации введем множитель  $k_{len} = 2 - f_{key}$ . При этом значение 256 бит принимается в качестве нормирующего значения в предлагаемой модели, а введение коэффициента позволяет учитывать повышенную уязвимость более коротких ключей в рамках рассматриваемой модели.

Базовая вероятность компрометации ключа до учета квантового ускорения определяется как:

$$P_{raw}^0 = p_{base} \cdot m_T \cdot k_{len}$$

где  $p_{base}$  — базовая вероятность компрометации ключа за горизонт наблюдения;

$m_T$  — доля эффективного срока ключа внутри горизонта наблюдения;

$k_{len}$  — множитель, отражающий зависимость вероятности компрометации от длины криптографического ключа.

Учет возможного вычислительного преимущества нарушителя выполняется с помощью коэффициента  $K \geq 1$ :

$$P_{raw} = \min(1, P_{raw}^0 \cdot K).$$

Необходимость учета такого параметра связана с перспективой появления криптографически значимых квантовых вычислительных систем и переходом к постквантовым алгоритмам<sup>8</sup>. При этом  $K$  является параметром сценарного анализа, а не характеристикой конкретного квантового устройства.

Для обычной схемы с одним ключом вероятность прохождения этапа подписания принимается равной  $P_{raw}$ . Если используется пороговая схема *t*-из-*n*, вероятность компрометации необходимого количества участников определяется биномиальной моделью:

$$P_{binomial} = P(X \geq t) = \sum_{k=t}^n C_n^k \cdot p_{party}^k (1 - p_{party})^{n-k},$$

где  $p_{party}$  — вероятность компрометации одного участника.

Итоговая вероятность после подписания имеет вид:

$$P_{after-sign} = P_{raw} \text{ — для одного ключа,}$$

$P_{after-sign} = \min(1, P_{raw} \cdot P_{binomial})$  — для схемы *t*-из-*n*.

Влияние механизмов защиты учитывается коэффициентами  $\varepsilon_i$ , характеризующими вероятность блокирования атаки отдельным механизмом. В модели рассматриваются HSM, ротация ключей, *allowlist*, мониторинг, ручное подтверждение, задержка вывода и ограничение суммы транзакции.

При допущении независимости защитных механизмов вероятность после их применения определяется как:

$$P_{after-defend} = P_{after-sign} \cdot \prod_i (1 - \varepsilon_i).$$

Если механизм защиты отсутствует, соответствующий множитель принимается равным единице. Значе-

<sup>8</sup> National Cybersecurity Center of Excellence. Frequently Asked Questions about Post-Quantum Cryptography. URL: <https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/FAQ/index.htm>

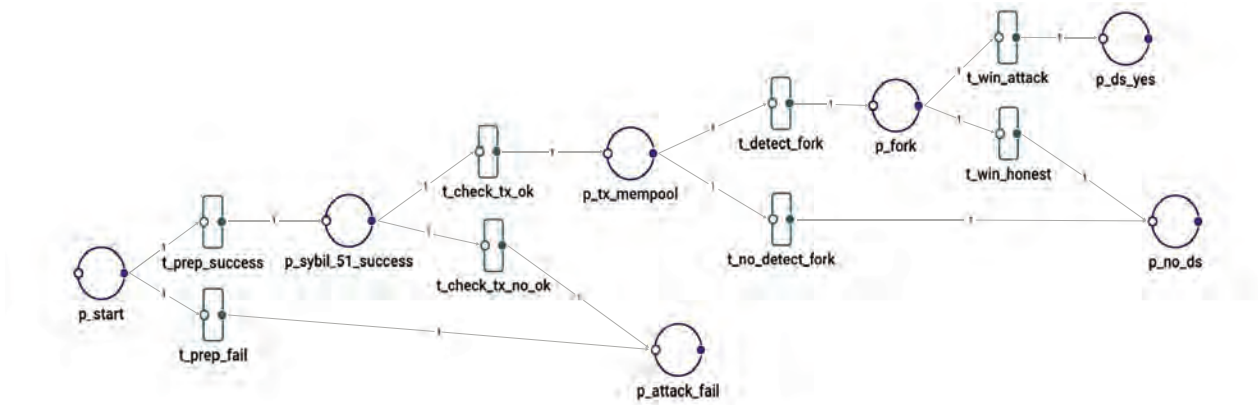


Рис. 2. Сеть Петри для сценария двойной траты для блокчейн-платформы с консенсусом PoW

ния  $\epsilon_i$  могут задаваться на основе экспертных оценок, результатов аудита или испытаний системы.

При наличии задержки вывода вводится коэффициент:

$$\eta_{delay} = \min(1, \max(0, \frac{T_{det}}{T_{pol}^{PoS}}))$$

где  $T_{det}$  — время обнаружения инцидента;

$T_{pol}$  — длительность защитного окна.

Для валидатора PoS дополнительно учитывается период разблокировки стека:

$$T_{pol}^{PoS} = T_{pol} + T_{unbond}.$$

Итоговая вероятность успешного завершения атаки определяется выражением

$$p_{succ} = P_{after-defend} \cdot \eta_{delay}.$$

Для оценки экономических последствий учитывается ограничение максимальной суммы одной транзакции:

$$V_{eff} = \min(V_{attack}, V_{cap}),$$

где  $V_{cap}$  — установленный лимит вывода.

При отсутствии лимита  $V_{eff} = V_{attack}$ . Если при вероятности  $p_{succ}$  злоумышленник провел атаку, то он выведет всю сумму  $V_{eff}$  с вероятностью  $1 - p_{succ}$ , а если нет успешной атаки, то и ущерб равен нулю. Тогда ожидаемый ущерб  $L$  вычисляется так

$$L = p_{succ} \cdot V_{eff} + (1 - p_{succ}) \cdot 0 = p_{succ} \cdot V_{eff}.$$

Таким образом, методика объединяет формальное описание последовательности атаки в сети Петри и вероятностную оценку ее реализации. Для PoW и PoS используется единая логика сценария, а различие между платформами учитывается параметрами модели, включая дополнительный период разблокировки стека для PoS. Формулы являются расчетной частью предлагаемой авторской модели, тогда как использованные источники обосновывают роль криптографических ключей, оценку угроз и необходимость учета постквантового фактора [1—22].

### Методика оценки сценария двойной траты в блокчейн-платформе с консенсусом Proof-of-Work

В блокчейн-платформах с механизмом консенсуса Proof-of-Work (PoW) безопасность распределенного реестра обеспечивается за счет вычислительной слож-

ности формирования блоков и принятия в качестве канонической цепи ветви с наибольшим объемом выполненной работы. Такой принцип лежит в основе механизма защиты от двойного расходования: при условии, что совокупная вычислительная мощность добросовестных участников превышает мощность нарушителя, альтернативная цепь не успевает опередить основную<sup>9</sup>. NIST также относит возможность получения злоумышленником достаточной доли вычислительных ресурсов, известную как атака 51%, к основным угрозам механизмам PoW.

В настоящей работе сценарий двойной траты для PoW рассматривается как последовательность взаимосвязанных этапов:

- атака Сивиллы;
- получение необходимой доли вычислительных ресурсов;
- атака 51%;
- формирование конфликтующей транзакции;
- возникновение конкурирующих цепей;
- разрешение форка;
- двойная трата.

Сеть Петри (Рис. 2) позволяет представить указанный сценарий как последовательность состояний и событий, при которой переход к следующему этапу осуществляется только при выполнении заданного условия.

На первом этапе определяется возможность реализации атаки Сивиллы. Максимальное число узлов, которое нарушитель способен создать с учетом имеющихся вычислительных ресурсов, определяется выражением:

$$N_{tech} = N_{phys} \cdot V_{per-phys}$$

где  $N_{phys}$  — количество физических серверов нарушителя,  $V_{per-phys}$  — количество виртуальных узлов на одном сервере.

После учета ограничений сети определяется фактическое количество узлов атакующего  $N_{att}$ . В модели учитываются ограничения по IP-адресам и доверенным организационным сущностям.

Доля узлов, контролируемых нарушителем, определяется как

<sup>9</sup> Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

$$P_{sybil} = \frac{N_{att}}{N_{total} + N_{att}}$$

где  $N_{total}$  — количество добросовестных узлов сети.

Атака Сивиллы считается успешной при выполнении условия

$$P_{sybil} \geq T_{sybil}$$

где  $T_{sybil}$  — установленный порог успешности атаки.

При этом даже при недостижении основного порога может быть разрешен переход к следующему этапу, если доля ресурсов нарушителя превышает минимальный порог продолжения сценария.

На втором этапе определяется доля вычислительной мощности, контролируемой нарушителем. С учетом коэффициента квантового ускорения  $K$  базовая мощность условной единицы сети рассчитывается следующим образом:

$$H_{base} = \frac{H_{net}}{m+n \cdot K}$$

где  $H_{net}$  — суммарный хешрейт сети,

$m$  — количество добросовестных узлов,

$n = N_{att}$  — количество узлов нарушителя.

Вычислительная мощность одного узла атакующего составляет  $H_{att} = K \cdot H_{base}$ , а его суммарная доля вычислительных ресурсов определяется выражением

$$D_{att} = \frac{n \cdot H_{att}}{H_{net}} \cdot 100\%$$

В рамках модели условие атаки 51% выполняется при  $D_{att} \geq 51\%$ . Достижение данного значения рассматривается как условие, при котором нарушитель получает возможность формировать альтернативную цепь с достаточной вычислительной мощностью для последующей реорганизации истории транзакций

На следующем этапе моделируется двойная трата. Нарушитель формирует конфликтующую транзакцию, которая направляется получателю, одновременно создавая альтернативную ветвь цепи. Количество подтверждений  $z$ , полученных основной транзакцией, используется в качестве параметра, характеризующего глубину ее нахождения в цепи. Вероятность создания следующего блока нарушителем определяется как

$$q = \frac{D_{att}}{100}, p = 1 - q,$$

где  $p$  — вероятность формирования блока добросовестными участниками.

Для  $q < 0,5$  вероятность того, что атакующий сможет догнать добросовестную цепь после  $z$  подтверждений, определяется по вероятностной модели Накамото:

$$\lambda = z \cdot \frac{q}{p}, P_{nak} = 1 - \sum_{k=0}^z (e^{-\lambda} \cdot \frac{\lambda^k}{k!}) (1 - (\frac{q}{p})^{z-k}).$$

При  $q = 0$  вероятность успеха принимается равной нулю, а при  $q \geq 0,5$  — единице в соответствии с принятой моделью гонки цепей.

Дополнительно учитывается ограничение на максимальную последовательность блоков, которую способен сформировать атакующий:  $L_{req} = z + 1$ .

Если  $L_{req} > L_{max}$ , сценарий считается технически блокируемым.

Также в модели учитывается вероятность обнаружения конфликтующей транзакции в мемпуле. При включенной проверке коэффициент прохождения данного защитного механизма определяется как

$$f_{mempool} = 1 - \frac{S_{detect}}{100}$$

где  $S_{detect}$  — вероятность обнаружения конфликтующей транзакции.

Итоговая вероятность успешной двойной траты определяется как

$$P_{final} = \min(1, P_{after-sequence} \cdot f_{mempool}).$$

Ожидаемый ущерб рассчитывается как:

$$E_{damage} = V_{tx} \cdot P_{final}$$

где  $V_{tx}$  — стоимость конфликтующей транзакции.

Данная величина позволяет перейти от оценки вероятности реализации атаки к количественной оценке ее последствий.

Таким образом, разработанная методика позволяет оценить устойчивость PoW-блокчейна с учетом последовательного характера атаки, вычислительных ресурсов нарушителя, квантового ускорения, количества подтверждений и механизмов обнаружения двойного расходования. Формализация сценария сетью Петри обеспечивает связь между расчетными вероятностными показателями и дискретными состояниями развития атаки, что позволяет получить итоговую оценку вероятности успешной двойной траты и ожидаемого ущерба.

### Методика оценки сценария двойной траты в блокчейн-платформе с консенсусом Proof-of-Stake

В блокчейн-платформах с механизмом консенсуса Proof-of-Stake (PoS) возможность влияния нарушителя на процесс формирования и подтверждения блоков определяется не вычислительной мощностью, как в Proof-of-Work, а величиной контролируемого им стеика. Поэтому после реализации общего для рассматриваемых сценариев этапа атаки Сивиллы, описанного в прошлом разделе, основное внимание уделяется оценке доли стеика, находящейся под контролем нарушителя.

В рамках рассматриваемой модели (Рис. 3) этап атаки Сивиллы для PoS не рассматривается повторно, поскольку алгоритм формирования подконтрольных узлов и оценки их количества является общим для сценариев PoW\_2 и PoS\_2. Отличие возникает на следующем этапе, когда определяется ресурс, позволяющий нарушителю влиять на механизм консенсуса. Для PoW таким ресурсом является вычислительная мощность, тогда как для PoS — контролируемая доля стеика [21].

Совокупная доля стеика валидаторов, контролируемых нарушителем, определяется выражением

$$D_{stake} = \frac{S_{total}}{S_{att}} 100\%$$

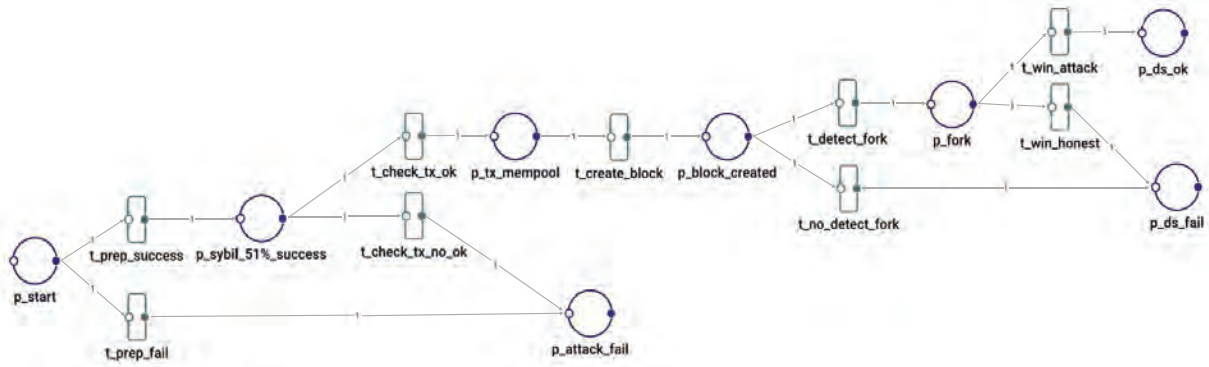


Рис. 3. Сеть Петри для сценария двойной траты для блокчейн-платформы с консенсусом Proof-of-Stake

где  $S_{att}$  — совокупный стейк валидаторов, контролируемых нарушителем,

$S_{total}$  — общий объем стейка сети.

Условием перехода к этапу формирования альтернативной ветви является достижение установленного порога

$$D_{stake} \geq T_{stake},$$

где  $T_{stake}$  — критическая доля стейка, необходимая для реализации рассматриваемого сценария.

Таким образом, общая структура атаки Сивиллы сохраняется для обоих механизмов консенсуса, однако критерий получения контроля над процессом подтверждения транзакций различается: в PoW оценивается доля вычислительных ресурсов нарушителя, а в PoS — доля контролируемого стейка [1, 21, 22]. После получения необходимой доли стейка нарушитель формирует конфликтующую транзакцию и начинает построение альтернативной ветви блокчейна. При этом вероятность успешного формирования и подтверждения альтернативной цепочки зависит от доли голосующей силы, контролируемой атакующим. В модели вводится величина  $q = \frac{D_{stake}}{100}$ , характеризующая долю ресурса, доступного нарушителю. Оставшаяся доля  $p = 1 - q$  соответствует добросовестным валидаторам.

При  $q < 0,5$  вероятность успешного формирования альтернативной цепочки уменьшается с увеличением количества подтверждений исходной транзакции. В качестве базовой модели вероятности догоняющей цепи используется вероятностный подход Накамото, адаптированный для рассматриваемого механизма консенсуса:

$$\lambda = z \cdot \frac{q}{p}, P_{nak} = 1 - \sum_{k=0}^z (e^{-\lambda} \cdot \frac{\lambda^k}{k!}) (1 - (\frac{q}{p})^{z-k}).$$

В PoS дополнительно учитывается временной фактор, связанный с периодом разблокировки стейка. При наличии механизма unbonding нарушение может быть обнаружено до момента, когда контролируемый стейк станет доступен для вывода. Поэтому эффективное защитное окно определяется выражением

$$T_{pol}^{PoS} = T_{pol} + T_{unbound},$$

где  $T_{pol}$  — базовая задержка операции,

$T_{unbond}$  — период разблокировки стейка.

Увеличение данного интервала повышает продолжительность периода, в течение которого может быть обнаружена подозрительная активность и применены защитные меры. Вероятность прохождения временно-го защитного механизма определяется как

$$\eta_{delay} = \min(1, \max(0, \frac{T_{det}}{T_{pol}^{PoS}})),$$

где  $T_{det}$  — время обнаружения атаки.

Итоговая вероятность успешной двойной траты определяется с учетом вероятности формирования альтернативной цепочки и эффективности временного механизма защиты

$$P_{final} = P_{nak} \cdot \eta_{delay}.$$

При наличии дополнительных механизмов защиты итоговая вероятность может быть скорректирована с учетом соответствующих коэффициентов их эффективности. Как и для PoW, окончательная оценка сценария включает потенциальный экономический ущерб:

$$E_{damage} = V_{tx} \cdot P_{final}$$

где  $V_{tx}$  — стоимость конфликтующей транзакции.

Таким образом, разработанная методика позволяет оценить вероятность успешной двойной траты в PoS-блокчейне с учетом количества контролируемых валидаторов, доли принадлежащего им стейка, количества подтверждений, временных механизмов защиты и потенциального ущерба. В отличие от рассмотренного ранее сценария PoW, в котором ключевым ресурсом является вычислительная мощность, для PoS определяющим параметром является доля стейка, находящаяся под контролем нарушителя. Это позволяет применять единую общую структуру сети Петри для анализа обоих механизмов консенсуса при различии количественных параметров соответствующих переходов.

## Результаты и сравнительный анализ

Для оценки разработанной методики проведен вычислительный эксперимент по рассмотренным сценариям компрометации ключей и двойной траты в блокчейн-платформах с механизмами консенсуса Proof-of-Work и Proof-of-Stake. В качестве основных показателей использовались вероятность успешной реализации атаки и ожидаемый ущерб.



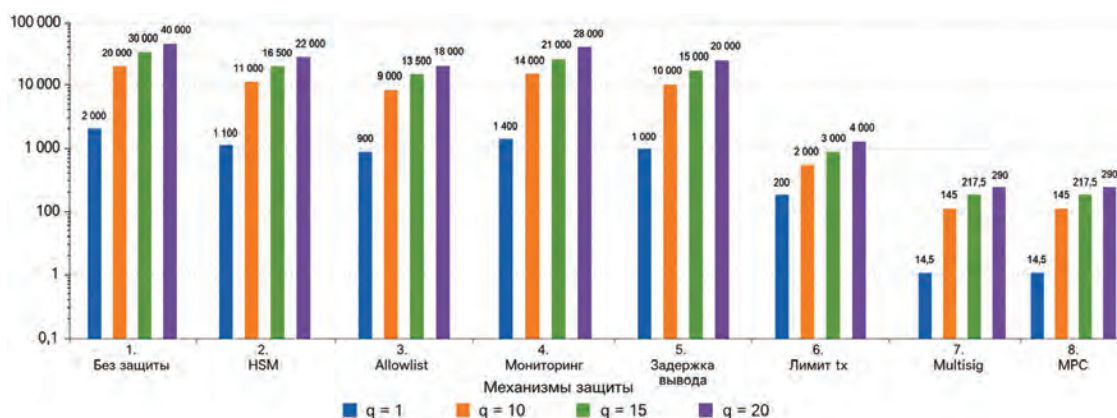


Рис. 4. Зависимость ожидаемого ущерба от квантового ускорения при различных механизмах защиты

Результаты моделирования сценария компрометации ключей показывают, что увеличение коэффициента квантового ускорения  $K$  приводит к росту вероятности успешной атаки и, соответственно, ожидаемого ущерба (Рис. 4).

Наиболее существенное снижение риска достигается при использовании пороговых схем подписи Multisig и MPC, поскольку для завершения атаки требуется компрометация нескольких участников. Дополнительное снижение потенциальных потерь обеспечивается ограничением суммы одной транзакции. Для PoS важным фактором также является период разблокировки стейка, увеличивающий время, доступное для обнаружения и блокирования подозрительной операции.

При анализе сценария двойной траты в PoW установлено, что увеличение доли вычислительных ресурсов, контролируемых нарушителем, сопровождается ростом вероятности успешного формирования альтернативной цепи и ожидаемого ущерба (Рис. 5).

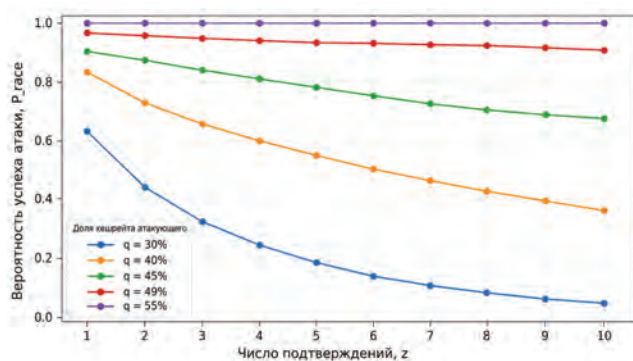


Рис. 5. Зависимость вероятности успешной двойной траты от числа подтверждений в PoW

При относительно небольшой доле ресурсов увеличение числа подтверждений  $z$  существенно снижает вероятность атаки.

Однако при приближении доли ресурсов нарушителя к критической области влияние количества подтверждений уменьшается. Таким образом, одного по-

рогового значения 51% недостаточно для комплексной оценки устойчивости: необходимо учитывать вероятность выигрыша гонки цепей и эффективность механизмов обнаружения конфликта.

Аналогичная закономерность наблюдается для PoS, однако определяющим ресурсом выступает доля стейка, контролируемая нарушителем (Рис. 6).

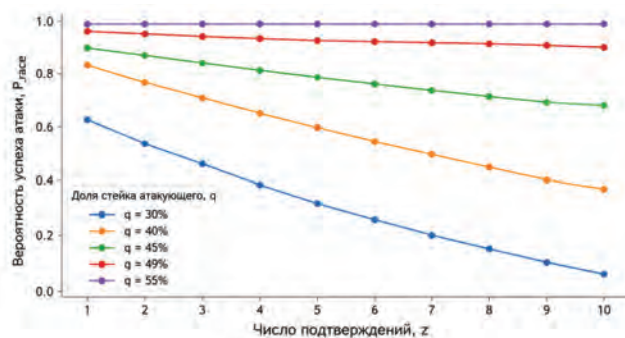


Рис. 6. Зависимость вероятности успешной двойной траты от числа подтверждений в PoS

При ее увеличении ожидаемый ущерб возрастает и в критической области достигает высокого уровня. Механизм slashing в рассматриваемой модели влияет прежде всего на экономическую привлекательность атаки и не уменьшает непосредственно размер уже возникшего ущерба. Более существенное влияние на вероятность успешного завершения сценария оказывают механизмы обнаружения конфликтующих транзакций и временные ограничения.

Сравнение результатов показывает, что для PoW и PoS характерна общая зависимость: чем выше доля ресурса, контролируемого нарушителем, тем выше вероятность успешной атаки и потенциальный ущерб. Различие заключается в природе данного ресурса: для PoW им является вычислительная мощность, для PoS — контролируемый стейк. В обоих случаях увеличение числа подтверждений эффективно преимущественно при относительно небольшом влиянии атакующего.



Таким образом, результаты эксперимента подтверждают, что оценка квантовой устойчивости блокчейн-платформ не должна ограничиваться проверкой достижения одного порогового значения. Более информативным является комплексный анализ последовательности развития атаки, вероятности прохождения отдельных этапов, механизмов защиты и потенциального ущерба. Предложенная методика позволяет проводить такую оценку в единой формальной модели на основе сетей Петри и сопоставлять устойчивость платформ с различными механизмами консенсуса.

### **Выводы**

В работе предложена методика оценки квантовой устойчивости блокчейн-платформ на основе математического аппарата сетей Петри. Методика позволяет формализовать последовательность развития квантовых атак, учитывать особенности механизмов консенсуса Proof-of-Work и Proof-of-Stake и получать количественные оценки вероятности успешной реализации атаки и ожидаемого ущерба.

В рамках исследования сформированы модели четырех сценариев квантовых угроз: компрометации криптографических ключей в PoW и PoS, а также двойной траты в блокчейн-платформах с соответствующими механизмами консенсуса. Для каждого сценария определены состояния, события и условия переходов, отражающие последовательность реализации атаки.

Для сценариев компрометации ключей разработанная методика позволяет учитывать длину ключа, срок его действия, квантовое ускорение, используемый механизм подписи и применяемые средства защиты. Для сценариев двойной траты учитываются доля контролируемых нарушителем ресурсов, количество подтверждений транзакции, вероятность обнаружения

конфликта и дополнительные ограничения, влияющие на возможность завершения атаки.

Проведенные вычислительные эксперименты показали, что увеличение контролируемого атакующим ресурса приводит к росту вероятности успешной реализации двойной траты и ожидаемого ущерба. При этом увеличение числа подтверждений эффективно преимущественно при относительно небольшой доле ресурсов нарушителя; при приближении к критической области защитный эффект данного механизма снижается. Для PoW определяющим ресурсом выступает вычислительная мощность, тогда как для PoS — контролируемая доля стейка.

Установлено также, что применение отдельных механизмов защиты воздействует на различные характеристики риска. Пороговые схемы подписи и ограничения суммы транзакции снижают вероятность или потенциальный размер ущерба при компрометации ключей, тогда как механизмы обнаружения конфликтующих транзакций непосредственно ограничивают вероятность успешного завершения сценария двойной траты. В PoS механизм slashing дополнительно формирует экономические последствия для нарушителя, однако не исключает непосредственно возникновение ущерба от состоявшейся атаки.

Таким образом, результаты исследования подтверждают целесообразность сценарного подхода к оценке квантовой устойчивости блокчейн-платформ, при котором учитывается не отдельный пороговый показатель, а совокупность последовательных событий, параметров механизма консенсуса, криптографических характеристик, защитных механизмов и потенциальных последствий атаки. Разработанная методика может использоваться для сравнительного анализа различных конфигураций блокчейн-платформ и выбора мер, направленных на повышение их устойчивости к квантовым угрозам.

*Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение от 27.09.2024 г. № 23—03).*

### **Литература**

1. Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Vol. 18, № 2. P. 56—73. DOI: 10.18721/JCSTCS.18205. EDN: DCDMZF.
2. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3(49). С. 2—22. DOI 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.
3. Ларина М.В., Скиба В.Ю. О классификации угроз информационных систем в условиях развития квантовых технологий // Правовая информатика. 2026. № 1. С. 5—15. DOI: 10.24412/1994-1404-2026-1-00-01. EDN: XMQASS.
4. Ларина М.В., Скиба В.Ю. Уточнение классификации информационных систем и угроз в условиях развития квантовых технологий // Экономика устойчивого развития региона: инновации, финансовые аспекты, технологические драйверы развития в сфере туризма и гостеприимства : материалы XII межд. науч.-практ. конф.,

- посвященной празднованию 80-летия победы, Ялта, 26—29 марта 2025 г. Симферополь : ООО «Типография «Ариал», 2025. С. 182—184. EDN: CDFVGN.
5. Ларина М.В., Скиба В.Ю. Модель цифровой платформы для анализа устойчивости к квантовым угрозам // Правовая информатика. 2025. № 3. С. 12—26. DOI: 10.24412/1994-1404-2025-3-00-02. EDN: NDONZQ.
  6. Ищукова Е.А. О влиянии криптографической стойкости функций хеширования на устойчивость современных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 3 (67). С. 63—71. DOI: 10.21681/2311-3456-2025-3-63-71. EDN: UUSWXP.
  7. Sahu S.K., Mazumdar K. State-of-the-art analysis of quantum cryptography: applications and future prospects // Frontiers in Physics. 2024. Vol. 12. Art. 1456491. DOI: 10.3389/fphy.2024.1456491.
  8. Петренко С.А., Балябин А.А. Модель квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 1 (65). С. 7—17. DOI: 10.21681/2311-3456-2025-1-7-17. EDN: YYRSOI.
  9. Абдуллин Р.Р., Егоров Д.А., Крупенина Н.В., Рудь В.Ю., Сапожникова Ю.Д. Исследование безопасности квантовых вычислений классическими алгоритмами шифрования // Информационные процессы. 2025. Т. 25, № 3.1. С. 559—572. DOI: 10.53921/18195822\_2025\_25\_3.1\_559. EDN: HYZMFC.
  10. Балябин А.А., Петренко С.А. Модель блокчейн-платформы с кибериммунитетом в условиях квантовых атак // Вопросы кибербезопасности. 2025. № 3 (67). С. 72—82. DOI: 10.21681/2311-3456-2025-3-72-82. EDN: YEVGTS.
  11. Балябин А.А., Петренко С.А. Методика синтеза квантово-устойчивых блокчейн-платформ с кибериммунитетом // Вопросы кибербезопасности. 2025. № 4 (68). С. 46—54. DOI: 10.21681/2311-3456-2025-4-46-54. EDN: CEPHDA.
  12. Ищукова Е.А., Балябин А.А., Петренко С.А. Математическая модель киберустойчивой информационной системы на основе блокчейн-платформы // Вопросы кибербезопасности. 2026. № 3 (73). С. 92—100. DOI: 10.21681/2311-3456-2026-3-92-100. EDN: OWTROC.
  13. Ищукова Е.А., Петренко С.А., Леонтьева Ю.П. Уязвимости асимметричных шифров блокчейн-платформ // Вопросы кибербезопасности. 2025. № 6(70). С. 35—47. DOI: 10.21681/2311-3456-2025-6-35-47. EDN: HUXBQW.
  14. Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Вопросы кибербезопасности. 2023. № 1 (53). С. 100—115. DOI: 10.21681/2311-3456-2023-1-100-115. EDN: COMUIK.
  15. Петренко А.С. Метод построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2025. № 2 (66). С. 52—63. DOI: 10.21681/2311-3456-2025-2-52-63. EDN: RHCWAK.
  16. Петренко А.С. Подход к оптимизации устойчивости национальных блокчейн-платформ и экосистем с помощью квантово-вдохновлённых алгоритмов. Часть 1 // Вопросы кибербезопасности. 2026. № 2 (72). С. 101—111. DOI: 10.21681/2311-3456-2026-2-101-111. EDN: FFBYJF.
  17. Петренко А.С. Подход к оптимизации устойчивости национальных блокчейн-платформ и экосистем с помощью квантово-вдохновлённых алгоритмов. Часть 2 // Вопросы кибербезопасности. 2026. № 3 (73). С. 82—91. DOI: 10.21681/2311-3456-2026-3-82-91. EDN: KWDDJV.
  18. Сундеев П.В. Кластерная модель защиты распределенного реестра // Вопросы кибербезопасности. 2025. № 4 (68). С. 2—8. DOI: 10.21681/2311-3456-2025-4-2-8. EDN: RAXVGN.
  19. Сундеев П.В. Метод оценки выполнения нормативных требований к защите информации // Правовая информатика. 2025. № 4. С. 4—15. DOI: 10.24412/1994-1404-2025-4-4-15. EDN: DSWFHY.
  20. Сундеев П.В. Функциональная устойчивость распределенного реестра в условиях появления новой квантовой угрозы // Вопросы кибербезопасности. 2025. № 3 (67). С. 83—89. DOI: 10.21681/2311-3456-2025-3-83-89. EDN: MIYFUK.
  21. Saleh F. Blockchain without Waste: Proof-of-Stake // The Review of Financial Studies. 2021. Vol. 34. No. 3. P. 1156—1190. DOI: 10.1093/rfs/hhaa075.
  22. Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems // Journal of Information Security and Applications. 2021. Vol. 58. P. 102717. DOI: 10.1016/j.jisa.2020.102717. EDN: EFXKUB.

# METHODOLOGY FOR ASSESSING THE QUANTUM RESILIENCE OF BLOCKCHAIN PLATFORMS BASED ON PETRI NETS

Larina M.V.<sup>10</sup>, Skiba V.Yu.<sup>11</sup>

**Keywords:** quantum threats, consensus, critical information infrastructure, risk assessment, post-quantum cryptography, attack formalization, digital platforms, Proof-of-Stake, Proof-of-Work.

## Abstract

**Purpose of work** is to develop a methodology for assessing the quantum resilience of blockchain platforms based on the mathematical apparatus of Petri nets, designed to model quantum attack scenarios and identify critical states in the operation of a distributed system.

**Research methods:** analysis of the resilience of Proof-of-Work and Proof-of-Stake consensus mechanisms, formalization of attacks and disruption scenarios using Petri nets, and assessment of the impact of cryptographic, network, and computational parameters on the probability of successful threat realization.

**Results of the study:** the paper proposes a model that accounts for the relationships between system states, transition parameters, and the probabilities of successful attacks. Based on this approach, a software system was developed for modeling and comparative analysis of security scenarios for blockchain platforms.

**Scientific novelty:** the proposed methodology for assessing the quantum resilience of blockchain platforms integrates cryptographic, computational, and network parameters within a unified model, together with a scenario-based analysis of the resilience of Proof-of-Work and Proof-of-Stake consensus mechanisms. Formalization in terms of Petri nets links the logical sequence of attack stages with quantitative conditions for their execution, making it possible to identify critical system states, assess the probability of successful attacks, and account for the relationship between cryptographic mechanisms and network structure.

**Practical significance:** the proposed methodology can be used in the design of quantum-resilient blockchain ecosystems and protection systems for critical information infrastructure.

## References

1. Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Vol. 18. No. 2. P. 56—73. DOI: 10.18721/JCSTCS.18205. EDN: DCDMZF.
2. Petrenko A.S., Petrenko S.A. Metod otsenivaniya kvantovoy ustoychivosti blokcheyn-platform // Voprosy kiberbezopasnosti. 2022. No. 3(49). P. 2—22. DOI: 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.
3. Larina M.V., Skiba V.Yu. O klassifikatsii ugroz informatsionnykh sistem v usloviyakh razvitiya kvantovykh tekhnologiy // Pravovaya informatika. 2026. No. 1. P. 5—15. DOI: 10.24412/1994-1404-2026-1-00-01. EDN: XMQASS.
4. Larina M.V., Skiba V.Yu. Utochnenie klassifikatsii informatsionnykh sistem i ugroz v usloviyakh razvitiya kvantovykh tekhnologiy // Ekonomika ustoychivogo razvitiya regiona: innovatsii, finansovye aspekty, tekhnologicheskie drayvery razvitiya v sfere turizma i gostepriimstva: materialy XII mezhd. nauch.-prakt. konf., posvyashchennoy prazdnovaniyu 80-letiya pobedy, Yalta, 26—29 marta 2025 goda. Simferopol: OOO «Tipografiya “Arial”», 2025. P. 182—184. EDN: CDFVGN.

<sup>10</sup> **Maria V. Larina**, research technician of Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sirius, Krasnodar region, Russian Federation. ORCID: 0009-0009-7826-0180.

E-mail: [larina.mv@talantiuspeh.ru](mailto:larina.mv@talantiuspeh.ru)

<sup>11</sup> **Vladimir Yu. Skiba**, Doctor of Technical Sciences, Senior Researcher, Chief Research Engineer at the Scientific Center for Information Technology and Artificial Intelligence, Sirius Scientific and Technological University, Sirius, Krasnodar region, Russian Federation, Professor of the IBM-6 Department, Federal State Autonomous Educational Institution of Higher Education «Bauman Moscow State Technical University», Moscow, Russian Federation, Professor of Department № 2 «Automation», National Research Nuclear University MEPhI, Moscow, Russian Federation. ORCID: 0000-0002-9805-7800.

E-mail: [skiba.vy@talantiuspeh.ru](mailto:skiba.vy@talantiuspeh.ru)

5. Larina M.V., Skiba V.Yu. Model tsifrovoy platformy dlya analiza ustoychivosti k kvantovym ugrozam // Pravovaya informatika. 2025. No. 3. P. 12—26. DOI: 10.24412/1994-1404-2025-3-00-02. EDN: NDONZQ.
6. Ishchukova E.A. O vliyaniy kriptograficheskoy stoykosti funktsiy kheshirovaniya na ustoychivost sovremennykh blokcheyn-ekosistem i platform // Voprosy kiberbezopasnosti. 2025. No. 3 (67). P. 63—71. DOI: 10.21681/2311-3456-2025-3-63-71. EDN: UUSWXP.
7. Sahu S.K., Mazumdar K. State-of-the-art analysis of quantum cryptography: applications and future prospects // Frontiers in Physics. 2024. Vol. 12. Art. 1456491. DOI: 10.3389/fphy.2024.1456491.
8. Petrenko S.A., Balyabin A.A. Model kvantovykh ugroz bezopasnosti informatsii dlya natsionalnykh blokcheyn-ekosistem i platform // Voprosy kiberbezopasnosti. 2025. No. 1 (65). P. 7—17. DOI: 10.21681/2311-3456-2025-1-7-17. EDN: YYRSOI.
9. Abdullin R.R., Egorov D.A., Krupenina N.V., Rud V.Yu., Sapozhnikova Yu.D. Issledovanie bezopasnosti kvantovykh vychisleniy klassicheskimi algoritmami shifrovaniya // Informatsionnye protsessy. 2025. Vol. 25. No. 3.1. P. 559—572. DOI: 10.53921/18195822\_2025\_25\_3.1\_559. EDN: HYZMFC.
10. Balyabin A.A., Petrenko S.A. Model blokcheyn-platformy s kiberimmunitetom v usloviyakh kvantovykh atak // Voprosy kiberbezopasnosti. 2025. No. 3 (67). P. 72—82. DOI: 10.21681/2311-3456-2025-3-72-82. EDN: YEVGTS.
11. Balyabin A.A., Petrenko S.A. Metodika sinteza kvantovo-ustoychivyykh blokcheyn-platform s kiberimmunitetom // Voprosy kiberbezopasnosti. 2025. No. 4 (68). P. 46—54. DOI: 10.21681/2311-3456-2025-4-46-54. EDN: CEPHDA.
12. Ishchukova E.A., Balyabin A.A., Petrenko S.A. Matematicheskaya model kiberustoychivoy informatsionnoy sistemy na osnove blokcheyn-platformy // Voprosy kiberbezopasnosti. 2026. No. 3 (73). P. 92—100. DOI: 10.21681/2311-3456-2026-3-92-100. EDN: OWTROC.
13. Ishchukova E.A., Petrenko S.A., Leonteva Yu.P. Uyazvimosti asimmetrichnykh shifrov blokcheyn-platform // Voprosy kiberbezopasnosti. 2025. No. 6 (70). P. 35—47. DOI: 10.21681/2311-3456-2025-6-35-47. EDN: HUXBQW.
14. Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Voprosy kiberbezopasnosti. 2023. No. 1 (53). P. 100—115. DOI: 10.21681/2311-3456-2023-1-100-115. EDN: COMUIK.
15. Petrenko A.S. Metod postroeniya postkvantovykh algoritmov ETsP s dvumya skrytymi gruppami // Voprosy kiberbezopasnosti. 2025. No. 2 (66). P. 52—63. DOI: 10.21681/2311-3456-2025-2-52-63. EDN: RHCWAK.
16. Petrenko A.S. Podkhod k optimizatsii ustoychivosti natsionalnykh blokcheyn-platform i ekosistem s pomoshchyu kvantovo-vdokhnovlennykh algoritmov. Chast 1 // Voprosy kiberbezopasnosti. 2026. No. 2 (72). P. 101—111. DOI: 10.21681/2311-3456-2026-2-101-111. EDN: FFYJF.
17. Petrenko A.S. Podkhod k optimizatsii ustoychivosti natsionalnykh blokcheyn-platform i ekosistem s pomoshchyu kvantovo-vdokhnovlennykh algoritmov. Chast 1 // Voprosy kiberbezopasnosti. 2026. No. 3 (73). P. 82—91. DOI: 10.21681/2311-3456-2026-3-82-91. EDN: KWDDJV.
18. Sundeev P.V. Klasternaya model zashchity raspredelennogo reestra // Voprosy kiberbezopasnosti. 2025. No. 4 (68). P. 2—8. DOI: 10.21681/2311-3456-2025-4-2-8. EDN: RAXVGN.
19. Sundeev P.V. Metod otsenki vypolneniya normativnykh trebovaniy k zashchite informatsii // Pravovaya informatika. 2025. No. 4. P. 4—15. DOI: 10.24412/1994-1404-2025-4-4-15. EDN: DSWFHY.
20. Sundeev P.V. Funktsionalnaya ustoychivost raspredelennogo reestra v usloviyakh poyavleniya novoy kvantovoy ugrozy // Voprosy kiberbezopasnosti. 2025. No. 3 (67). P. 83—89. DOI: 10.21681/2311-3456-2025-3-83-89. EDN: MIYFUK.
21. Saleh F. Blockchain without Waste: Proof-of-Stake // The Review of Financial Studies. 2021. Vol. 34. No. 3. P. 1156—1190. DOI: 10.1093/rfs/hhaa075.
22. Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems // Journal of Information Security and Applications. 2021. Vol. 58. P. 102717. DOI: 10.1016/j.jisa.2020.102717. EDN: EFXKUB.





# МЕТОД ИНТЕРПРЕТАЦИОННОГО ДИАГНОСТИРОВАНИЯ СОСТОЯНИЯ ЭЛЕМЕНТОВ БЛОКЧЕЙН-СИСТЕМ ПО РЕШЕНИЯМ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ

Лисов Д.Н.<sup>1</sup>, Гнидко К.О.<sup>2</sup>

**Ключевые слова:** объяснимый искусственный интеллект, оценка качества объяснения, локальное объяснение, статистическое обучение, диагностические правила, диагностический профиль, калибровка порогов, подозрительное состояние, угрозы нового типа.

## Аннотация

**Цель работы:** разработать метод интерпретационного диагностирования состояния элементов блокчейн-систем по решениям моделей машинного обучения при появлении угроз нового типа.

**Методы исследования:** различия между правильными и ошибочными решениями ML-модели исследовались по показателям локального объяснения. Эти показатели характеризовали изменение выхода модели при контролируемой замене входных признаков, структуру атрибуций и согласованность результатов нескольких объяснителей. Полученные диагностические профили использовались для построения правил методами статистического обучения. Пороговые границы определялись в соответствии со статистической теорией принятия решений при ограничении доли корректных прогнозов, направляемых на дополнительную проверку. Различимость правильных и ошибочных решений оценивалась по AUC на независимых данных. Практический результат характеризовался изменением охвата ранее не наблюдавшейся вредоносной активности, концентрацией пропущенных угроз в подозрительной области и объемом дополнительной проверки.

**Результаты исследования:** разработан метод, дополняющий бинарный прогноз ML-модели диагностическим состоянием, формируемым по характеристикам локального объяснения без изменения исходного классификатора. Научная новизна состоит в построении отдельных диагностических правил для положительной и отрицательной ветвей прогноза и в независимой калибровке их порогов с учётом допустимой доли корректных решений, направляемых на дополнительную проверку. Экспериментальное исследование на сетевых данных и различных представлениях смарт-контрактов показало, что сформированные правила различают правильные и ошибочные решения при разных XAI-конфигурациях. В сценариях появления вредоносной активности, не использованной при обучении ML-модели и построении диагностических правил, часть пропущенных объектов была переведена в подозрительное состояние. Одновременно определялся возникающий объем дополнительной проверки. Результаты подтвердили диагностическую информативность показателей локального объяснения и показали её зависимость от данных, ML-модели и XAI-конфигурации. Универсально предпочтительная XAI-конфигурация не установлена.

DOI: 10.24412/1994-1404-2026-3-29-40

## Введение и постановка задачи

В исследованиях цифровых и облачных платформ выявление деструктивных воздействий и учёт новых типов угроз рассматриваются как условия устойчивого функционирования защищаемых систем [1, 2]. При включении ML-моделей в процедуры защиты возникает проблема объяснимости получае-

мых решений, поскольку достоверность автоматизированного контроля зависит не только от предсказанного класса, но и от возможности установить признаки, повлиявшие на результат [3]. Для решения этой проблемы вместе с моделями машинного обучения применяются средства объяснимого искусственного интеллекта.

<sup>1</sup> Лисов Дмитрий Николаевич, аспирант, младший научный сотрудник центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус»», пгт Сириус, Краснодарский край, Российская Федерация. ORCID: 0000-0002-8214-4109.

E-mail: lisov.dn@talantiuspeh.ru

<sup>2</sup> Гнидко Константин Олегович, доктор технических наук, доцент, заместитель руководителя группы Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус»», пгт Сириус, Краснодарский край, Российская Федерация. ORCID: 0000-0002-8605-8865.

E-mail: gnidko.ko@talantiuspeh.ru

При анализе транзакций блокчейна они позволяют определить признаки, обусловившие отнесение операции к аномальным [4]. В системах обнаружения сетевых атак локальные объяснения используются для анализа решений классификаторов, в том числе при исследовании активности, отличающейся от представленной в обучающих данных [5—7]. В этих работах ML-модель устанавливает класс объекта, после чего ХАИ раскрывает влияние входных признаков на уже полученный прогноз. Такой подход повышает прозрачность классификации, однако объяснение не участвует в определении состояния объекта.

Более тесное включение ХАИ в защитный контур предложено в работах [8, 9]. В первом случае значения атрибуций передаются дополнительному классификатору, уточняющему результат обнаружения распределённой атаки. Во втором объяснения используются для оценки поведения участников федеративного обучения и ограничения влияния потенциально скомпрометированных узлов. Другой подход основан на наблюдении за изменением распределений объяснений [10, 11]. Он позволяет связать сдвиг входных данных с изменением поведения модели, но характеризует группу поступивших объектов, а не отдельное решение. Таким образом, результаты ХАИ могут использоваться не только для последующего пояснения прогноза. Вместе с тем известные решения либо изменяют исходную схему классификации, либо решают задачу наблюдения на другом уровне и не формируют диагностическое состояние отдельного объекта по характеристикам его локального объяснения.

Возможность такого применения ХАИ связана с развитием методов количественной оценки объяснений [12—14]. Предложенные показатели характеризуют реакцию модели на изменение выделенных признаков, структуру атрибуций и согласованность результатов разных объяснителей. Каждый из них отражает отдельное свойство объяснения, а его информативность зависит от данных, ML-модели и применяемого ХАИ-метода. Поэтому значение одного показателя не может непосредственно рассматриваться как диагностическое состояние. Для совместного использования нескольких характеристик необходимо установить, как их сочетания проявляются в правильных и ошибочных решениях конкретной ML-модели.

В ранее выполненном исследовании [15] разработана интерпретационная модель наблюдения и диагностирования состояния элементов блокчейн-систем. Предусмотренная моделью последовательность связывает прогноз и локальное объяснение с диагностическим профилем, оценкой соответствия и состоянием объекта:

$$\begin{aligned} (\hat{y}_{(B_i)}(t), \text{Expl}_{(B_i)}(t)) &\rightarrow \mathcal{M}_{(B_i)}(t) \rightarrow \\ &\rightarrow \tau_{(B_i)}(t) \rightarrow (\text{Rep}_{(B_i)}(t), \text{ALERT}_{(B_i)}(t)). \end{aligned} \quad (1)$$

В выражении (1) определены состав результатов и порядок их получения, но не установлено правило  $g$ ,

преобразующее диагностический профиль  $\mathcal{M}_{(B_i)}(t)$  в оценку  $\tau_{(B_i)}(t)$ . Не определены также пороговые границы, по которым эта оценка связывается с диагностическим состоянием. Назначить их одинаковыми для разных защищаемых элементов нельзя, поскольку распределения показателей зависят от используемых данных, поведения ML-модели и выбранной ХАИ-конфигурации. Для практической реализации модели требуется способ воспроизводимого формирования правила и его порогов применительно к зафиксированному сочетанию этих компонентов.

Исследование проводится применительно к защищаемому элементу  $B_i$ , на котором используются обученная бинарная ML-модель, зафиксированная предобработка данных и совместимая ХАИ-конфигурация. Для эталонных объектов известны фактические метки и прогнозы модели, поэтому среди них могут быть выделены правильные и ошибочные решения. При поступлении нового объекта доступны его признаки, прогноз ML-модели и локальное объяснение, тогда как фактическое состояние устанавливается позднее. Следовательно, зависимость между характеристиками объяснения и типом решения должна быть выявлена по эталонным данным, после чего полученное правило может применяться к поступающим объектам.

В основу исследования положена гипотеза о том, что для фиксированной ML-модели и выбранной ХАИ-конфигурации совместное распределение показателей локального объяснения различается у правильных и ошибочных решений. Если это различие сохраняется на независимых данных, диагностический профиль может использоваться для выделения решений, требующих дополнительной проверки, в том числе при появлении вредоносной активности, не представленной при обучении модели.

Цель работы состоит в разработке и экспериментальном исследовании метода интерпретационного диагностирования состояния элементов блокчейн-систем по решениям моделей машинного обучения. Метод должен обеспечить формирование диагностического профиля локального объяснения, построение правил для положительной и отрицательной ветвей прогноза и установление порогов, ограничивающих направление корректных решений на дополнительную проверку.

### Принцип построения метода

Проверка сформулированной гипотезы требует сначала установить связь между диагностическим профилем локального объяснения и типом решения ML-модели, а затем использовать найденную зависимость для объектов, фактическое состояние которых в момент обработки неизвестно. Этим обусловлено разделение метода на подготовительный и рабочий этапы. До формирования профилей эталонная выборка разделяется на непересекающиеся части  $D_{fit}$  и  $D_{cal}$ . Первая используется для выявления закономерностей,

характеризующих правильные и ошибочные решения, тогда как вторая предназначена для независимого установления пороговых границ.

Для объектов  $D_{fit}$  их сопоставление позволяет выделить группы TP, FP, TN и FN, которые характеризуют правильные и ошибочные решения положительной и отрицательной ветвей прогноза. Различный смысл ошибок не позволяет описывать их одним правилом. В положительной ветви необходимо установить, насколько объяснение подтверждает прогноз угрозы, а в отрицательной требуется выявить сходство с известными пропусками вредоносной активности. Поэтому по диагностическим профилям объектов  $D_{fit}$  различает TP и FP, а правило  $\mathfrak{D}_0$  различает TN и FN.

Получаемые правила связывают диагностический профиль с числовой оценкой  $\tau$ , но границы диагностических состояний устанавливаются отдельно. Для этого к объектам  $D_{cal}$  применяются сформированные по  $D_{fit}$  профили и правила. В положительной ветви порог  $\theta_{TP}$  разделяет состояния «угроза» и «подозрительное», в отрицательной порог  $\theta_{FN}$  отделяет «важное» состояние от «подозрительного». Параметры  $\alpha_{TP}$  и  $\alpha_{TN}$  ограничивают долю правильных решений соответствующей ветви, которые могут быть направлены на дополнительную проверку. Среди удовлетворяющих этому ограничению порогов выбирается вариант, обеспечивающий наиболее полное выявление ошибочных решений. Результатом подготовительного этапа становятся правила расчёта диагностического профиля, правила  $\mathfrak{D}_1$  и  $\mathfrak{D}_0$ , а также установленные для них пороги.

На рабочем этапе для поступившего объекта  $X_{(B_i)}(t)$  формируются прогноз  $\hat{y}_{(B_i)}(t)$  и локальное объяснение  $Expl_{(B_i)}(t)$ . По объяснению рассчитывается диагностический профиль  $M_{(B_i)}(t)$ , а прогноз определяет выбор правила  $\mathfrak{D}_1$  или  $\mathfrak{D}_0$ . Полученная оценка  $\tau_{(B_i)}(t)$  сопоставляется с порогом соответствующей ветви,

после чего устанавливается диагностическое состояние  $Rep_{(B_i)}(t)$ . На его основе формируются сигнал  $ALERT_{(B_i)}(t)$  и объяснимый отчет  $Report_{(B_i)}(t)$ . Взаимосвязь подготовительного и рабочего этапов представлена на рис. 1.

### Формирование диагностического профиля объяснения

Диагностические правила  $\mathfrak{D}_1$  и  $\mathfrak{D}_0$  должны различать правильные и ошибочные решения по свойствам локального объяснения. Исходные атрибуции для этого недостаточны, поскольку они показывают вклад признаков, но не характеризуют его соответствие реакции ML-модели и известным типам решений. Для формирования такого описания объекты  $D_{fit}$  распределяются по результатам сопоставления фактической метки  $y$  и прогноза  $\hat{y}$ :

$$\begin{aligned} TP &= \{X_{(B_i)} \in D_{fit} : y_{(B_i)} = 1, \hat{y}_{(B_i)} = 1\}, \\ FP &= \{X_{(B_i)} \in D_{fit} : y_{(B_i)} = 0, \hat{y}_{(B_i)} = 1\}, \\ TN &= \{X_{(B_i)} \in D_{fit} : y_{(B_i)} = 0, \hat{y}_{(B_i)} = 0\}, \\ FN &= \{X_{(B_i)} \in D_{fit} : y_{(B_i)} = 1, \hat{y}_{(B_i)} = 0\}. \end{aligned}$$

Группы TP и TN содержат правильные решения положительной и отрицательной ветвей, а FP и FN содержат ошибки этих ветвей. Локальное объяснение объекта, полученное  $r$ -м XAI-методом, представляется вектором атрибуций:

$$\begin{aligned} \varepsilon_r^{(B_i)}(t) &= in_r(X_{(B_i)}(t), \hat{y}_{(B_i)}(t)) = \\ &= \left(a_{1,r}^{(B_i)}(t), a_{2,r}^{(B_i)}(t), \dots, a_{k,r}^{(B_i)}(t)\right), \\ &r = 1, \dots, p, \end{aligned}$$

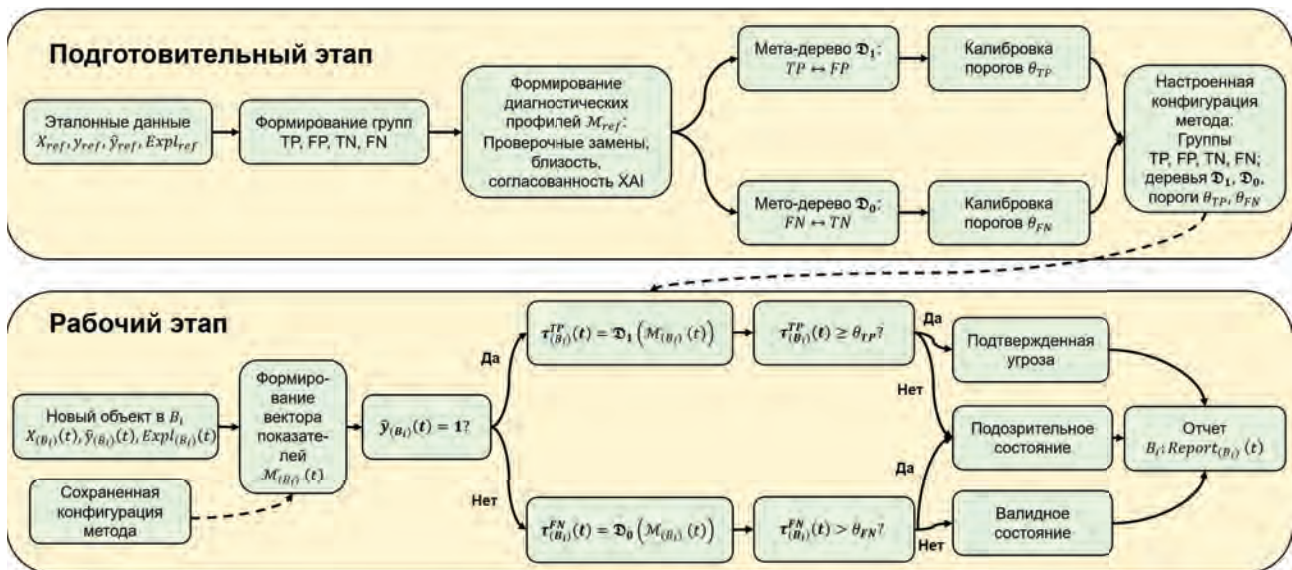


Рис. 1. Общая схема метода интерпретационного диагностирования состояния элемента блокчейн-системы



где  $a$  характеризует направление и величину вклада признака  $x$  в прогноз объекта  $X_{(B_i)}(t)$ ,  $k$  — число входных признаков,  $p$  — число ХАИ-методов в используемой конфигурации. Соответствие атрибуций поведению ML-модели проверяется заменой выбранных признаков значениями ближайших правильных решений той же ветви прогноза. Источником замен служит группа:

$$Cand_{(B_i)}(t) = \begin{cases} TP_{(B_i)}, & \hat{y}_{(B_i)}(t) = 1, \\ TN_{(B_i)}, & \hat{y}_{(B_i)}(t) = 0. \end{cases}$$

После зафиксированной предобработки кандидаты упорядочиваются по расстоянию:

$$d(X_{(B_i)}(t), X_{(B_i),cand}) = \sqrt{\sum_{l=1}^k (x_l - x_{l,cand})^2}. \quad (2)$$

Совпадающий с исследуемым объект исключается. Первые  $R$  кандидатов образуют последовательность локальных замен:

$$X_{(B_i)}^{rep}(t) = \{X_{(B_i),cand_1}, \dots, X_{(B_i),cand_R}\}.$$

Положительные и отрицательные атрибуции отбираются отдельно, чтобы проверить влияние каждого направления на выход модели. Предельное число рассматриваемых признаков определяется выражением:

$$K = \max(k_{min}, [\rho k]),$$

где  $\rho$  — доля анализируемых признаков,  $k_{min}$  — их минимально допустимое число. Множество  $P_r^{(B_i)}(t)$  содержит индексы не более  $K$  положительных атрибуций  $r$ -го объяснителя с наибольшими абсолютными значениями. Множество  $N_r^{(B_i)}(t)$  формируется аналогично среди отрицательных атрибуций.

Для каждого объекта  $X \in X_{(B_i)}^{rep}(t)$  и множества индексов  $Index \in \{P_r^{(B_i)}(t), N_r^{(B_i)}(t)\}$  строятся два проверочных объекта. В первом заменяются признаки, выделенные объяснителем:

$$\begin{aligned} X_j^{(-Index)(B_i)} &= (x_{1,j}^{(-Index)(B_i)}, x_{2,j}^{(-Index)(B_i)}, \dots, \\ &\quad x_{k,j}^{(-Index)(B_i)}), \\ x_{l,j}^{(-Index)(B_i)}(X_{(B_i)}(t)) &= \begin{cases} x_{l,j}^{(B_i),rep}, l \in Index \\ x_l^{(B_i)}, l \notin Index \end{cases}, \end{aligned} \quad (3)$$

Во втором сохраняются выбранные признаки и заменяются остальные:

$$\begin{aligned} X_j^{(+Index)(B_i)} &= (x_{1,j}^{(+Index)(B_i)}, x_{2,j}^{(+Index)(B_i)}, \dots, \\ &\quad x_{k,j}^{(+Index)(B_i)}), \\ x_{l,j}^{(+Index)(B_i)}(X_{(B_i)}(t)) &= \begin{cases} x_{l,j}^{(B_i),rep}, l \notin Index \\ x_l^{(B_i)}, l \in Index \end{cases}. \end{aligned} \quad (4)$$

Первое изменение позволяет проверить, проявляется ли указанное объяснителем влияние в выходе модели. Второе характеризует способность выбранных признаков воспроизвести исходный результат [12, 13]. Если  $z_{B_i}(X_{(B_i)}(t))$  обозначает вероятность положительного класса, реакция модели на замену признаков определяется показателями:

$$E_r^{(+)(B_i)}(X_{(B_i)}(t)) = \frac{1}{R} \sum_{j=1}^R (z_{B_i}(X_{(B_i)}(t)) - z_{B_i}(X_j^{(-P)(B_i)})) \quad (5)$$

$$E_r^{(-)(B_i)}(X_{(B_i)}(t)) = \frac{1}{R} \sum_{j=1}^R (z_{B_i}(X_j^{(-N)(B_i)}) - z_{B_i}(X_{(B_i)}(t))) \quad (6)$$

Положительное значение  $E_r^{(\pm)}$  соответствуют реакции модели, согласованной с направлением выбранных атрибуций. Отклонение выхода при сохранении только этих признаков оценивается показателями достаточности:

$$S_r^{(+)(B_i)}(X_{(B_i)}(t)) = \frac{1}{R} \sum_{j=1}^R |z_{B_i}(X_{(B_i)}(t)) - z_{B_i}(X_j^{(+P)(B_i)})| \quad (7)$$

$$S_r^{(-)(B_i)}(X_{(B_i)}(t)) = \frac{1}{R} \sum_{j=1}^R |z_{B_i}(X_{(B_i)}(t)) - z_{B_i}(X_j^{(+N)(B_i)})| \quad (8)$$

Меньшее значение  $S_r^{(\pm)}$  или  $S_r^{(-)}$  означает более полное воспроизведение исходного выхода. Для совместной ХАИ-конфигурации проверочные показатели усредняются:

$$E^{(\pm)(B_i)}(X_{(B_i)}(t)) = \frac{1}{p} \sum_{r=1}^p E_r^{(\pm)(B_i)}(X_{(B_i)}(t)), \quad (9)$$

$$S^{(\pm)(B_i)}(X_{(B_i)}(t)) = \frac{1}{p} \sum_{r=1}^p S_r^{(\pm)(B_i)}(X_{(B_i)}(t)). \quad (10)$$

Различие в достаточности двух направлений выражается показателем:

$$\begin{aligned} \Delta S(X_{(B_i)}(t)) &= \\ &= S^{(-)(B_i)}(X_{(B_i)}(t)) - S^{(+)(B_i)}(X_{(B_i)}(t)), \end{aligned} \quad (11)$$

Положительное значение  $\Delta S$  указывает на меньший остаток для положительных атрибуций, отрицательное значение соответствует более высокой достаточности противоположного направления.

Проверочные изменения не отражают распределение влияния между входными признаками. Для его оценки модули атрибуций преобразуются в относительные веса:



$$\omega_{l,r}^{(B_i)}(t) = \frac{|a_{l,r}^{(B_i)}(t)|}{\sum_{h=1}^k |a_{h,r}^{(B_i)}(t)|}, \quad l = 1, \dots, k. \quad (12)$$

Энтропия полученного распределения рассчитывается по ненулевым весам:

$$H_r^{(B_i)}(t) = - \sum_{\substack{l=1 \\ \omega_{l,r}^{(B_i)}(t) > 0}}^k \omega_{l,r}^{(B_i)}(t) \ln \omega_{l,r}^{(B_i)}(t). \quad (13)$$

Концентрация атрибуций определяется дополнением нормированной энтропии до единицы:

$$C_r^{(B_i)}(t) = 1 - \frac{H_r^{(B_i)}(t)}{\ln k}. \quad (14)$$

Значение  $C_r^{(B_i)}(t)$  близкое к единице, соответствует сосредоточению влияния на небольшом числе признаков. При отсутствии ненулевых атрибуций принимается  $C_r^{(B_i)}(t) = 0$ . Для совместной ХАИ-конфигурации используется среднее значение:

$$C^{(B_i)}(t) = \frac{1}{p} \sum_{r=1}^p C_r^{(B_i)}(t). \quad (15)$$

Усреднение проверочных показателей не учитывает различия между отдельными объяснителями. Их разброс сохраняется с помощью стандартных отклонений:

$$\sigma_{E^{(+)}}^{(B_i)}(X_{(B_i)}(t)) = \sqrt{\frac{1}{p} \sum_{r=1}^p \left( E_r^{(+)(B_i)} - E^{(+)(B_i)} \right)^2}, \quad (16)$$

$$\sigma_{E^{(-)}}^{(B_i)}(X_{(B_i)}(t)) = \sqrt{\frac{1}{p} \sum_{r=1}^p \left( E_r^{(-)(B_i)} - E^{(-)(B_i)} \right)^2}, \quad (17)$$

$$\sigma_{S^{(+)}}^{(B_i)}(X_{(B_i)}(t)) = \sqrt{\frac{1}{p} \sum_{r=1}^p \left( S_r^{(+)(B_i)} - S^{(+)(B_i)} \right)^2}, \quad (18)$$

$$\sigma_{S^{(-)}}^{(B_i)}(X_{(B_i)}(t)) = \sqrt{\frac{1}{p} \sum_{r=1}^p \left( S_r^{(-)(B_i)} - S^{(-)(B_i)} \right)^2}, \quad (19)$$

Близость числовых оценок не означает, что ХАИ-методы выделили одинаковые признаки. Состав положительных и отрицательных топ-множеств сопоставляется с помощью коэффициента Жаккара:

$$J^{(+)}(X_{(B_i)}(t)) = \frac{2}{p(p-1)} \sum_{r=1}^{p-1} \sum_{h=r+1}^p \frac{|P_r^{(B_i)}(t) \cap P_h^{(B_i)}(t)|}{|P_r^{(B_i)}(t) \cup P_h^{(B_i)}(t)|}, \quad (20)$$

$$J^{(-)}(X_{(B_i)}(t)) = \frac{2}{p(p-1)} \sum_{r=1}^{p-1} \sum_{h=r+1}^p \frac{|N_r^{(B_i)}(t) \cap N_h^{(B_i)}(t)|}{|N_r^{(B_i)}(t) \cup N_h^{(B_i)}(t)|}, \quad (21)$$

При пустом объединении двух множеств соответствующее отношение принимается равным единице. Коэффициенты  $J^{(\pm)}$  учитывают состав топ-множеств,

но не порядок влияния всех признаков. Пусть  $Ind_{l,r}$

обозначает ранг  $|a_{l,r}^{(B_i)}(t)|$  в последовательности атрибуций  $r$ -го объяснителя, причем совпадающим значениям назначается средний ранг:

$$\overline{Ind}_r = \frac{1}{k} \sum_{l=1}^k Ind_{l,r}. \quad (22)$$

Согласованность рангов объяснителей  $r$  и  $h$  определяется выражением:

$$Corr_{r,h}(X_{(B_i)}(t)) = \frac{\sum_{l=1}^k (Ind_{l,r} - \overline{Ind}_r)(Ind_{l,h} - \overline{Ind}_h)}{\sqrt{\sum_{l=1}^k (Ind_{l,r} - \overline{Ind}_r)^2} \sqrt{\sum_{l=1}^k (Ind_{l,h} - \overline{Ind}_h)^2}}, \quad (23)$$

Корреляция определяется для пар ХАИ-методов, у которых обе последовательности рангов имеют ненулевой разброс. Множество таких пар обозначается  $\mathcal{P}_{rank}(t)$ , а их количество —  $kol_{rank}(t)$ . Средняя ранговая согласованность составляет:

$$A_{rank}(X_{(B_i)}(t)) = \frac{2}{kol_{rank}(t)} \sum_{(r,h) \in \mathcal{P}_{rank}(t)} Corr_{r,h}(X_{(B_i)}(t)). \quad (24)$$

Если ранговую корреляцию невозможно вычислить ни для одной пары ХАИ-методов, принимается  $A_{rank} = 0$ . Ранговая согласованность рассчитывается по модулям атрибуций и потому не учитывает направление влияния признаков. Для его сопоставления используется знаковая функция:

$$sign(a) = \begin{cases} 1, & a > 0, \\ 0, & a = 0, \\ -1, & a < 0. \end{cases}$$

В оценку включаются признаки, которым хотя бы один ХАИ-метод назначил ненулевую атрибуцию. Их активность обозначается  $u_l^{(B_i)}$ , а количество —  $k_a^{(B_i)}$ :

$$u_l^{(B_i)}(t) = I \left( \sum_{r=1}^p |a_{l,r}^{(B_i)}(t)| > 0 \right), \quad (25)$$

$$k_a^{(B_i)}(t) = \sum_{l=1}^k u_l^{(B_i)}(t). \quad (26)$$

Для каждого активного признака сопоставляются направления, полученные отдельными объяснителями. Их средняя согласованность определяется выражением:

$$A_{sign}(X_{(B_i)}(t)) = \frac{1}{k_a^{(B_i)}(t)} \sum_{l=1}^k u_l^{(B_i)}(t) \left| \frac{1}{p} \sum_{r=1}^p sign(a_{l,r}^{(B_i)}(t)) \right|, \quad (27)$$

Если  $k_a^{(B_i)}(t) = 0$ , принимается  $A_{sign} = 0$ . Значение показателя уменьшается при расхождении направлений и при отсутствии атрибуции у части объяснителей.

Полученные показатели характеризуют объяснение, но не положение самого объекта относительно известных решений. Для каждой группы

$G \in \{TP, FP, TN, FN\}$  определяется расстояние до ближайшего объекта:

$$d_G(X_{(B_i)}(t)) = \min_{X_{(B_i),c} \in G, X_{(B_i),c} \neq X_{(B_i)}(t)} \sqrt{\sum_{l=1}^k (x_l - x_{l,c})^2}, \quad (28)$$

Относительное положение между правильной и ошибочной группами соответствующей ветви выражается показателями:

$$Near_{FN}(X_{(B_i)}(t)) = d_{TN} - d_{FN}, \quad (29)$$

$$Near_{FP}(X_{(B_i)}(t)) = d_{TP} - d_{FP}, \quad (30)$$

Положительное значение  $Near_{FN}$  и  $Near_{FP}$  соответствуют большей близости объекта к известным ошибочным решениям FN и FP.

Совместное использование показателей требует привести их к сопоставимому диапазону. Преобразования определяются по их эмпирическим распределениям на объектах  $D_{fit}$ . Для исходного показателя  $\tilde{m}_s$ , увеличение которого используется в прямом направлении, применяется выражение:

$$m_s^{(B_i)}(t) = \frac{1}{kol_{fit}} \sum_{k_{fit}=1}^{kol_{fit}} I(\tilde{m}_{s,k_{fit}}^{(B_i)}(t) \leq \tilde{m}_s^{(B_i)}(t)). \quad (31)$$

где  $kol_{fit}$  – число объектов  $D_{fit}$ . Прямое преобразование применяется к  $E^{(\pm)}$ ,  $\Delta S$ ,  $Near_{FN}$  и  $Near_{FP}$ . Для показателей  $S^{(\pm)}$  и  $\sigma$  используется обратное направление шкалы:

$$m_s^{(B_i)}(t) = 1 - \frac{1}{kol_{fit}} \sum_{k_{fit}=1}^{kol_{fit}} I(\tilde{m}_{s,k_{fit}}^{(B_i)}(t) \leq \tilde{m}_s^{(B_i)}(t)). \quad (32)$$

Показатели  $C$ ,  $J^{(\pm)}$  и  $A_{sign}$  уже принадлежат диапазону  $[0,1]$ . Значение  $A_{rank}$  линейно переносится из диапазона  $[-1,1]$  в  $[0,1]$ . Распределения  $D_{fit}$  используются при преобразовании показателей калибровочных, тестовых и поступающих объектов.

При использовании одного XAI-метода диагностический профиль имеет вид:

$$\mathcal{M}_{(B_i)}(t) = (E^{(\pm)}, S^{(\pm)}, \Delta S, C, Near_{FN}, Near_{FP}).$$

При совместной XAI-конфигурации он дополняется компонентами:  $\sigma_{E^{(\pm)}}$ ,  $\sigma_{S^{(\pm)}}$ ,  $J^{(\pm)}$ ,  $A_{rank}$ ,  $A_{sign}$ .

Сформированный профиль характеризует реакцию ML-модели на проверочные изменения, распределение влияния между признаками, согласованность объяснителей и положение объекта относительно известных типов решений. Совместное проявление этих свойств образует признаковое описание для синтеза правил  $\mathfrak{D}_1$  и  $\mathfrak{D}_0$ .

## Синтез диагностического правила

Различие правильных и ошибочных решений может определяться сочетанием нескольких компонентов диагностического профиля, поэтому оно не сводится к пороговой проверке отдельного показателя. Искомая зависимость устанавливается в пространстве сформированных профилей. Прогноз ML-модели разделяет эту задачу на две ветви. При  $\hat{y}_{(B_i)}(t) = 1$  сопоставляются решения TP и FP, а при  $\hat{y}_{(B_i)}(t) = 0$  сопоставляются TN и FN. Различный диагностический смысл этих сравнений приводит к построению правил  $\mathfrak{D}_1$  и  $\mathfrak{D}_0$ .

Обучающее множество положительной ветви включает профили объектов TP и FN:

$$\mathcal{M}_{(B_i)}^{fit-\mathfrak{D}_1} = \{(\mathcal{M}_{(B_i),k_{fit}}(t), Class_{k_{fit}}^{\mathfrak{D}_1}) : TP \cup FP\},$$

где

$$Class_{k_{fit}}^{\mathfrak{D}_1} = \begin{cases} 1, & X_{(B_i)}^{k_{fit}} \in TP \\ 0, & X_{(B_i)}^{k_{fit}} \in FP \end{cases}.$$

Положительный класс представлен правильно выявленными угрозами. Поэтому выход  $\mathfrak{D}_1$  характеризует соответствие исследуемого профиля сочетаниям показателей, наблюдавшимся у TP. Снижение этой оценки указывает на смещение профиля в сторону ложноположительных решений.

Для отрицательной ветви формируется множество:

$$\mathcal{M}_{(B_i)}^{fit-\mathfrak{D}_0} = \{(\mathcal{M}_{(B_i),k_{fit}}(t), Class_{k_{fit}}^{\mathfrak{D}_0}) : TN \cup FN\},$$

где

$$Class_{k_{fit}}^{\mathfrak{D}_0} = \begin{cases} 0, & X_{(B_i)}^{k_{fit}} \in TN \\ 1, & X_{(B_i)}^{k_{fit}} \in FN \end{cases}.$$

В этой ветви положительный класс соответствует пропускам угроз. Выход  $\mathfrak{D}_0$  характеризует сходство исследуемого профиля с сочетаниями показателей, наблюдавшимися у FN. Формирование каждого правила требует наличия обеих сравниваемых групп в  $D_{fit}$ .

Различия между группами могут одновременно проявляться по нескольким координатам профиля. Для представления таких сочетаний используются деревья решений (Decision Trees), последовательно разделяющие пространство  $\mathcal{M}_{(B_i)}$ . Неравное число правильных и ошибочных решений компенсируется весами:

$$\varphi_{TP} = \frac{1}{2Kol_{fit,TP}}, \quad \varphi_{FP} = \frac{1}{2Kol_{fit,FP}},$$

$$\varphi_{TN} = \frac{1}{2Kol_{fit,TN}}, \quad \varphi_{FN} = \frac{1}{2Kol_{fit,FN}},$$

где  $Kol_{fit,G}$  обозначает число объектов группы  $G$  в  $D_{fit}$ . При таком распределении суммарный вес каждой из двух групп соответствующей ветви равен  $1/2$ . Правила формируются выражениями:

$$\mathfrak{D}_1 = \text{DecisionTreeClassifier} \left( \mathcal{M}_{(B_i)}^{fit_{\mathfrak{D}_1}}, \varphi_{TP}, \varphi_{FP} \right), \quad (33)$$

$$\mathfrak{D}_0 = \text{DecisionTreeClassifier} \left( \mathcal{M}_{(B_i)}^{fit_{\mathfrak{D}_0}}, \varphi_{TN}, \varphi_{FN} \right). \quad (34)$$

Глубина дерева и минимальное число объектов в листе ограничивают сложность получаемых правил. Внутренние условия выбираются по координатам диагностического профиля, а каждому листу ставится в соответствие оценка, определяемая взвешенным соотношением сравниваемых классов.

Полученные оценки еще не задают границы диагностических состояний. Для их установления применяются объекты  $D_{cal}$ , профили которых рассчитываются с использованием эталонных групп и эмпирических преобразований, сформированных по  $D_{fit}$ . В положительной и отрицательной ветвях вычисляются оценки:

$$\tau_{(B_i),TP,k_{cal}}^{cal_{\mathfrak{D}_1}} = \mathfrak{D}_1 \left( \mathcal{M}_{(B_i),k_{cal}}^{cal_{\mathfrak{D}_1}} \right), \quad (35)$$

$$\tau_{(B_i),FN,k_{cal}}^{cal_{\mathfrak{D}_0}} = \mathfrak{D}_0 \left( \mathcal{M}_{(B_i),k_{cal}}^{cal_{\mathfrak{D}_0}} \right). \quad (36)$$

Обе оценки принадлежат диапазону  $[0,1]$ , но имеют разную смысловую направленность. Увеличение  $\tau_{(B_i),TP}^{cal_{\mathfrak{D}_1}}$

означает большее соответствие профилю TP, тогда как увеличение  $\tau_{(B_i),FN}^{cal_{\mathfrak{D}_0}}$  означает большее соответствие

профилю FN. Поэтому в положительной ветви подозрительная область задается условием  $\tau_{(B_i),TP}^{cal_{\mathfrak{D}_1}} < \theta_{TP}$ , а в отрицательной условием  $\tau_{(B_i),FN}^{cal_{\mathfrak{D}_0}} > \theta_{FN}$ . Оценки дерева

принимают конечное число значений, поэтому все возможные варианты разделения калибровочных объектов могут быть представлены конечной последовательностью порогов. Пусть различные оценки соответствующей ветви упорядочены как  $\tau_1 < \tau_2 < \dots < \tau_{kol_{cal}}$ . В последовательность кандидатов включаются границы диапазона 0 и 1, значения  $\tau$ , а также середины интервалов между соседними оценками  $\frac{\tau_{k_{cal}} + \tau_{k_{cal}+1}}{2}$ . Повторяющиеся значения исключаются, после чего кандидаты упорядочиваются по возрастанию. Кандидат обозначается  $\theta_j^{cand}$ , а их общее число —  $kol_{cand}$ .

Каждый кандидат определяет состав подозрительной области, в которую вместе с ошибочными могут быть направлены правильные решения ML-модели. Поэтому допустимость порога сначала оценивается по доле правильных решений соответствующей ветви, отнесенных к подозрительному состоянию. Для положительной ветви эта доля составляет:

$$\begin{aligned} FPR_{TP}^{\theta_j^{cand}} &= \\ &= \frac{1}{kol_{cal,TP}} \sum_{k_{cal}: X_{k_{cal}}^{cal} \in TP} I \left( \tau_{(B_i),TP,k_{cal}}^{cal_{\mathfrak{D}_1}} < \theta_j^{cand} \right), \end{aligned} \quad (37)$$

а для отрицательной ветви:

$$\begin{aligned} FPR_{TN}^{\theta_j^{cand}} &= \frac{1}{kol_{cal,TN}} \sum_{k_{cal}: X_{k_{cal}}^{cal} \in} \\ &\in TN I \left( \tau_{(B_i),FN,k_{cal}}^{cal_{\mathfrak{D}_0}} > \theta_j^{cand} \right). \end{aligned} \quad (38)$$

Показатели  $FPR_{TP}$  и  $FPR_{TN}$  выражают доли правильных решений соответствующих ветвей, направленных в подозрительное состояние. Допустимыми признаются кандидаты, для которых выполняются условия:

$$FPR_{TP}^{\theta_j^{cand}} \leq \alpha_{TP}, \quad FPR_{TN}^{\theta_j^{cand}} \leq \alpha_{TN}, \quad (39)$$

где  $\alpha_{TP}$  и  $\alpha_{TN}$  задают предельные доли правильных решений соответствующих ветвей, допускаемые к дополнительной проверке. Среди удовлетворяющих этим ограничениям кандидатов порог выбирается по полноте выделения ошибочной группы. Для положительной ветви полнота обнаружения FP определяется выражением:

$$\begin{aligned} Recall_{FP}^{\theta_j^{cand}} &= \frac{1}{kol_{cal,FP}} \sum_{k_{cal}: X_{k_{cal}}^{cal} \in} \\ &\in FP I \left( \tau_{(B_i),TP,k_{cal}}^{cal_{\mathfrak{D}_1}} < \theta_j^{cand} \right), \end{aligned} \quad (40)$$

а в отрицательной ветви полнота выявления FN составляет:

$$\begin{aligned} Recall_{FN}^{\theta_j^{cand}} &= \frac{1}{kol_{cal,FN}} \sum_{k_{cal}: X_{k_{cal}}^{cal} \in} \\ &\in FN I \left( \tau_{(B_i),FN,k_{cal}}^{cal_{\mathfrak{D}_0}} > \theta_j^{cand} \right), \end{aligned} \quad (41)$$

Ограничения по правильной группе не характеризуют полный размер формируемой подозрительной области. Ее доля среди всех решений соответствующей ветви рассчитывается как:

$$\begin{aligned} SuspShare_{\mathfrak{D}_1}^{\theta_j^{cand}} &= \frac{1}{kol_{cal,TP} + kol_{cal,FP}} \sum_{k_{cal}: X_{k_{cal}}^{cal} \in} \\ &\in FP \cup TP I \left( \tau_{(B_i),TP,k_{cal}}^{cal_{\mathfrak{D}_1}} < \theta_j^{cand} \right), \end{aligned} \quad (42)$$

$$\begin{aligned} SuspShare_{\mathfrak{D}_0}^{\theta_j^{cand}} &= \frac{1}{kol_{cal,TN} + kol_{cal,FN}} \sum_{k_{cal}: X_{k_{cal}}^{cal} \in} \\ &\in FN \cup TN I \left( \tau_{(B_i),FN,k_{cal}}^{cal_{\mathfrak{D}_0}} > \theta_j^{cand} \right), \end{aligned} \quad (43)$$

Для каждой ветви выбирается допустимый порог с наибольшим  $Recall$ . При одинаковой полноте предпочтение получает кандидат с меньшей долей подозрительных объектов  $SuspShare$ . Если оба показателя совпадают, для  $\mathfrak{D}_1$  выбирается наименьший порог, а для  $\mathfrak{D}_0$  — наибольший. Такой порядок сохраняет достигнутое выявление ошибок при наименьшем объеме дополнительной проверки.

Полученные пороги  $\theta_{TP}$  и  $\theta_{FN}$  связывают оценки двух правил с диагностическими состояниями. Для

поступающего объекта применяемая ветвь определяется прогнозом ML-модели:

$$\begin{aligned} \tau_{(B_i)}(t) &= g_{\hat{y}_{(B_i)}(t)}(\mathcal{M}_{(B_i)}(t)) = \\ &= \begin{cases} \mathfrak{D}_1(\mathcal{M}_{(B_i)}(t)), & \hat{y}_{(B_i)}(t) = 1, \\ \mathfrak{D}_0(\mathcal{M}_{(B_i)}(t)), & \hat{y}_{(B_i)}(t) = 0. \end{cases} \end{aligned} \quad (44)$$

Выход  $\mathfrak{D}_1$  образует оценку  $\tau_{(B_i)}^{TP}$ , а выход  $\mathfrak{D}_0$  образует оценку  $\tau_{(B_i)}^{FN}$ . Их сопоставление с порогами определяет диагностическое состояние объекта:

$$\begin{aligned} Rep_{(B_i)}(t) &= \\ &= \begin{cases} \text{угроза,} & \hat{y}_{(B_i)}(t) = 1 \wedge \tau_{(B_i)}^{TP}(t) \geq \theta_{TP}, \\ \text{подозрительное,} & \hat{y}_{(B_i)}(t) = 1 \wedge \tau_{(B_i)}^{TP}(t) < \theta_{TP}, \\ \text{подозрительное,} & \hat{y}_{(B_i)}(t) = 0 \wedge \tau_{(B_i)}^{FN}(t) > \theta_{FN}, \\ \text{валидное,} & \hat{y}_{(B_i)}(t) = 0 \wedge \tau_{(B_i)}^{FN}(t) \leq \theta_{FN}. \end{cases} \end{aligned} \quad (45)$$

Таким образом, правило  $\mathfrak{D}_1$  оценивает соответствие положительного прогноза профилям правильно выявленных угроз, а правило  $\mathfrak{D}_0$  устанавливает сходство отрицательного прогноза с известными пропусками. Сопоставление полученной оценки с калибровочным порогом определяет диагностическое состояние объекта при заданном ограничении на долю правильных решений, направляемых на дополнительную проверку.

### Экспериментальное исследование метода

Экспериментальная проверка была построена по двум следствиям выдвинутой гипотезы. Если диагностический профиль содержит сведения о правильности решения ML-модели, правила  $\mathfrak{D}_1$  и  $\mathfrak{D}_0$  должны сохранять различимость соответствующих групп на независимых данных. После калибровки порогов выявленные различия должны проявляться в составе диагностических состояний, обеспечивая дополнительный охват ошибочных решений при ограниченной доле правильных объектов, направляемых на проверку. В соответствии с этим сначала оценивалась различимость профилей, а затем охват ранее не наблюдавшейся вредоносной активности и связанная с ним нагрузка.

Исследование проведено на девяти самостоятельных задачах. Шесть из них были сформированы по сетевым данным CIC-IDS2017<sup>3</sup> и UNSW-NB15<sup>4</sup>, три использовали табличные признаки смарт-контрактов, исход-

ный код Solidity<sup>5</sup> и байткод<sup>6</sup> [16, 17]. Feature Ablation, GradientSHAP и LIME были выбраны как методы, основанные соответственно на проверочном изменении признаков, градиентном приближении их вкладов и локальной суррогатной модели. Рассматривались три отдельных объяснителя, две парные конфигурации и совместное применение трех методов. Такой состав позволил проверить, зависит ли диагностическая информация от принципа формирования атрибуций и их совместного использования.

Данные, использованные для обучения ML-модели, формирования диагностических правил, калибровки порогов и итоговой оценки, не пересекались. Эталонные группы и правила  $\mathfrak{D}_1$ ,  $\mathfrak{D}_0$  формировались по  $D_{fit}$ , а пороги определялись по  $D_{cal}$ . Для сопоставимости XAI-конфигураций во всех задачах принималось  $\alpha_{TP} = \alpha_{TN} = 0,1$ . В семи из девяти задач один или несколько типов вредоносной активности исключались из всех предшествующих частей данных и вводились только в  $D_{test}$ . Наборы BCCC и Solidity не содержат самостоятельных типов уязвимостей, поэтому на них оценивался перенос диагностических правил без моделирования появления нового типа угрозы.

Способность правил различать правильные и ошибочные решения оценивалась по AUC. Для  $\mathfrak{D}_1$  сопоставлялись оценки объектов TP и FP, для  $\mathfrak{D}_0$  объектов TN и FN. AUC рассчитывалась на  $D_{test}$  отдельно для шести XAI-конфигураций. В табл. 1 приведены минимальные и максимальные значения AUC среди шести XAI-конфигураций, характеризующие зависимость разделяющей способности правил от способа получения локального объяснения.

Таблица 1  
Различение правильных и ошибочных решений на тестовых данных

| Сценарий                                             | $AUC(\mathfrak{D}_1)$ | $AUC(\mathfrak{D}_0)$ |
|------------------------------------------------------|-----------------------|-----------------------|
| CIC-IDS2017: DDoS                                    | 0,891—0,968           | 0,494—0,516           |
| CIC-IDS2017: PortScan                                | 0,940—0,996           | 0,504—0,654           |
| CIC-IDS2017: DoS GoldenEye, FTP-Patator, SSH-Patator | 0,894—0,925           | 0,525—0,638           |
| UNSW-NB15: Fuzzers                                   | 0,714—0,767           | 0,766—0,789           |
| UNSW-NB15: Generic                                   | 0,861—0,885           | 0,909—0,916           |
| UNSW-NB15: Exploits, DoS, Reconnaissance             | 0,741—0,763           | 0,890—0,904           |
| Смарт-контракты: табличные признаки                  | 0,606—0,639           | 0,575—0,598           |
| Смарт-контракты: Solidity                            | 0,731—0,766           | 0,579—0,673           |
| Смарт-контракты: байткод                             | 0,674—0,717           | 0,717—0,759           |

<sup>3</sup> Network Intrusion dataset (CIC-IDS-2017) // Kaggle. URL: <https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset> (дата обращения: 14.08.2026); Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISp. 2018. Vol. 1. Pp. 108—116.

<sup>4</sup> UNSW\_NB15 // Kaggle. URL: <https://www.kaggle.com/datasets/mrwellsdavid/unswnb15> (дата обращения: 14.08.2026); Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) // 2015 military communications and information systems conference (MilCIS). IEEE, 2015. Pp. 1—6.

<sup>5</sup> Vulnerable Solidity Smart Contracts dataset // Kaggle. URL: <https://www.kaggle.com/datasets/rha4365/vulnerable-solidity-smart-contracts-dataset> (дата обращения: 14.08.2026).

<sup>6</sup> Vulnerable Smart Contracts Detection using ML/DL (BCCC-VoSCs-2023) // Kaggle. URL: <https://www.kaggle.com/datasets/bcccdatasets/bccc-vulscs-2023> (дата обращения: 14.08.2026).



Результаты выявили различный характер диагностической информации в двух ветвях прогноза. Правило  $\mathfrak{D}_1$  различало TP и FP во всех девяти задачах и при каждой XAI-конфигурации. Для  $\mathfrak{D}_0$  наиболее выраженное разделение FN и TN получено в задачах UNSW-NB15. В сценариях CIC-IDS2017 результат зависел от сочетания данных и объяснителя. Для PortScan смена XAI-конфигурации заметно изменяла различимость, а в DDoS значения оставались около уровня случайного упорядочения. При анализе смарт-контрактов диагностическая информация сохранялась во всех трех представлениях данных, хотя значения AUC были ниже, чем в большинстве сетевых задач. Следовательно, в положительной ветви различия между профилями правильных и ошибочных решений сохранялись во всех задачах. В отрицательной ветви возможность их разделения определялась сочетанием данных, ML-модели и XAI-конфигурации, что подтверждает необходимость самостоятельного формирования  $\mathfrak{D}_1$  и  $\mathfrak{D}_0$ .

AUC характеризует упорядочение правильных и ошибочных решений, но не показывает результат применения калиброванных порогов. Чтобы установить, приводит ли выявленная различимость к дополнительному охвату ранее не наблюдавшейся вредоносной активности, рассматривалась целевая группа  $\Omega_{\text{цель}}$  представленная только в  $D_{\text{test}}$ . Исходный охват этой группы определялся долей положительных прогнозов ML-модели:

$$\rho_{ML} = \frac{1}{|\Omega_{\text{цель}}|} \sum_{j \in \Omega_{\text{цель}}} I(\hat{y}_j = 1), \quad (46)$$

После применения диагностических правил в области наблюдения сохранялись объекты, получившие состояния «угроза» и «подозрительное». Их совокупная доля составляла:

$$\rho_{ML+XAI} = \frac{1}{|\Omega_{\text{цель}}|} \sum_{j \in \Omega_{\text{цель}}} I(ALERT_j). \quad (47)$$

Разность  $\rho_{ML+XAI} - \rho_{ML}$  определяет дополнительную долю удержанной вредоносной активности, переведенной правилом  $\mathfrak{D}_0$  в подозрительное состояние. Однако этот результат не характеризует объем дополнительной проверки, поскольку целевая группа составляет лишь часть подозрительных объектов. Доля

всех объектов  $D_{\text{test}}$ , получивших подозрительное состояние, определялась выражением:

$$\rho_{\text{доп}} = \frac{1}{N_{\text{test}}} \sum_{j=1}^{N_{\text{test}}} I(Rep_j = \text{подозрительное}), \quad (48)$$

где  $N_{\text{test}}$  — число объектов тестовой выборки. Воздействие метода на обработку объектов нормы оценивалось показателем:

$$\rho_{\text{норм}} = \frac{\sum_{j=1}^{N_{\text{test}}} I(y_j=0 \wedge Rep_j=\text{подозрительное})}{\sum_{j=1}^{N_{\text{test}}} I(y_j=0)}. \quad (49)$$

Объем дополнительной проверки не показывает, насколько избирательно правило  $\mathfrak{D}_0$  выделяет пропуски угроз. Поэтому доля FN среди подозрительных объектов отрицательной ветви сопоставлялась с их долей среди всех отрицательных прогнозов ML-модели. Отношение этих величин определялось коэффициентом:

$$\begin{aligned} Lift_{FN} &= \frac{\sum_{j=1}^{N_{\text{test}}} I(\hat{y}_j=0 \wedge y_j=1 \wedge Rep_j=\text{подозрительное})}{\sum_{j=1}^{N_{\text{test}}} I(\hat{y}_j=0 \wedge Rep_j=\text{подозрительное})} \\ &= \frac{\sum_{j=1}^{N_{\text{test}}} I(\hat{y}_j=0 \wedge y_j=1)}{\sum_{j=1}^{N_{\text{test}}} I(\hat{y}_j=0)}. \end{aligned} \quad (50)$$

$Lift_{FN} > 1$  означает повышенную концентрацию FN в подозрительной области. В табл. 2 исходный охват приведен одним значением, а результаты шести XAI-конфигураций — диапазонами.

Во всех семи сценариях итоговый охват удержанной вредоносной активности превышал исходный результат ML-модели. Возможный прирост ограничивался долей целевых объектов, пропущенных исходной ML-моделью. Его фактическое значение зависело от разделяющей способности  $\mathfrak{D}_0$  и выбранного порога. Поэтому почти полный исходный охват Generic оставлял небольшой резерв для улучшения. В DDoS значительная часть целевой активности оставалась пропущенной, однако значения AUC, близкие к 0,5, сопровождалась малым приростом. Для Fuzzers правило  $\mathfrak{D}_0$  сохраняло высокую разделяющую способность при всех XAI-конфигурациях, тогда как результат PortScan заметно зависел от выбранного объяснителя.

Таблица 2

**Охват удержанной вредоносной активности и показатели дополнительной проверки**

| Сценарий                                | $\rho_{ML}$ | $\rho_{ML+XAI}$ | $Lift_{FN}$ | $\rho_{\text{норм}}$ | $\rho_{\text{доп}}$ |
|-----------------------------------------|-------------|-----------------|-------------|----------------------|---------------------|
| DDoS                                    | 0,6332      | 0,636—0,647     | 1,134—1,789 | 0,0253—0,0413        | 0,0202—0,1280       |
| DoS GoldenEye, FTP-Patator, SSH-Patator | 0,2629      | 0,3210—0,4757   | 1,384—1,643 | 0,0345—0,0625        | 0,0914—0,2303       |
| PortScan                                | 0,0030      | 0,0389—0,3464   | 1,120—1,496 | 0,0312—0,0452        | 0,0322—0,1775       |
| Exploits, DoS, Reconnaissance           | 0,8105      | 0,8406—0,9242   | 2,318—2,974 | 0,0290—0,1193        | 0,0743—0,1834       |
| Fuzzers                                 | 0,2370      | 0,4404—0,5822   | 1,494—1,536 | 0,0673—0,1165        | 0,2052—0,2876       |
| Generic                                 | 0,9782      | 0,9839—0,9920   | 3,529—3,949 | 0,1032—0,1273        | 0,0731—0,0919       |
| Смарт-контракты: байткод                | 0,3750      | 0,4571—0,5571   | 1,928—2,190 | 0,0410—0,1270        | 0,0571—0,1700       |

Значения  $Lift_{FN} > 1$ , полученные во всех сценариях, свидетельствуют о преимущественной концентрации пропусков угроз в подозрительной области отрицательной ветви. Этот показатель дополняет оценку охвата, но не заменяет ее. Для Generis высокая концентрация FN сочеталась с небольшим приростом из-за малого числа исходных пропусков, тогда как для PortScan меньшие значения  $Lift_{FN}$  могли сопровождаться существенно большим дополнительным охватом.

Увеличение охвата обычно расширяло область дополнительной проверки  $P_{доп}$ , однако эта зависимость не была пропорциональной. В DDoS изменение  $P_{доп}$  почти не влияло на результат, а в PortScan и объединенном сценарии CIC-IDS2017 отдельные XAI-конфигурации обеспечивали заметный прирост при ограниченном воздействии на объекты нормы. Для Fuzzers больший охват сопровождался более широкой проверкой, тогда как в Generis воздействие на норму оказалось высоким относительно полученного прироста.

Полученные зависимости показывают, что XAI-конфигурация определяет соотношение между охватом пропущенной активности, концентрацией FN и объемом дополнительной проверки. Универсально предпочтительного варианта по совокупности этих характеристик не выявлено. Более широкий охват мог сопровождаться увеличением очереди, а высокая концентрация FN могла достигаться при охвате лишь небольшой части исходных пропусков. Эксперимент подтвердил возможность сохранять часть ранее не наблюдавшейся вредоносной активности в области наблюдения, но показал, что практический результат метода нельзя характеризовать максимумом одного показателя. Эта зависимость определяет требование к последующей методике применения, предусматрива-

ющей выбор XAI-конфигурации по допустимому соотношению охвата, концентрации FN и объема дополнительной проверки.

## Заключение

Исследование показало, что количественное описание локального объяснения содержит диагностическую информацию о правильности решения ML-модели. В положительной и отрицательной ветвях прогноза эта информация проявляется по-разному, что обосновывает формирование самостоятельных правил  $\mathfrak{D}_1$  и  $\mathfrak{D}_0$ . Их применение с калиброванными порогами дополняет исходный прогноз подозрительным состоянием без изменения классификатора.

Экспериментальное исследование подтвердило гипотезу в положительной ветви всех девяти задач при каждой XAI-конфигурации. В отрицательной ветви возможность разделения TN и FN зависела от данных и способа формирования объяснения. Во всех семи сценариях с удержанной вредоносной активностью часть пропущенных объектов была переведена в подозрительное состояние, где концентрация FN превышала исходную концентрацию среди отрицательных прогнозов. Следовательно, дополнительный охват обеспечивался не только расширением области проверки, но и преимущественным выделением пропусков. Соотношение достигнутого результата и объема проверки различалось между XAI-конфигурациями, поэтому универсально предпочтительный вариант не установлен. Полученная зависимость определяет необходимость разработки методики выбора ML- и XAI-конфигураций, допустимых значений  $\alpha$  и условий актуализации диагностических правил.

*Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение от 27.09.2024 г. № 23-03).*

## Литература

1. Ларина М.В., Скиба В.Ю. Модель цифровой платформы для анализа устойчивости к квантовым угрозам // Правовая информатика. 2025. № 3. С. 12—26.
2. Скиба В.Ю., Балябин А.А., Петренко С.А. Проблема обеспечения киберустойчивости облачных платформ управления киберфизическими объектами // Правовая информатика. 2025. № 4. С. 26—38.
3. Петренко С.А., Сундеев П.В. Контроль требований к защите информации на основе модели логического вывода и графовой нейронной сети // Правовая информатика. 2026. № 2. С. 85—94.
4. Hasan M. et al. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis // Blockchain: Research and Applications. Elsevier, 2024. Vol. 5. No. 3. Article 100207.
5. Hosain Y., Çakmak M. XAI-XGBoost: an innovative explainable intrusion detection approach for securing internet of medical things systems // Scientific reports. Nature Publishing Group London, 2025. Vol. 15. No. 1. Article 22278.
6. Krishnan D., Singh S., Sugumaran V. Explainable AI for zero-day attack detection in IoT networks using attention fusion model // Discov. Internet Things. 2025. Vol. 5. No. 1. Article 83.
7. Kaya K. et al. X-cba: Explainability aided catboosted anomaly for intrusion detection system // ICC 2024-IEEE International Conference on Communications. IEEE, 2024. Pp. 2288—2293.

8. Senevirathna T. et al. From Insight to Action: XAI-Enhanced Detection of DDoS Attacks in Software Defined Networks // 2025 IEEE 36th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2025. Pp. 1—6.
9. Villegas-Ch W. et al. Autonomous federated defense for zero-day threats in IIoT: explainable agents with real-time edge inference // Frontiers in Communications and Networks. Frontiers Media SA, 2025. Vol. 6. Article 1697204.
10. Mougan C. et al. Explanation Shift: How Did the Distribution Shift Impact the Model? // Transactions on Machine Learning Research. 2024.
11. Decker T. et al. Explanatory Model Monitoring to Understand the Effects of Feature Shifts on Performance // Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, KDD 2024, Barcelona, Spain, August 25—29, 2024. Pp. 550—561.
12. Nauta M. et al. From Anecdotal Evidence to Quantitative Evaluation Methods: A Systematic Review on Evaluating Explainable AI // ACM Comput. Surv. 2023. Vol. 55. No. 13s. Pp. 1—42.
13. Hedström A. et al. Quantus: An Explainable AI Toolkit for Responsible Evaluation of Neural Network Explanations and Beyond // Journal of Machine Learning Research. 2023. Vol. 24. No. 34. Pp. 1—11.
14. Weber R.O. et al. XAI is in trouble // AI Magazine. 2024. Vol. 45. No. 3. Pp. 300—316.
15. Лисов Д.Н. Интерпретационная модель наблюдения и диагностирования состояния элементов блокчейн-систем по решениям моделей машинного обучения // Правовая информатика. 2026. № 3. В печати.
16. Alnuman R. et al. Ensemble multi-label machine learning solidity smart contract vulnerability detection model // Cluster Comput. 2025. Vol. 28. No. 16. Article 1014.
17. HajiHosseiniKhani S., Lashkari A.H., Oskui A.M. Unveiling vulnerable smart contracts: Toward profiling vulnerable smart contracts using genetic algorithm and generating benchmark dataset // Blockchain: Research and Applications. Elsevier, 2024. Vol. 5. No. 1. Article 100171.

**SECTION:**

*SYSTEM ANALYSIS, MANAGEMENT, ARTIFICIAL INTELLIGENCE, AND INFORMATION PROTECTION*

# **A METHOD FOR INTERPRETATIVE DIAGNOSIS OF THE STATE OF BLOCKCHAIN SYSTEM COMPONENTS USING MACHINE LEARNING MODEL SOLUTIONS**

*Lisov D.N.<sup>7</sup>, Gnidko K.O.<sup>8</sup>*

**Keywords:** *explainable artificial intelligence, explanation quality assessment, local explanation, statistical learning, diagnostic rules, diagnostic profile, threshold calibration, suspicious state, new types of threats.*

**Abstract**

**Purpose of work:** *to develop a method for interpretative diagnosis of the state of blockchain system components based on machine learning model outputs when new types of threats emerge.*

**Research method:** *the differences between correct and incorrect decisions made by the ML model were investigated using local explanation metrics. These metrics characterised changes in the model's output following controlled substitution of input features, the structure of attributions, and the consistency of results across multiple explainers. The resulting diagnostic profiles were used to formulate rules using statistical learning methods. Threshold limits were determined in accordance with statistical decision theory, whilst limiting the proportion of correct predictions sent for further verification. The distinguishability between correct and incorrect decisions was assessed using the AUC on independent data. The practical outcome was characterised by a change in the coverage of previously unobserved malicious activity, the concentration of missed threats in the suspicious region, and the volume of additional verification.*

---

<sup>7</sup> **Dmitry N. Lisov**, Ph.D. student, Junior Researcher at the Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sirius, Krasnodar region, Russian Federation. ORCID: 0000-0002-8214-4109.  
E-mail: [lisov.dn@talantiuspeh.ru](mailto:lisov.dn@talantiuspeh.ru)

<sup>8</sup> **Konstantin O. Gnidko**, Dr.Sc. (Technology), Associate Professor, Deputy Head of Group at the Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sirius, Krasnodar region, Russian Federation. ORCID: 0000-0002-8605-8865.  
E-mail: [gnidko.ko@talantiuspeh.ru](mailto:gnidko.ko@talantiuspeh.ru)

**Results of the study:** a method has been developed that supplements the binary prediction of an ML model with a diagnostic state generated on the basis of local explanation characteristics, without altering the original classifier. The scientific novelty lies in the construction of separate diagnostic rules for the positive and negative branches of the prediction and in the independent calibration of their thresholds, taking into account the acceptable proportion of correct decisions sent for additional verification. An experimental study using network data and various representations of smart contracts has shown that the generated rules distinguish between correct and incorrect decisions across different XAI configurations. In scenarios involving malicious activity not encountered during the training of the ML model or the development of diagnostic rules, some of the missed objects were reclassified as suspicious. At the same time, the resulting volume of additional verification was determined. The results confirmed the diagnostic informativeness of local explanation metrics and demonstrated its dependence on the data, the ML model and the XAI configuration. No universally preferred XAI configuration has been identified.

## References

1. Larina M.V., Skiba V.Iu. Model' tsifrovoy platformy dlia analiza ustoichivosti k kvantovym ugrozam // Pravovaia informatika. 2025. No. 3. S. 12—26.
2. Skiba V.Iu., Baliabin A.A., Petrenko S.A. Problema obespecheniia kiberustoiichivosti oblachnykh platform upravleniia kiberfizicheskimi ob'ektami // Pravovaia informatika. 2025. No. 4. S. 26—38.
3. Petrenko S.A., Sundeev P.V. Kontrol' trebovanii k zashchite informatsii na osnove modeli logicheskogo vyvoda i grafovoi neironnoi seti // Pravovaia informatika. 2026. No. 2. S. 85—94.
4. Hasan M. et al. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis // Blockchain: Research and Applications. Elsevier, 2024. Vol. 5. No. 3. Article 100207.
5. Hosain Y., Çakmak M. XAI-XGBoost: an innovative explainable intrusion detection approach for securing internet of medical things systems // Scientific reports. Nature Publishing Group UK London, 2025. Vol. 15. No. 1. Article 22278.
6. Krishnan D., Singh S., Sugumaran V. Explainable AI for zero-day attack detection in IoT networks using attention fusion model // Discov. Internet Things. 2025. Vol. 5. No. 1. Article 83.
7. Kaya K. et al. X-cba: Explainability aided catboosted anomal-e for intrusion detection system // ICC 2024-IEEE International Conference on Communications. IEEE, 2024. Pp. 2288—2293.
8. Senevirathna T. et al. From Insight to Action: XAI-Enhanced Detection of DDoS Attacks in Software Defined Networks // 2025 IEEE 36th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2025. Pp. 1—6.
9. Villegas-Ch W. et al. Autonomous federated defense for zero-day threats in IIoT: explainable agents with real-time edge inference // Frontiers in Communications and Networks. Frontiers Media SA, 2025. Vol. 6. Article 1697204.
10. Mougan C. et al. Explanation Shift: How Did the Distribution Shift Impact the Model? // Transactions on Machine Learning Research. 2024.
11. Decker T. et al. Explanatory Model Monitoring to Understand the Effects of Feature Shifts on Performance // Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, KDD 2024, Barcelona, Spain, August 25—29, 2024. Pp. 550—561.
12. Nauta M. et al. From Anecdotal Evidence to Quantitative Evaluation Methods: A Systematic Review on Evaluating Explainable AI // ACM Comput. Surv. 2023. Vol. 55. No. 13s. Pp. 1—42.
13. Hedström A. et al. Quantus: An Explainable AI Toolkit for Responsible Evaluation of Neural Network Explanations and Beyond // Journal of Machine Learning Research. 2023. Vol. 24. No. 34. Pp. 1—11.
14. Weber R.O. et al. XAI is in trouble // AI Magazine. 2024. Vol. 45. No. 3. Pp. 300—316.
15. Lisov D.N. Interpretatsionnaia model' nabliudeniia i diagnostirovaniia sostoiianiia elementov blokchein-sistem po resheniiam modelei mashinnogo obucheniia // Pravovaia informatika. 2026. No. 3. V pechaty.
16. Alnuman R. et al. Ensemble multi-label machine learning solidity smart contract vulnerability detection model // Cluster Comput. 2025. Vol. 28. No. 16. Article 1014.
17. HajiHosseinKhani S., Lashkari A.H., Oskui A.M. Unveiling vulnerable smart contracts: Toward profiling vulnerable smart contracts using genetic algorithm and generating benchmark dataset // Blockchain: Research and Applications. Elsevier, 2024. Vol. 5. No. 1. Article 100171.





# РАЗВИТИЕ ОТЕЧЕСТВЕННЫХ СИСТЕМ ИНФОРМАЦИОННО-ТЕЛЕМЕТРИЧЕСКОГО ОБЕСПЕЧЕНИЯ ОТРАБОТКИ СРЕДСТВ ВЫВЕДЕНИЯ В КОНТЕКСТЕ СЛОЖИВШИХСЯ ПРОИЗВОДСТВЕННЫХ ОТНОШЕНИЙ

Воронцов В.Л.<sup>1</sup>

**Ключевые слова:** инструменты регламентирования, концепция, метод, научно-методическое обеспечение, организация, предприятие, программно-технические средства, система, стандарты, стратегия, телеметрируемый объект, телеметрическая информация, телеметрический комплекс космодрома.

## Аннотация

**Цель работы:** рекомендации по адаптации процесса развития отечественных систем информационно-телеметрического обеспечения отработки средств выведения к сложившимся производственным отношениям.

**Методы исследования:** системный и экспертный анализ публикаций, концептуальное моделирование, систематизация знаний.

**Результаты:** на основе анализа возможностей адаптации процесса развития отечественных систем информационно-телеметрического обеспечения отработки средств выведения (СИТО<sub>св</sub>) к сложившимся производственным отношениям сформулированы рекомендации. Рекомендовано в качестве научно-методической основы использовать разработанное научно-методическое обеспечение развития СИТО<sub>св</sub>, отражающее научно-технические и организационно-технические аспекты, и, соответственно, позволяющее создать инструменты регламентирования и способы их применения для решения практических задач развития СИТО<sub>св</sub>, причём без необходимости изменения существующих производственных отношений. Показана сущность обновлённого механизма отбора и реализации ценных для развития СИТО<sub>св</sub> предложений, поступающих от заинтересованных предприятий/организаций, что актуально в существующих условиях острой потребности в консолидации усилий.

**Практическая ценность:** полученные результаты могут быть использованы при выработке мер по улучшению управления развитием отечественных СИТО<sub>св</sub> путём использования разработанного научно-методического обеспечения развития СИТО<sub>св</sub> в качестве научно-методической основы.

DOI: 10.24412/1994-1404-2026-3-41-50

## Введение

При значительном количестве (в том числе весьма ценных) предложений/решений по совершенствованию отечественных средств информационно-телеметрического обеспечения отработки средств выведения космических аппаратов и межконтинентальных баллистических ракет (средств ИТО) уровень развития самих средств ИТО остаётся недостаточным. В число вышеупомянутых входят также предложения/решения, сформулированные на основе разработанного [1—5 и др.] научно-методического обеспечения развития отечественных систем информационно-телеметрического обеспечения отработки средств выведения космических аппаратов и межконтинентальных баллистических ракет (СИТОСВ).

Создан солидный научный задел для развития отечественных СИТОСВ (см., в частности, [1—5]).

В этой связи проведён анализ предложений/решений, представленных в сборниках трудов научно-технических конференций [6—11], организованных профильными предприятиями (в частности, АО «Российские космические системы», АО «Научно-производственное объединение измерительной техники»); в научных статьях, опубликованных в открытой печати; в различных Программах (типа Стратегии развития космодрома); в материалах, поступивших от предприятий/организаций ракетно-космической отрасли (РКО) для

<sup>1</sup> **Воронцов Валерий Леонидович**, кандидат технических наук, ведущий инженер-исследователь АО «Российские космические системы», г. Москва, Российская Федерация.  
E-mail: a762642@yandex.ru

разработки документов типа Дорожной карты развития *средств* ИТО, разрабатываемой под эгидой Госкорпорации (ГК) «Роскосмос», и других документов такого рода; в текущих презентациях (обсуждениях) специалистов.

Выявлены следующие причины сложившейся ситуации:

- противоречивые, порой, взаимоисключающие предложения (весьма ярко это проявляется в материалах, поступивших от разных предприятий/организаций РКО, для формулирования положений Дорожной карты развития *средств* ИТО);
- предложения, польза от осуществления которых неочевидна, а необходимые обоснования целесообразности осуществления отсутствуют (типа предложений по применению каналов «борт-Земля» с информативностью до 20 Мбит/с для передачи телеметрической информации ракеты-носителя);
- актуальность отдельных предложений/решений, касающихся направлений развития *средств* ИТО, очевидна (типа перехода на «унифицированные сигнально-кодовые конструкции»), но неочевидны детали практических действий в указанных направлениях и сущности ожидаемого результата (см. особенности стандартизации и унификации структур телеметрической информации [2]);
- имеются предложения, базирующиеся на здравом смысле с элементами обоснования их актуальности (например,<sup>2</sup> сжатие данных телеизмерений в *бортowej информационно-телеметрической системе* (БИТС)<sup>3</sup>, позволяющее в 5—10 раз сократить объёмы передаваемой ТМИ и повысить на 5—6 дБ эквивалентную энергетику радиополучения и таким образом создать благоприятные условия для использования наземных приёмных антенн меньшего диаметра). Однако в условиях отсутствия необходимого механизма отбора и реализации ценных для ИТО предложений они зачастую остаются невостребованными для их дальнейшего развития;
- отдельные технические решения (безотносительные к существующим *средствам* ИТО, предлагаемые не только специалистами РКО), которые могли бы быть кандидатами на апробирование и в дальнейшем (в случае их успешного апробирования) использованы в практике ИТО, оказываются невостребованными (типа [12]), т.к. механизм отбора и реализации ценных для ИТО предложений не работает должным образом;
- существующие условия таковы, что значительная доля задач (и, соответственно, предложений/

решений) связана с вынужденными и имеющими приоритетное значение действиями по модернизации *средств* ИТО из-за физического старения программно-технических средств (ПТС), из-за новых задач ИТО, на которые отвлекаются значительные ресурсы, и на решение задач по качественному улучшению *средств* ИТО не хватает сил и средств. Под эти условия приходится выстраивать производственные отношения [13] предприятий/организаций РКО.

В сложившейся ситуации, кроме усовершенствования самих *средств* ИТО, необходимо улучшить качество управления их развитием, прежде всего, улучшением возможностей целенаправленного и оперативного отбора предложений от заинтересованных предприятий/организаций (функционирующих как в составе, так и вне РКО), направленных на улучшение качества ИТО в целом. В настоящее время существует острая потребность в консолидации усилий разных предприятий/организаций ГК «Роскосмос», Министерства обороны Российской Федерации (МО РФ), а также других заинтересованных предприятий/организаций, находящихся вне РКО. Необходима научно-методическая основа вышеупомянутой консолидации. В качестве такой основы предлагается разработанное [1—5 и др.] научно-методическое обеспечение развития отечественных СИТО<sub>св</sub>, включающее в себя как научно-технические, так и организационно-технические аспекты.

*Цель настоящей работы:* рекомендации по адаптации процесса развития отечественных систем информационно-телеметрического обеспечения отработки средств выведения к сложившимся производственным отношениям.

### **Особенности условий развития средств ИТО, обусловленные сложившимися производственными отношениями**

С научно-техническими аспектами развития *средств* ИТО связаны вопросы, заключающиеся в следующем: какие элементы *средств* ИТО и каким образом нужно улучшить, чтобы улучшить качество ИТО в целом; а с организационно-техническими аспектами — какие инструменты управления (инструменты регламентирования) и способы их применения для этого нужны. Научно-методическое обеспечение должно соответствовать условиям его применения. Особенности условий развития *средств* ИТО таковы:

- предприятия/организации РКО имеют относительно большую самостоятельность в вопросах выбора приоритетных направлений своего развития;
- динамично изменяются требования, интересы, предпочтения специалистов предприятий/организаций, связанных с решением задач разработки, изготовления, эксплуатации *средств* ИТО, использования ТМИ по целевому назначению;

<sup>2</sup> Кисляков М.Ю., Логачев Н.С., Петушков А.М. Системно-технические аспекты развития НАКУ КА НСЭН и измерений до 2025 года // Ракетно-космическое приборостроение и информационные системы. 2016. Т. 3. Вып. 1. С. 62—71.

<sup>3</sup> ГОСТ 19619-74. Оборудование радиотелеметрическое. Термины и определения.

- предприятия/организации РКО имеют большие возможности, связанные с созданием новых ПТС ИТО и информационных технологий (ИТ), с модифицированием структур ТМИ, исходя из своих потребностей и интересов;
- проявляется усиление неопределённых факторов, влияющих на процесс развития ПТС и ИТ (влияющих на общий фон условий развития *средств* ИТО), соответственно проявляется неочевидность развития *средств* ИТО [1];
- в условиях, когда предприятия/организации РКО обычно являются акционерными обществами и их основная цель развития состоит в получении прибыли, неизбежно проявление противоречия, заключающегося в получении наибольшей прибыли и улучшении *средств* ИТО (и качества ИТО в целом) [3];
- отсутствуют необходимые официальные инструменты, регламентирующие процесс развития *средств* ИТО, обеспечивающие гармонизацию целей развития предприятий/организаций РКО и целей развития *средств* ИТО, позволяющие устранить вышеупомянутое противоречие [3].

#### **Недостатки существующего ИТО. Искомый результат развития СИТО<sub>св</sub>**

При решении задач ИТО не удаётся устранить следующие, наиболее зримо проявляющиеся **недостатки** [1, 3]:

- имеют место значительные потери ТМИ, особенно из-за неопределённого поведения *телеметрируемых параметров* (ТМП)<sup>4</sup>, из-за помех, действующих в каналах «борт-Земля»;
- отвлекаются значительные трудовые и материальные ресурсы на подготовку к новым задачам отработки из-за неинвариантности СИТО<sub>св</sub> к изменяющимся задачам ИТО, причём подготовка в существующих условиях сжатых сроков оказывает негативное влияние на качество ПТС СИТО<sub>св</sub>;
- качество управления процессом развития СИТО<sub>св</sub> недостаточное (отсутствует системный, а доминируют субъективный и фрагментарный подходы) и не позволяет своевременно выявлять и устранять негативные тенденции, результативно использовать полезные аналоги из других областей, целенаправленно и своевременно принимать меры по устранению вышеупомянутых недостатков.

Они (недостатки) наиболее зримо проявляются в эвентуальных обстоятельствах, суть которых состоит в следующем:

- потери ТМИ зачастую оказываются замаскированными результатами относительно длинной серии успешных запусков и в значительной мере

проявляются при аварийном исходе запуска, когда ТМИ наиболее ценна;

- причиной неинвариантности СИТО<sub>св</sub> к изменяющимся задачам ИТО является прежде всего значительный разброс количества ТМП в зависимости от типа ракеты-носителя (РН). Обычно с увеличением количества ТМП пропорционально увеличивается количество комплектов *бортовой радиотелеметрической системы* (БРТС)<sup>5</sup> и лавинообразно (из-за необходимости разнесённого приёма ТМИ) количество ПТС телеметрического комплекса космодрома (ТК). Поэтому неинвариантность в полной мере проявится в случае возобновления лётных испытаний (ЛИ) сверхтяжёлых РН (типа РН «Энергия»). Потребуется дооснащение ТК дополнительными ПТС [1];
- недостаточное качество управления процессом развития СИТО<sub>св</sub> является следствием отсутствия необходимого научно-методического обеспечения и связанных с ним инструментов регламентирования (таких как официальная концепция развития СИТО и соответствующий ей комплекс стандартов телеметрии). Поэтому задачи подготовки к ИТО текущих (уже отлаженных) процессов отработки обычно решают относительно оперативно, а на подготовку к новым задачам (в частности, связанным с ЛИ РН) тратится значительное время из-за необходимости многочисленных согласований между предприятиями/организациями РКО, зачастую из-за жёстких ограничений сроков решения принимают в спешке.

Устранение перечисленных выше недостатков (получение искомого результата [1, 4]) связано с построением и развитием СИТО<sub>св</sub> и означает следующее:

- *существенное* сокращение потерь ТМИ в условиях жёстких ограничений материальных и временных ресурсов;
- построение компактного ТК, инвариантного по отношению к изменяющимся задачам ИТО;
- обеспечение подключения к ТК внешних ПТС (типа многофункциональной космической системы ретрансляции «Луч») для расширения его возможностей.

#### **Задачи информационно-телеметрического обеспечения отработки средств выведения**

Показаны [1] задачи ИТО и последовательность их выполнения (рис. 1).

Выделено (см. рис. 1) множество наиболее актуальных задач ИТО:

- формирование ТМИ на *телеметрируемом объекте*;
- приёмо-регистрация ТМИ;

<sup>4</sup> ГОСТ 19619-74. Оборудование радиотелеметрическое. Термины и определения.

<sup>5</sup> ГОСТ 19619-74. Оборудование радиотелеметрическое. Термины и определения.

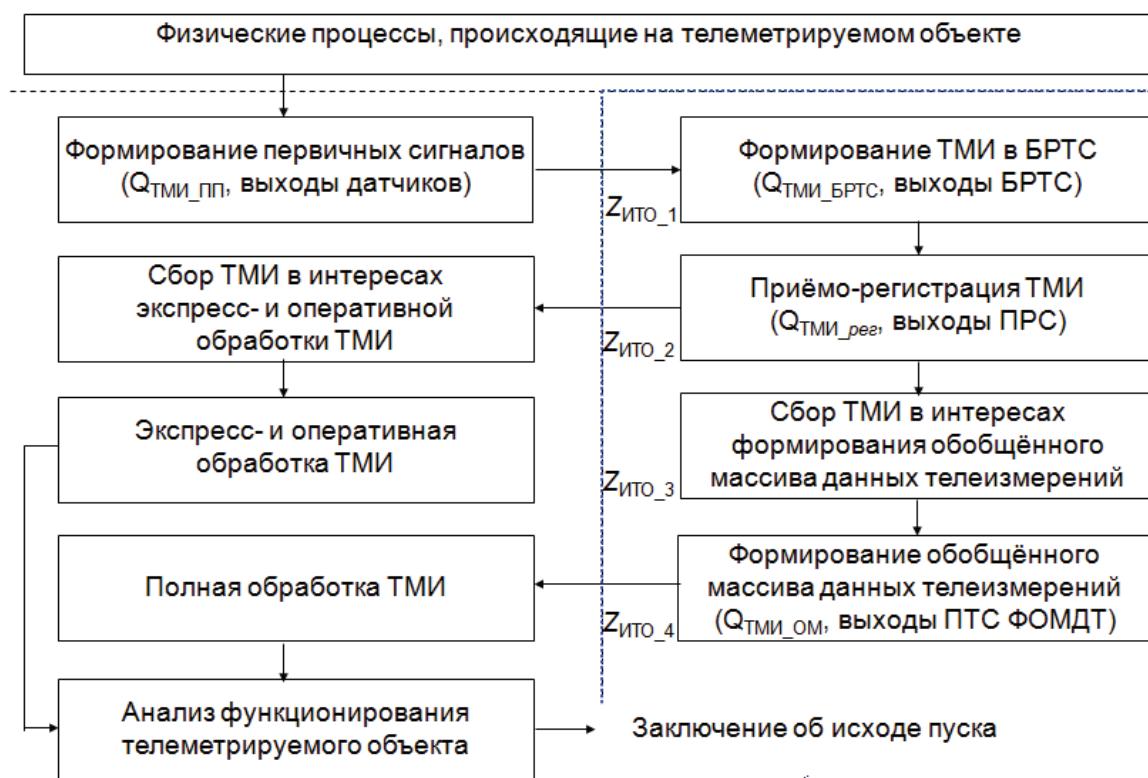


Рис. 1. Задачи информационно-телеметрического обеспечения отработки средств выведения

- сбор ТМИ в интересах формирования обобщённого массива данных телеизмерений;
- формирование обобщённого массива данных телеизмерений (ФОМДТ).

Актуальность выделенных задач обусловлена связанными с ними значительными потерями ТМИ вследствие действия *неопределённых факторов* разной природы.

Если эти выделенные задачи ИТО отнести к системе, то вход этой системы — первичные сигналы (т. е. сигналы на выходе датчиков), а её выход — обобщённые данные телеизмерений (т. е. данные, полученные методами разнесённого приёма), см. рис. 1.

СИТО<sub>св</sub> представляет собой распределённую в пространстве *информационную систему*, которая предназначена для получения в полётное время информации о *телеметрируемых объектах*, причём с учётом заданных ресурсных ограничений и требований к оперативности.

Она включает в себя бортовую радиотелеметрическую систему (БРТС), программно-технические средства (ПТС) телеметрического комплекса космодрома (ТК), являющегося частью измерительного комплекса космодрома (ИКК), а также внешние по отношению к ТК программно-технические средства (типа многофункциональной космической системы ретрансляции «Луч»).

Она компактна: в её составе всего четыре элемента, см. рис. 1. Соответственно, относительно мал объём действий по осуществлению практического *системного* подхода к развитию отечественных *средств* ИТО,

необходимого для выработки результативных мер по улучшению качества ИТО в целом.

#### Суть научно-технических и организационно-технических аспектов, отражённых в научно-методическом обеспечении развития отечественных СИТО<sub>св</sub>

С научно-техническими аспектами развития СИТО<sub>св</sub> связано достижение искомого результата (см. выше) целенаправленным осуществлением стратегий [1, 3] операций усовершенствования и применения усовершенствованных СИТО<sub>св</sub> по целевому назначению (далее — *стратегий усовершенствования и применения*). Сущности *стратегий усовершенствования и применения* описаны [1, 3]. Их ценность определяется по общим (обобщённым) показателям [1, 3, 4], характеризующим качество ИТО в целом. Соответственно, целесообразность усовершенствования отдельного элемента СИТО<sub>св</sub> определяется улучшением качества ИТО в целом.

Наиболее важными элементами стратегий [1, 3] являются методы действий над сигналами/данными, содержащими ТМИ, и сами сигналы/данные. Ими оперируют при построении *стратегий усовершенствования и применения*.

На основе анализа возможностей комплексирования элементов СИТО<sub>св</sub> разработан [1] проблемно-ориентированный метод установления ограничений (требований) к комплексированию средств ИТО, основанный на формальной процедуре морфологического



анализа, позволяющий существенно сузить без ущерба качеству область поиска рациональных стратегий. С использованием сформированных [1] ограничений (требований) и разработанных [1, 3, 4] общих (обобщённых) показателей, разработана **методика построения рациональных стратегий усовершенствования и применения СИТО<sub>СВ</sub>** для противодействия *неопределённым факторам* [1] разной природы управлением избыточностью данных телеизмерений, причём управления, касающегося прежде всего оперирования методами действий над сигналами/данными, содержащими ТМИ. Результаты противодействия оценивают по общим (обобщённым) показателям.

При традиционных действиях для достижения искомого результата проявляются противоречия.

**Основное противоречие** связано с управлением избыточностью данных телеизмерений в условиях изменяющихся *задач ИТО* и действия *неопределённых факторов* различной природы [1]. С одной стороны, сокращение потерь ТМИ традиционным путём приводит к существенному увеличению избыточности, которая и без того чрезвычайно велика. С другой стороны, на избыточные данные отвлекаются значительные ресурсы, что в условиях жёстких ресурсных ограничений не позволяет улучшить качество ИТО простым наращиванием количества программно-технических средств (т. е. экстенсивным путём). Необходимость существенного сокращения потерь ТМИ обусловлена высокими требованиями к достоверности и полноте ТМИ для достижения целей отработки, но дальнейшее увеличение избыточности лишь недопустимо обострит противоречие.

Для устранения противоречия необходимы способы управления избыточностью данных телеизмерений, в основе которых прежде всего новые методы действий над сигналами/данными, содержащими ТМИ.

В этой связи разработаны **алгоритм преобразования первичных сигналов** [1], уменьшающий потери ТМИ вследствие ошибок в выборе ожидаемого диапазона измерений, и обеспечивающий компактное представление данных в условиях жёстких ограничений пропускной способности каналов «борт-Земля; **технологии управляемого разнесённого приёма** [1], обеспечивающие уменьшение потерь ТМИ вследствие действия произвольных помех в каналах «борт-Земля» улучшением достоверности обобщённых данных — и т. д. С их использованием построены рациональные *стратегии усовершенствования и применения*, позволяющие получить вышеупомянутый искомый результат. Однако из-за отсутствия механизма отбора и реализации ценных предложений шансы рациональных стратегий на внедрение в отечественные СИТО<sub>СВ</sub> системы невелики.

Сущности этого механизма описаны [3, 4] в части организационно-технических аспектов разработанного научно-методического обеспечения, касающихся управления развитием СИТОСВ. Предложены [3, 4] инструменты управления (инструменты регламентирования) и способы их применения; в частности, предложены следующие инструменты:

- официальная Концепции развития СИТО<sub>СВ</sub> (с указанием направлений развития);
- *система* стандартов телеметрии, соответствующая вышеупомянутой концепции, обеспечивающая осуществление рациональных стратегий усовершенствования и применения по назначению СИТО<sub>СВ</sub>;
- административные положения (Устав) Рабочей Группы «СИТО<sub>СВ</sub>».

Необходимость *отбора и реализации ценных предложений* касается и вышеупомянутых инструментов регламентирования. Кроме того, что их положения должны ориентировать на получение искомого результата, необходимо создать условия для результативного практического применения *этих положений*. Очевидно, что при наличии нужных положений вышеупомянутых инструментов регламентирования (концепции, стандартов, Устава), необходимы определённые организационные меры для того, чтобы они стали полноценным руководством к действиям. Без создания необходимых условий для их полноценного применения они окажутся невосприимчивыми (бесполезными).

В этой связи предложены [3, 4] организационно-технические меры по созданию благоприятных условий применения и развития положений Концепции, стандартов и Устава.

#### **Актуальные организационно-технические меры по развитию отечественных СИТО<sub>СВ</sub>**

Показаны [2] подходы, касающиеся развития отечественных СИТО<sub>СВ</sub>.

Первый из них заключается в преобладании чисто административных (волюнтаристских) мер по определению каких-либо *радиотелеметрических систем* (РТС)<sup>6</sup> в качестве базовых. По сути, устанавливают «прокрустово ложе» в виде базовых РТС, выбранных для определённых РКН (для определённых *телеметрируемых объектов*<sup>7</sup>). При этом доминируют интересы, касающиеся чьей-то экономической выгоды, «проталкивания» чьих-то разработок.

Второй (проблемно-ориентированный) подход касается предложенного научно-методического обеспечения развития СИТО<sub>СВ</sub>. Оно содержит подходы, правила, стратегии и направления развития, а также — с необходимой степенью детализации — методы, модели, методики, критерии и т. д., причём предложенные элементы СИТО<sub>СВ</sub> актуальны по отношению к применяемым *средствам* ИТО, но безотносительны к ним (подобно тому, как метод модуляции или помехоустойчивого кодирования, описанный в стандарте, может быть реализован в разных программно-технических средствах). При этом ценность результатов определя-

<sup>6</sup> ГОСТ 19619-74. Оборудование радиотелеметрическое. Термины и определения.

<sup>7</sup> ГОСТ 19619-74. Оборудование радиотелеметрическое. Термины и определения.



Рис. 2. Организации/предприятия, Рабочая Группа «СИТО<sub>св</sub>»: отношения и зоны ответственности

ется [1] общими (обобщёнными) показателями операций усовершенствования СИТО<sub>св</sub>.

Соответствующий проблемно-ориентированному подходу порядок построения и применения системы стандартов для СИТО<sub>св</sub> таков: замысел — НИР — ОКР — положения стандартов — практическое их использование. Т.е. положения стандартов должны отражать апробированные решения, существенно улучшающие общие (обобщённые) показатели и (соответственно) качество ИТО в целом [1]. При этом направления развития указаны в Концепции развития СИТО<sub>св</sub> [4].

В предложенном научно-методическом обеспечении развития СИТО<sub>св</sub> учтено влияние неопределённых факторов разной природы на результаты решения текущих задач ИТО, изменений сущностей существующих ПТС и ИТ во времени (т. е. изменений условий, среды, в которой развиваются отечественные СИТО<sub>св</sub>), включая влияние подрывных технологий [5]. Другими словами, предложенное научно-методическое обеспечение ориентировано на упреждение требований к ИТО, на опережающий темп развития отечественных СИТО<sub>св</sub>, обеспечивающий инвариантность ТК к новым задачам ИТО (например, к ЛИ РН, в том числе сверхтяжёлых РН типа «Энергия»), обеспечивающий получение искомого результата. Такие СИТО<sub>св</sub> создадут задел для удовлетворения перспективных требований к ИТО.

Управление развитием отечественных СИТО<sub>св</sub> предложено [4] осуществлять через Рабочую Группу «СИТО<sub>св</sub>» (рис. 2), включающую в себя разносторонних специалистов. Её основные задачи заключаются в анализе предложений, поступающих от предприятий/организаций РКО и от заинтересованных предприятий/организаций вне РКО (в том числе от организаций Ми-

нистерства обороны РФ, от частных фирм), по коррекции Концепции развития СИТО<sub>св</sub> и системы стандартов телеметрии, а также в одобрении или отклонении НИР, инициируемых этими предприятиями/организациями, относящихся к развитию СИТО<sub>св</sub> и/или Концепции и системы стандартов телеметрии [4]. Показаны [1] (рис. 3) необходимые действия по созданию, поддержанию и развитию вышеупомянутых концепции и стандартов. Порядок формирования рабочей группы «СИТО<sub>св</sub>», регламент её работы и порядок её финансирования должны быть отражены в её Уставе.

Ожидается, что через Рабочую Группу «СИТО<sub>св</sub>» будет проводиться эффективная единая политика развития отечественных СИТО<sub>св</sub>, обеспечивающая согласованные действия разных подразделений разных предприятий/организаций, решающих задачи, относящиеся к СИТО<sub>св</sub>. Для обеспечения вышеупомянутой согласованности не требуется (что очень важно!) дополнительных организационно-штатных структур в составе предприятий/организаций, перераспределения их функциональных обязанностей. Фактически существующие в РКО производственные отношения не претерпевают изменений.

Кроме того, экспертов Рабочей Группы «СИТО<sub>св</sub>» целесообразно использовать для подготовки решений, обеспечивающих регулирование цен за выполнение НИР/ОКР. Это позволит устранить противоречия, касающиеся цели функционирования предприятий/организаций РКО (получение максимальной прибыли) и мотивирования их действий по улучшению общих (обобщённых) показателей усовершенствования СИТО<sub>св</sub>.

При выработке организационно-технических мер по развитию отечественных СИТО<sub>св</sub> целесообразно использовать опыт CCSDS.



**Рис. 3. Схема, иллюстрирующая действия по созданию, поддержанию и развитию концепции развития СИТОСВ и системы стандартов телеметрии**

### **Опыт CCSDS в разработке системы стандартов телеметрии для отечественных СИТО<sub>СВ</sub>**

В контексте настоящей работы актуален опыт CCSDS (CCSDS — Consultative Committee for Space Data Systems — Консультативный Комитет по космическим системам передачи данных), касающийся экспериментальных результатов, представленных в Оранжевых Книгах CCSDS (см., например, [14]<sup>8</sup>).

Экспериментальная работа CCSDS основана на «предполагаемых» требованиях. В процессе её выполнения возможно изучение перспективы или демонстрация технической исполнимости в ожидании «жесткого» требования, которое еще не появилось. Аналогичная работа в отечественной практике могла бы выполняться в ходе НИОКР. Обычно Оранжевые Книги трансформируют в Синие или Пурпурные Книги (рекомендации и лучшие практики CCSDS, соответственно), в качестве примера см. LDPC-кодирование<sup>9, 10</sup>. По правилам, до публикации Синей Книги CCSDS должны существовать по крайней мере два аппаратных или программных прототипа (или другое исполнение), которые демонстрируют и осуществляют все опции и особенности специфика-

ции в оперативно уместной среде (или реальной, или моделируемой), причём реализованные разными космическими агентствами. Другими словами, до формулирования тех или иных положений отечественных стандартов телеметрии необходима более чем однократная реализация (*апробирование*) соответствующих технических решений, причём независимыми исполнителями, например, в ходе выполнения НИОКР.

Из опыта CCSDS следует, что при формулировании положений отечественных стандартов нужно рассматривать *апробированные* элементы СИТО<sub>СВ</sub> (т. е. существующие элементы или те, по которым принято решение о внедрении). Поэтому начать разработку системы стандартов телеметрии для СИТО<sub>СВ</sub> целесообразно с элементов, связанных с широко применяемыми в настоящее время в практике отработки средств выведения БРТС типа «Орбита» и БРС-4. Такой подход позволит добиться следующего:

- получить необходимый опыт разработки отечественных стандартов для СИТО<sub>СВ</sub>;
- прекратить внедрение БРТС и ПТС ТК нестандартных разработок, значительно ухудшающее эффективность процесса развития СИТО<sub>СВ</sub> (особенно в условиях подготовки к решению новых задач ИТО).

### **Заключение**

По результатам анализа возможностей адаптации процесса развития отечественных систем информационно-телеметрического обеспечения отработки средств выведения к сложившимся производственным отношениям сформулированы следующие выводы.

<sup>8</sup> Low Density Parity Check codes for Use in Near-Earth and Deep Space Applications, Research and Development for Space Data System Standards CCSDS 131.1-O-1, Issue 1, Orange Book, Consultative Committee for Space Data Systems, August 2006.

<sup>9</sup> Low Density Parity Check codes for Use in Near-Earth and Deep Space Applications, Research and Development for Space Data System Standards CCSDS 131.1-O-1, Issue 1, Orange Book, Consultative Committee for Space Data Systems, August 2006.

<sup>10</sup> TM Synchronization and Channel Coding, Recommended Standard CCSDS 131.0-B-2, Issue 2, Blue Book, Consultative Committee for Space Data Systems, August 2011.



1. Разработанное научно-методическое обеспечение процесса развития СИТО<sub>св</sub> ориентировано на *существенное* уменьшение потерь ТМИ, на построение компактного телеметрического комплекса космодрома, инвариантного к изменяющимся задачам ИТО и с возможностью подключения внешних по отношению к нему ПТС (т. е. на улучшение качества ИТО отработки средств выведения в целом, на получение искомого результата). Его целесообразно принять за основу, чтобы без кардинальных изменений производственных отношений предприятий/организаций (РКО и вне РКО) консолидировать усилия для перехода от существующего уровня развития *средств* ИТО на более высокий уровень.

2. Разработанное научно-методическое обеспечение отражает научно-технические и организационно-технические аспекты развития СИТО<sub>св</sub>. Научно-технические аспекты связаны с содержанием стратегий операций усовершенствования СИТО<sub>св</sub>, обеспечивающих управление избыточностью данных телеизмерений, определяющих, какие элементы СИТО<sub>св</sub> и каким образом будут улучшены, чтобы в итоге обеспечить требуемые (заданные) общие (обобщённые) показатели, характеризующие качество ИТО в целом. Организационно-технические аспекты связаны с целенаправленными действиями по построению, поддержанию и развитию официальной Концепции развития СИТО<sub>св</sub>, соответствующей ей *системы* стандартов телеметрии и Устава Рабочей Группы «СИТО<sub>св</sub>», а также по реализации содержащихся в них требований. Результативность действий Рабочей Группы «СИТО<sub>св</sub>» во многом опреде-

ляется результативностью научно-технических и организационно-технических мер по развитию отечественных СИТО<sub>св</sub>.

3. Решению о внедрении какого-либо элемента в состав СИТО<sub>св</sub> должно предшествовать его *апробирование*. Необходим обновлённый механизм отбора и реализации ценных для развития СИТО<sub>св</sub> предложений, поступающих от заинтересованных предприятий/организаций. Предложенный порядок построения и применения *системы* стандартов для СИТО<sub>св</sub> таков: замысел — НИР — ОКР — положения стандартов — практическое их использование. Положения стандартов должны отражать *апробированные* решения, *существенно* улучшающие общие (обобщённые) показатели и (соответственно) качество ИТО в целом. Они должны соответствовать Концепции развития СИТО<sub>св</sub>.

4. Разработанное научно-методическое обеспечение актуально в существующих условиях острой потребности в консолидации усилий разных предприятий/организаций ГК «Роскосмос», Министерства обороны Российской Федерации и других заинтересованных (в том числе частных) предприятий/организаций, находящихся вне РКО, а также в условиях неочевидности сущностей рациональных стратегий развития СИТО<sub>св</sub> и отсутствия необходимого механизма отбора и реализации ценных для развития СИТО<sub>св</sub> предложений. Его целесообразно использовать в качестве научно-методической основы, прежде всего при формировании положений Концепции развития СИТО<sub>св</sub>, *системы* стандартов телеметрии и Устава Рабочей Группы «СИТО<sub>св</sub>».

## Литература

1. Воронцов В.Л. Система информационно-телеметрического обеспечения отработки средств выведения. Стратегии усовершенствования и применения. М. : Горячая линия — Телеком, 2021. 236 с.
2. Воронцов В.Л., Давыдов И.А., Тишкин Р.В. Совершенствование информационно-телеметрического обеспечения отработки средств выведения стандартизацией и унификацией структур телеметрической информации // Правовая информатика. 2026. № 1. С. 68—84.
3. Воронцов В.Л., Давыдов И.А. Научно-технические и организационно-технические аспекты управления развитием отечественных систем информационно-телеметрического обеспечения отработки средств выведения // Информация и Космос. 2024. № 4. С. 170—181.
4. Воронцов В.Л., Давыдов И.А. Регламентирование процесса развития систем информационно-телеметрического обеспечения отработки средств выведения // Ракетно-космическое приборостроение и информационные системы. 2021. Т. 8. Вып. 2. С. 43—50.
5. Воронцов В.Л. Управление развитием систем информационно-телеметрического обеспечения отработки средств выведения в условиях влияния подрывных технологий // Лесной вестник. 2023. Т. 27. № 6. С. 160—177.
6. Губайдуллин И.Р., Мамедов Т.Т., Климов Д.И. Адаптивное конфигурирование информационно-телеметрической системы. В сб.: Информационно-управляющие и измерительные системы — 2021. Материалы XIV отрасл. науч.-тех. конф. приборостроительных организаций Госкорпорации «Роскосмос», посвященной 55-летию образования АО «НПО ИТ» (22 апреля 2021 г.). М. : 2021. С. 168.
7. Шошин А.В., Мухин А.В., Шошин И.А. Состояние и основные направления развития телеметрических систем испытательных полигонов. В сб.: Информационно-управляющие и измерительные системы — 2021. Материалы XIV отрасл. науч.-тех. конф. приборостроительных организаций Госкорпорации «Роскосмос», посвященной 55-летию образования АО «НПО ИТ» (22 апреля 2021 г.). М. : 2021. С. 183—190.



8. Богданов С.А., Коновалов В.П., Мурашов А.А. Требования к информационно-телеметрическому обеспечению контроля выведения многоспутниковых низкоорбитальных космических систем. В сб.: Информационно-управляющие и измерительные системы — 2023. Материалы отрасл. науч.-тех. конф. приборостроительных организаций Госкорпорации «Роскосмос», посвященной 60-летию полёта первой женщины-космонавта В.В.Терешковой (20 апреля 2023 г.). М. : 2023. С. 51—59.
9. Бердников С.М., Гончарук А.Н., Ковзалова А.А. Перспективы использования авиационных средств вертолётного типа в качестве ретранслятора радиосигнала при проведении лётных испытаний ракетной техники. В сб.: Информационно-управляющие и измерительные системы — 2023. Материалы отрасл. науч.-тех. конф. приборостроительных организаций Госкорпорации «Роскосмос», посвященной 60-летию полёта первой женщины-космонавта В.В.Терешковой (20 апреля 2023 г.). М. : 2023. С. 180—185.
10. Коновалов В.П., Мурашов А.А., Ващенко И.И., Чаплинский В.С. Развитие отечественной телеметрии от первых пусков ракет и космических аппаратов. В сб.: Информационно-управляющие и измерительные системы — 2023. Материалы отрасл. науч.-тех. конф. приборостроительных организаций Госкорпорации «Роскосмос», посвященной 60-летию полёта первой женщины-космонавта В.В.Терешковой (20 апреля 2023 г.). М. : 2023. С. 186—193.
11. Таланов А.А., Федотов С.А. Пути развития наземной космической инфраструктуры // Ракетно-космическое приборостроение и информационные технологии. 2023. Сборник трудов XI Всерос. науч.-тех. конф. «Актуальные проблемы ракетно-космического приборостроения и информационных технологий» (6—8 июня 2023 г.) / Под ред. д.т.н., проф. А.В. Круглова. М. : АО «Российские космические системы», 2023. С. 236—245.
12. Мальцев Г.Н., Якимов В.Л. Подход к формированию обобщенных параметров технического состояния сложных технических систем с использованием нейросетевых структур // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23. № 4. С. 828—835.
13. Вандышева О. «Менять придётся чуть более чем всё!»: Алексей Чадаев о причинах технологического лидерства Запада // БизнесOnline. URL: <https://www.business-gazeta.ru/article/567396> (дата обращения: 05.11.2024).
14. Correlated Data Generation, Research and Development for Space Data System Standards CCSDS 551.1-O-2, Issue 2, Orange Book, Consultative Committee for Space Data Systems, August 2020.

#### SECTION:

SYSTEM ANALYSIS, MANAGEMENT, ARTIFICIAL INTELLIGENCE, AND INFORMATION PROTECTION

## DEVELOPMENT OF DOMESTIC INFORMATION AND TELEMETRY SUPPORT SYSTEMS FOR LAUNCH VEHICLE IN THE CONTEXT OF THE EXISTING PRODUCTION RELATIONS

Vorontsov V.L.<sup>11</sup>

**Keywords:** concept, cosmodrome telemetry complex, enterprise, method, organization, regulatory tools, scientific and methodological support, software and hardware tools, standards, strategy, system, telemetered object, telemetry information.

#### Abstract

**Purpose of the paper:** recommendations for adapting the development process of domestic information and telemetry support systems for the testing of launch vehicle components to the existing production relations.

**Methods used:** systematic and expert analysis of publications, conceptual modeling, knowledge systematization.

**Results:** Based on an analysis of the possibilities for adapting the development process of domestic Information and Telemetry Support Systems for Launch Vehicle development (ITSSLV) to the existing production relations, recommendations have been formulated. It is recommended to use the developed scientific and methodological support for the development of ITSSLV as a scientific and methodological basis; this support reflects the scientific, technical, and organizational-technical aspects and, accordingly, makes it possible to create regulatory tools and methods for their application to solve practical tasks related to the development of ITSSLV, without the need to change the existing production relations. The essence of the updated

---

<sup>11</sup> **Valery L. Vorontsov**, Ph.D. (Technology), Leading Research Engineer at JSC “Russian Space Systems”, Moscow, Russian Federation.  
E-mail: [a762642@yandex.ru](mailto:a762642@yandex.ru)

*mechanism for selecting and implementing valuable proposals for the development of ITSSLV, which come from interested enterprises/organizations, is demonstrated. This is relevant in the current conditions, given the urgent need to consolidate efforts.*

**Practical value:** *The obtained results can be used to develop measures to improve the management of the development of domestic ITSSLV by using the developed scientific and methodological support for the development of ITSSLV, as a scientific and methodological foundation.*

## References

1. Vorontsov V.L. Sistema informatsionno-telemetricheskogo obespecheniia otrabotki sredstv vyvedeniia. Strategii usovershenstvovaniia i primeneniia. M. : Goriachaia liniia — Telekom, 2021. 236 s.
2. Vorontsov V.L., Davydov I.A., Tishkin R.V. Sovershenstvovanie informatsionno-telemetricheskogo obespecheniia otrabotki sredstv vyvedeniia standartizatsiei i unifikatsiei struktur telemetricheskoi informatsii // Pravovaia informatika. 2026. No. 1. S. 68—84.
3. Vorontsov V.L., Davydov I.A. Nauchno-tekhicheskie i organizatsionno-tekhicheskie aspekty upravleniia razvitiem otechestvennykh sistem informatsionno-telemetricheskogo obespecheniia otrabotki sredstv vyvedeniia // Informatsiia i Kosmos. 2024. No. 4. S. 170—181.
4. Vorontsov V.L., Davydov I.A. Reglamentirovanie protsessa razvitiia sistem informatsionno-telemetricheskogo obespecheniia otrabotki sredstv vyvedeniia // Raketno-kosmicheskoe priborostroenie i informatsionnye sistemy. 2021. T. 8. Vyp. 2. S. 43—50.
5. Vorontsov V.L. Upravlenie razvitiem sistem informatsionno-telemetricheskogo obespecheniia otrabotki sredstv vyvedeniia v usloviakh vliianiia podryvnykh tekhnologii // Lesnoi vestnik. 2023. T. 27. No. 6. S. 160—177.
6. Gubaidullin I.R., Mamedov T.T., Klimov D.I. Adaptivnoe konfigurirovanie informatsionno-telemetricheskoi sistemy. V sb.: Informatsionno-upravliaiushchie i izmeritel'nye sistemy — 2021. Materialy XIV otrasl. nauch.-tekhn. konf. priborostroitel'nykh organizatsii Goskorporatsii "Roskosmos", posviashchennoi 55-letiiu obrazovaniia AO "NPO IT" (22 apreliia 2021 g.). M. : 2021. S. 168.
7. Shoshin A.V., Mukhin A.V., Shoshin I.A. Sostoianie i osnovnye napravleniia razvitiia telemetricheskikh sistem ispytatel'nykh poligonov. V sb.: Informatsionno-upravliaiushchie i izmeritel'nye sistemy — 2021. Materialy XIV otrasl. nauch.-tekhn. konf. priborostroitel'nykh organizatsii Goskorporatsii "Roskosmos", posviashchennoi 55-letiiu obrazovaniia AO "NPO IT" (22 apreliia 2021 g.). M. : 2021. S. 183—190.
8. Bogdanov S.A., Konovalov V.P., Murashov A.A. Trebovaniia k informatsionno-telemetricheskoiu obespecheniiu kontroliia vyvedeniia mnogospurnikovykh nizkoorbital'nykh kosmicheskikh sistem. V sb.: Informatsionno-upravliaiushchie i izmeritel'nye sistemy — 2023. Materialy otrasl. nauch.-tekhn. konf. priborostroitel'nykh organizatsii Goskorporatsii "Roskosmos", posviashchennoi 60-letiiu poleta pervoi zhenshchiny-kosmonavta V.V.Tereshkovoi (20 apreliia 2023 g.). M. : 2023. S. 51—59.
9. Berdnikov S.M., Goncharuk A.N., Kovzalova A.A. Perspektivy ispol'zovaniia aviatsionnykh sredstv vertoletnogo tipa v kachestve retransliatora radiosignala pri provedenii letnykh ispytaniia raketnoi tekhniki. V sb.: Informatsionno-upravliaiushchie i izmeritel'nye sistemy — 2023. Materialy otrasl. nauch.-tekhn. konf. priborostroitel'nykh organizatsii Goskorporatsii "Roskosmos", posviashchennoi 60-letiiu poleta pervoi zhenshchiny-kosmonavta V.V.Tereshkovoi (20 apreliia 2023 g.). M. : 2023. S. 180—185.
10. Konovalov V.P., Murashov A.A., Vashchenko I.I., Chaplinskii V.S. Razvitie otechestvennoi telemetrii ot pervykh puskov raket i kosmicheskikh apparatov. V sb.: Informatsionno-upravliaiushchie i izmeritel'nye sistemy — 2023. Materialy otrasl. nauch.-tekhn. konf. priborostroitel'nykh organizatsii Goskorporatsii "Roskosmos", posviashchennoi 60-letiiu poleta pervoi zhenshchiny-kosmonavta V.V.Tereshkovoi (20 apreliia 2023 g.). M. : 2023. S. 186—193.
11. Talanov A.A., Fedotov S.A. Puti razvitiia nazemnoi kosmicheskoi infrastruktury // Raketno-kosmicheskoe priborostroenie i informatsionnye tekhnologii. 2023. Sbornik trudov XI Vseros. nauch.-tekhn. konf. "Aktual'nye problemy raketno-kosmicheskogo priborostroeniia i informatsionnykh tekhnologii" (6—8 iunია 2023 g.) / Pod red. d.t.n., prof. A.V. Kruglova. M. : AO "Rossiiskie kosmicheskie sistemy", 2023. S. 236—245.
12. Mal'tsev G.N., Iakimov V.L. Podkhod k formirovaniu obobshchennykh parametrov tekhnicheskogo sostoiianiia slozhnykh tekhnicheskikh sistem s ispol'zovaniem neirosetevykh struktur // Nauchno-tekhicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki. 2023. T. 23. No. 4. S. 828—835.
13. Vandysheva O. "Meniat' pridetsia chut' bolee chem vse!": Aleksei Chadaev o prichinakh tekhnologicheskogo liderstva Zapada // BiznesOnline. URL: <https://www.business-gazeta.ru/article/567396> (data obrashcheniia: 05.11.2024).
14. Correlated Data Generation, Research and Development for Space Data System Standards CCSDS 551.1-O-2, Issue 2, Orange Book, Consultative Committee for Space Data Systems, August 2020.



# БАЗА ЗНАНИЙ В СИСТЕМЕ РАССЛЕДОВАНИЯ АВАРИЙ И ИНЦИДЕНТОВ НА ПРОИЗВОДСТВЕННЫХ ОБЪЕКТАХ

Маркарян А.О.<sup>1</sup>, Поляховская О.А.<sup>2</sup>, Якубовская Ю.А.<sup>3</sup>

**Ключевые слова:** информационная система, расследование, формализация знаний, база данных, правила обработки данных, обработка естественного языка, регулярные выражения, Lakehouse-архитектура, промышленная безопасность, цифровизация.

## Аннотация

**Цель работы:** разработка базы знаний — централизованной системы хранения и автоматизированной обработки данных для расследования причин аварий и инцидентов на производственных объектах, обеспечивающей единый доступ к гетерогенной информации и сокращение времени анализа аварий.

**Методы:** системный анализ процесса расследования и существующих информационных решений в области промышленной безопасности; математический аппарат теории множеств для построения формальной модели данных; методы обработки естественного языка и регулярные выражения для автоматизированного извлечения фактов из разнородных документов; проектирование Lakehouse-архитектуры и технологий для программной реализации системы.

**Результаты:** проведён анализ регламента расследования аварий и существующих информационных решений, выявивший необходимость разработки инструментария для централизованного хранения разнородных материалов расследования с автоматизированным извлечением фактов и расчётом нормативных показателей. Предложена концептуальная модель и осуществлена формализация знаний системы расследования: витрины данных, сущности, характеризующие предметную область, отношения между ними и правила прослеживаемого извлечения фактов из документов разных типов. Определена структура базы данных, предложен алгоритм её автоматизированного наполнения, предусматривающий маршрутизацию документов, применение специализированных парсеров и вычисление показателей по материалам расследования. Разработано программное обеспечение на основе Lakehouse-архитектуры, включая модуль обработки данных и панель администратора. Тестирование на материалах реального расследования показало точность извлечения фактов 91,5%, полноту 88,7%, полное совпадение расчётных показателей с ручным расчётом и сокращение времени формирования знаний по инциденту примерно на 97%.

DOI: 10.24412/1994-1404-2026-3-51-59

## Введение и постановка задачи

Производственные объекты — шахты, заводы и иные промышленные предприятия — играют ключевую роль в экономике страны, однако работа на них сопряжена с риском аварий и инцидентов, способных привести к человеческим жертвам, экологическим катастрофам и значительным экономическим потерям. Несмотря на ужесточение требований промышленной безопасности и модернизацию оборудования, аварийность на опасных производственных объектах

сохраняется: по сравнению с 2024 годом число аварий увеличивается, а число внеплановых проверок растёт; большинство аварий по-прежнему связано с неисправностью оборудования и человеческим фактором.

Ключевым инструментом предотвращения повторения инцидентов является качественное и оперативное расследование, направленное на установление цепочки событий и первопричины происшествия. Расследование на промышленном объекте регламентировано

<sup>1</sup> **Маркарян Анна Оганесовна**, кандидат технических наук, доцент, доцент кафедры автоматизированных систем управления НИТУ МИСИС, г. Москва, Российская Федерация. ORCID: 0009-0004-2181-2144.

E-mail: [anestrelle@gmail.com](mailto:anestrelle@gmail.com)

<sup>2</sup> **Поляховская Ольга Александровна**, студент кафедры автоматизированных систем управления НИТУ МИСИС, г. Москва, Российская Федерация. ORCID: 0009-0005-4053-6357.

E-mail: [plkhvskl@gmail.com](mailto:plkhvskl@gmail.com)

<sup>3</sup> **Якубовская Юлия Александровна**, студент кафедры автоматизированных систем управления НИТУ МИСИС, г. Москва, Российская Федерация. ORCID: 0009-0009-7196-0774.

E-mail: [yakuboyulia@gmail.com](mailto:yakuboyulia@gmail.com)

на федеральном уровне и сопровождается формированием комиссии, которая в сжатые сроки собирает и анализирует большой объём разнородной информации: показания датчиков, фото- и видеофиксацию, протоколы осмотра, опросы свидетелей, техническую документацию. На практике эта информация консолидируется вручную в виде текстовых отчётов и таблиц, что ведёт к потере контекста и причинно-следственных связей между событиями, субъективности интерпретации и задержкам в принятии решений. Накопленный опыт расследований сложно систематизировать и использовать для проактивного анализа рисков.

Анализ существующих информационных систем в данной области — зарубежной базы крупных промышленных аварий MHIDAS, отечественного автоматизированного рабочего места «БАЭ» для электроэнергетики, программного комплекса «1С: Охрана труда и промышленная безопасность» и европейской базы eMARS — показал, что ни одно из решений не обеспечивает единого централизованного хранения разнородных данных расследования с автоматическим извлечением фактов и расчётом нормативных показателей применительно к российским производственным объектам, что свидетельствует об актуальности создания такого инструментария.

Проблема расследования аварий рассматривается в научной литературе с разных сторон. Кузнецова Е.А. показывает эволюцию подходов к анализу аварий от линейных моделей до системных, многоуровневых [1], что подтверждается систематическим обзором Ahmadi Rad с соавторами, демонстрирующим превосходство методов системного мышления (STAMP, AcciMap, FRAM, HFACS) над традиционными линейными подходами [2]. Статистический анализ отраслевой аварийности (Стасева с соавторами [3]; Пигилова с соавторами [4]) указывает на устойчивые причины аварий — неисправность оборудования и человеческий фактор. Derdowski и Mathisen [5], а также Ванякин с соавторами [6] обращают внимание на то, что традиционные методики расследования не учитывают психосоциальные и организационные факторы и не успевают за усложнением современного производства. Adumene с соавторами предлагают адаптивную модель на основе таксономии HFACS-MA с байесовскими сетями для количественной оценки человеческого фактора в морских операциях с учётом динамики изменения производительности персонала и неопределённости операционной среды [7], а Климова с соавторами показывают ограниченность классических инструментов (анализ дерева отказов, FMEA, диаграммы Исикавы) при изолированном рассмотрении случаев [8].

Принципиально важной для настоящего исследования является работа Маркарян А.О., предложившей концептуальную модель системы поддержки принятия решений при расследовании авиационных происшествий, включающую шесть специализированных подсистем и завершающий их работу блок хранения и систематизации сведений — базу знаний [9]. Настоя-

щее исследование развивает данное направление, фокусируясь на наполнении и структурной организации именно этого компонента применительно к расследованию аварий на производственных объектах. Архитектурные решения для подобных задач (клиент-серверная модель, разграничение пользователей, модульная организация) представлены в работе Шамина и Зеленко [10]. Вопрос выбора подхода к организации данных (Data Lake против Data Warehouse) рассмотрен Гунтупалли [11]; типовые атрибуты и классификаторы баз данных о техногенных чрезвычайных ситуациях в горнодобывающей отрасли выявлены Кудрявцевым с соавторами [12]. Sahoo с соавторами [13] и Karimi Dehkordi с соавторами [14] показывают эффективность методов машинного обучения и текстовой аналитики для извлечения цепочек событий и факторов риска из неструктурированных описаний инцидентов. Опыт агрегирования разнородных источников (телеметрия, дистанционное зондирование) представлен Ерошенко с соавторами [15]; Захаров с соавторами обосновывают применение протоколов IIoT и подхода ELT, при котором сырые данные сначала загружаются в хранилище, а затем трансформируются под конкретные аналитические задачи [16], что соответствует гибкой природе проектируемой базы знаний. Библиометрический обзор применения машинного обучения для анализа защитных барьеров [17], а также работы Rodriguez и Fernandez [18], Wang с соавторами [19], Thompson и Lee [20], Kumar и Singh [21] подтверждают актуальность внедрения интеллектуальных систем поддержки процесса расследования и важность интероперабельности между источниками данных. Наконец, Потеева с соавторами подчёркивают необходимость интеграции новой системы в общую информационную архитектуру предприятия, а не её изолированное существование [22]. Проведенный обзор подтвердил актуальность данного исследования, а также заложил основу для выбора технологий создания инструментария, позволяющего автоматизировать процесс извлечения значимых для расследования фактов из множества неструктурированной информации и организовать их хранение.

На основании этого поставлена цель исследования — разработать базу знаний системы расследования аварий и инцидентов на производственных объектах, включающую базу данных с фактами о происшествиях и правила автоматизированного извлечения фактов из гетерогенных источников. В результате должна быть создана централизованная система хранения и обработки данных, обеспечивающая единый доступ к гетерогенной информации и позволяющая сократить время анализа аварий и инцидентов.

Для достижения цели поставлены следующие задачи:

- 1) построение концептуальной модели;
- 2) формализация знаний системы расследования;
- 3) разработка архитектурно-технического решения и программного обеспечения;
- 4) анализ результатов тестирования на данных реального расследования.



### Концептуальная модель

База знаний представляет собой систему, объединяющую базу данных и логические правила автоматизированной обработки исходных материалов, преобразующих разрозненный документно-ориентированный процесс расследования в централизованную цифровую среду. В связи с этим структура разрабатываемой системы включает три компонента: централизованное хранилище (базу) данных; модуль обработки данных, осуществляющий автоматизированное извлечение фактов из разнородных документов и расчёт нормативных показателей; панель администратора для просмотра и ручного редактирования информации экспертами (рис. 1).

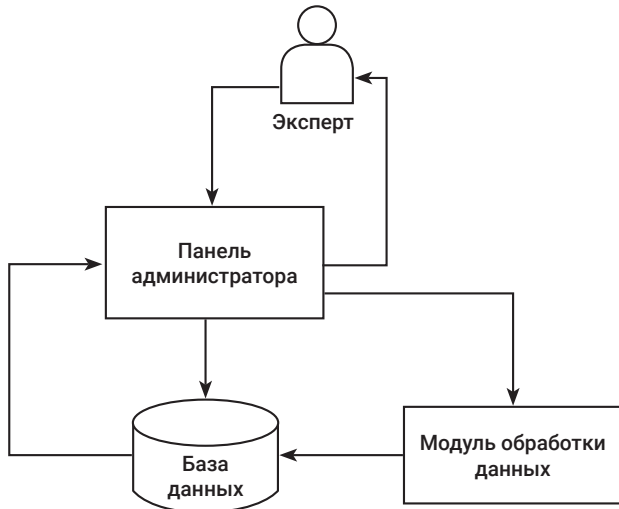


Рис. 1. Концептуальная модель системы

В свою очередь, модуль обработки данных декомпозирован на четыре подсистемы: загрузки и маршрутизации данных; извлечения фактов; вычисления расчётных показателей; хранения и доступа к данным (рис. 2). Такая реализация освобождает экспертов от рутинных операций по консолидации и расчётам, в которых возможна ошибка, и создаёт единую платформу, в которой накапливаются данные обо всех расследованных и расследуемых инцидентах. Ниже описаны формальные модели каждой из подсистем.

### Формализация знаний системы расследования

Пусть  $U = \{u_1, u_2, \dots, u_n\}$  — множество всех инцидентов, зарегистрированных в системе. Для каждого инцидента  $u_i$  определено множество его исходных материалов  $P(u_i) = \{p_1, \dots, p_{m_i}\}$ , которое разбивается на три непересекающихся подмножества:

$$P = P_{struct} \cup P_{unstruct} \cup P_{media} \quad (1)$$

где  $P_{struct}$  — формализованные материалы с чёткой структурой (акты осмотра, протоколы замеров, журналы технического обслуживания, паспорта оборудо-

вания);  $P_{unstruct}$  — неструктурированные текстовые материалы (транскрипции аудиозаписей, опросы свидетелей, объяснительные записки);  $P_{media}$  — медиа-файлы (графика, аудио, видео, чертежи), не подлежащие обработке.

Множество сущностей предметной области  $E$  объединяет 12 типов объектов, описывающих инцидент и его контекст: инцидент  $E_{inc}$ , предприятие  $E_{comp}$ , причастные сотрудники  $E_{empl}$ , оборудование  $E_{eq}$ , сертификаты соответствия  $E_{cert}$ , журналы технического обслуживания  $E_{maint}$ , локации (выработки и помещения)  $E_{loc}$ , датчики  $E_{sens}$ , геологические объекты  $E_{geo}$ , эксперты  $E_{exp}$ , сейсмические события  $E_{seis}$  и нормативные документы  $E_{reg}$ .

Дополнительно определены множества: извлечённых фактов  $F_{inc}$ , структурированное хранилище  $T$ , хранилище исходных файлов  $O$  и множество пользователей системы  $S$  с ролями  $\{admin, expert, viewer\}$ .

Каждый извлечённый факт  $\varphi \in F_{inc}$  представляется кортежем

$$\varphi = \langle e, attr, value, source \rangle \quad (2)$$

где  $e \in E$  — сущность предметной области;  $attr$  — атрибут сущности;  $value$  — извлечённое значение;  $source = p$  — ссылка на исходный документ, обеспечивающая полную прослеживаемость факта к материалу расследования. Множество фактов по инциденту  $u_i$  определяется объединением фактов по всем его материалам.

Работа подсистемы загрузки и маршрутизации основана на действии оператора  $\Gamma$ , определяющего тип загружаемого документа по расширению файла и наличию повторяющейся структуры:

$$\Gamma(p) = \begin{cases} structured, & \text{если } p \in P_{struct} \\ unstructured, & \text{если } p \in P_{unstruct} \\ media, & \text{если } p \in P_{media} \end{cases} \quad (3)$$

В подсистеме извлечения фактов функционируют три оператора, в зависимости от типа документа:

1) формализованные документы обрабатываются оператором  $\Psi_{regex}$  на основе множества регулярных шаблонов  $\Pi = \{\pi_1, \dots, \pi_k\}$ , где  $\pi_k = \langle pattern, group\_map, attr\_target \rangle$  — регулярное выражение с правилами сопоставления найденных фрагментов с атрибутами сущности:

$$\begin{aligned} \Psi_{regex}(p) &= \\ &= \bigcup_{\pi \in \Pi} \{ \langle attr, value \rangle \mid \exists match = \\ &= \pi.pattern(content(p)), value \\ &= extract(match, \pi.group\_map) \} \end{aligned} \quad (4)$$

Например, шаблон вида «(?:Тип|Модель):\s\*([A-Z0-9/\.-]+)» из текста «Модель: FS300/1.0» возвращает значение  $MODEL = \text{«FS300/1.0»}$ ; аналогичные шаблоны определены для заводского номера, года

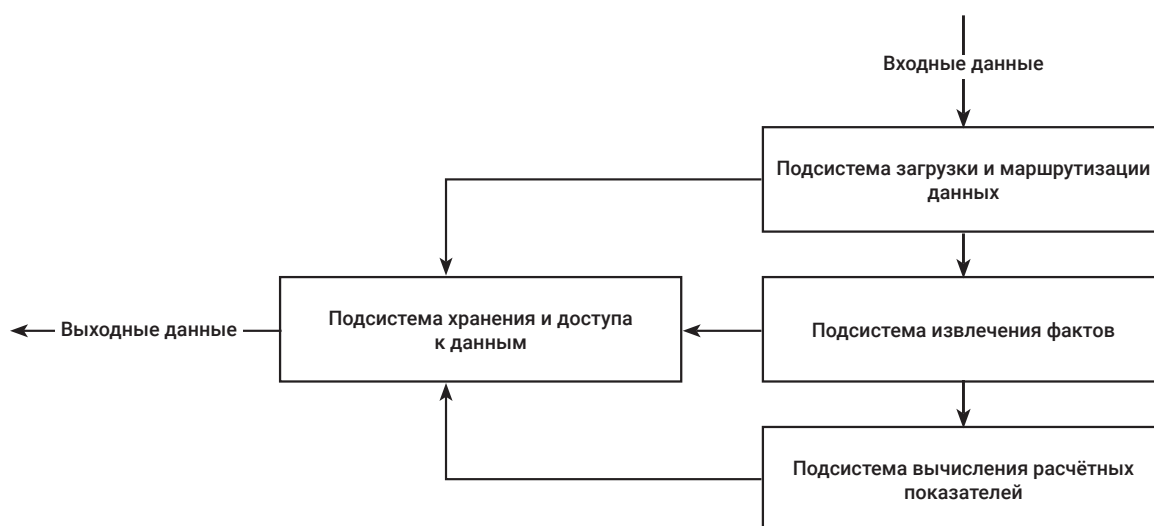


Рис. 2. Модуль обработки данных

выпуска, класса искробезопасности, технического состояния и места расположения оборудования.

2) неструктурированные тексты (транскрипции, опросы свидетелей) обрабатываются оператором

$$\Psi_{sem} = \theta_{NER} \circ \theta_{segm} \circ \theta_{token} \quad (5)$$

Он представляет собой композицию токенизации, сегментации на предложения и распознавания именованных сущностей типов PER (персоны), LOC (локации) и ORG (организации), с последующим применением семантических шаблонов, нацеленных на конкретные виды информации: имя опрашиваемого, дату и время опроса, ключевые события по словарю  $K_{events} = \{\text{взрыв, пожар, искра, задымление, обрушение, ...}\}$ . Так, в предложении «горный мастер Петров находился в лаве 512» распознаются сущности «Петров» → PER и «лава 512» → LOC.

3) медиафайлы обрабатываются оператором  $\Psi_{media}$ , фиксирующим только метаданные — имя, описание и ссылку на файл в хранилище.

Подсистема вычисления расчётных показателей построена по принципу действия оператора  $M$ , который на основе множества фактов  $F_{inc}$  вычисляет три группы показателей:

$$M : F_{inc} \rightarrow \{M_{inc}, M_{fire}, M_{vent}\} \quad (6)$$

Общие показатели инцидента  $M_{inc}$  включают суммарные потери (сумму погибших и пострадавших) и протяжённость зоны поражения. Вентиляционные показатели  $M_{vent}$  — относительный дефицит скорости воздуха  $\delta_v = \max(0, (v_{norm} - v_{fact}) / v_{norm} \times 100\%)$ , коэффициент утечек воздуха  $k_{leak} = (Q_{out} - Q_{in}) / Q_{in}$  и признак соответствия вентиляции нормам. Пожарные показатели  $M_{fire}$  вычисляются по R-коэффициентам диагностики эндогенных пожаров:

$$R_1 = \Delta O_2 / \Delta CO_2, R_2 = \Delta CO / \Delta O_2, R_3 = \Delta CO / \Delta CO_2 \quad (7)$$

где  $\Delta O_2$ ,  $\Delta CO_2$ ,  $\Delta CO$  — отклонения концентраций соответствующих газов в пробе воздуха от атмосферных

значений; при  $R_1 \geq R_{1crit} = 2,5$  фиксируется признак окислительного процесса. Дополнительно вычисляются эффективность дегазации и признак соответствия норме содержания негорючих веществ при оценке пылевзрывозащиты.

Подсистема хранения и доступа к данным предоставляет доступ пользователей  $c \in C$  к данным структурированного хранилища  $T$  посредством трех операторов: фильтрации  $\Omega_{filter}$  (запрос к таблице по заданным условиям),  $\Omega_{source}$  (переход от факта  $f$  к ссылке на исходный документ-источник) и CRUD (создание, чтение, обновление и удаление записей).

Полный цикл обработки информации об инциденте  $u_i$  представляет собой композицию операторов загрузки, маршрутизации, извлечения фактов, вычисления показателей и записи в хранилище:

$$Y_{total}(u_i) = \Delta_{load}(M(\bigcup_{p \in A_{load} P(u_i)} \Psi_{\Gamma(p)}(p))) \quad (8)$$

а база данных определяется как объединение структурированных представлений всех зарегистрированных инцидентов:

$$K = \bigcup_{i=1}^n S(u_i), \text{ где } S(u_i) = \langle E, F_{inc}, M(u_i) \rangle \quad (9)$$

### Архитектурно-техническое решение и программное обеспечение

Архитектурно-техническое решение строится вокруг трёх компонентов: централизованного хранилища данных, реализованного по принципу Lakehouse; модуля обработки входных данных; десктопного приложения панели администратора. Такое решение позволяет членам комиссии по расследованию, не имеющим глубоких навыков программирования, получать удобный графический инструмент для просмотра, добавления, изменения и удаления информации об инцидентах, в то время как расчётные показатели формируются автоматически модулем обработки данных.

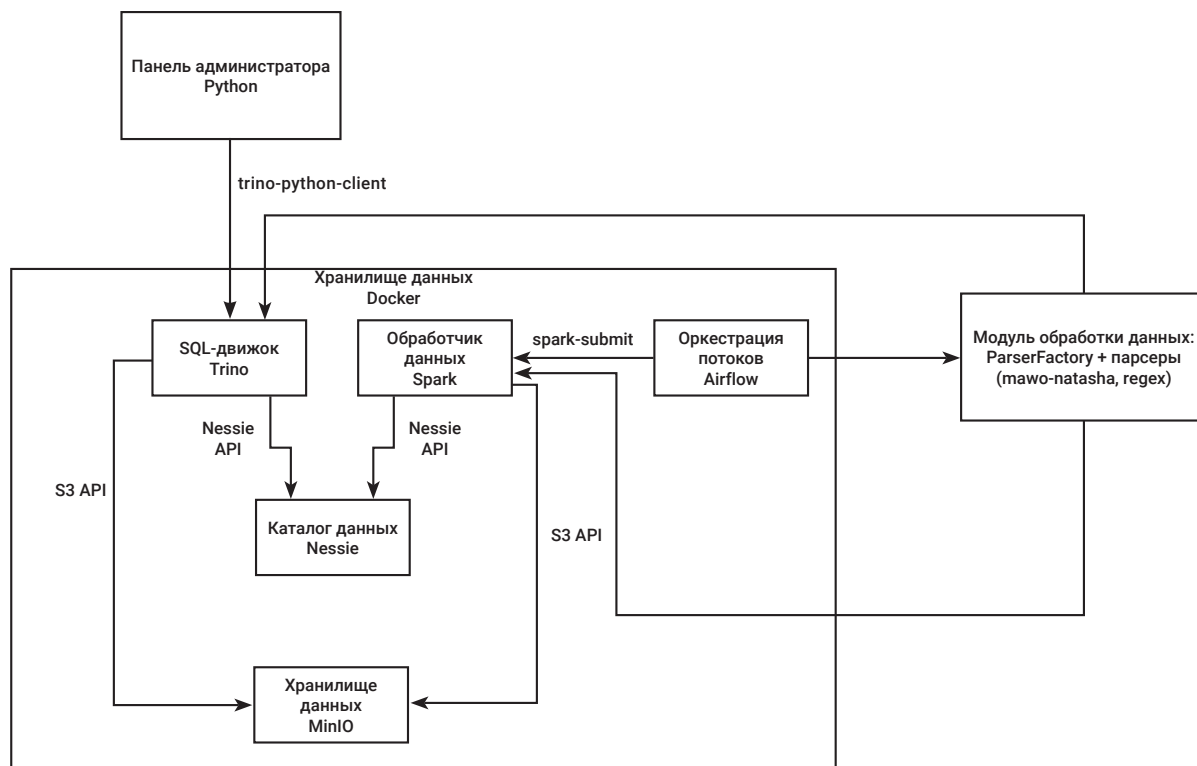


Рис. 3. Архитектурно-техническое решение

Хранилище данных, архитектура которого представлена на рис. 3, построено на трёх открытых технологиях. Объектное хранилище MinIO — S3-совместимое решение для размещения исходных файлов в их первоначальном виде и преобразованных данных в формате Apache Parquet. Распределённый SQL-движок Trino позволяет выполнять запросы к файлам Parquet непосредственно в MinIO без их предварительного перемещения, обеспечивая единый интерфейс доступа к хранилищу через JDBC/ODBC. Выбор архитектуры Lakehouse обусловлен необходимостью одновременной работы с разнородными типами данных — от структурированных таблиц до неструктурированных изображений и документов — при сохранении ACID-транзакций и эффективного выполнения аналитических запросов, что недостижимо при использовании классического Data Lake или Data Warehouse по отдельности. Структурированная часть хранилища организована в виде набора взаимосвязанных таблиц, отражающих ключевые сущности предметной области: инциденты, предприятия, сотрудники, оборудование, локации, документы, извлечённые факты, гипотезы и расчётные показатели. Связи между таблицами реализуют привязку фактов к конкретному инциденту и источнику данных, а также обеспечивают переход от сущностей к связанным документам и результатам расчётов.

Модуль обработки данных реализован как конвейер, оркестрируемый Apache Airflow. Обработка одного инцидента осуществляется по следующему алгоритму.

На вход подаётся множество исходных документов  $P(u_i)$  по инциденту  $u_i$ . Запускается цикл перебора

каждого документа  $p \in P(u_i)$ . Для текущего документа выполняется загрузка в объектное хранилище  $O$ , после чего срабатывает оператор маршрутизации  $G$ . Документ классифицируется как структурированный, неструктурированный текстовый или медийный.

Если документ признан структурированным, применяется оператор  $\Psi_{regex}$ , извлекающий факты на основе регулярных шаблонов. Если документ является неструктурированным текстом (транскрипции, опросы), применяется семантический конвейер  $\Psi_{sem}$ , включающий токенизацию, сегментацию и NER-распознавание сущностей типов PER, LOC, ORG, с последующим применением семантических шаблонов. Медийные файлы не обрабатываются автоматически; фиксируются только метаданные и ссылка для ручного анализа.

Все факты, извлечённые из текущего документа, добавляются в множество  $F_{inc}$ . Каждый факт представляется кортежем  $\varphi = \langle e, attr, value, source \rangle$ , где  $source$  — ссылка на исходный документ, обеспечивающая прослеживаемость. Цикл повторяется до обработки всех документов.

После завершения цикла на основе  $F_{inc}$  оператором  $M$  вычисляются три группы показателей:  $M_{inc}$ ,  $M_{vent}$ ,  $M_{fire}$ . Дополнительно рассчитываются показатели дегазации и пылевзрывозащиты.

Результаты объединяются в структурированное представление  $S(u_i)$  и записываются в хранилище  $T$ . Доступ пользователей  $C$  к данным реализован с помощью операторов фильтрации и CRUD с разграничением по ролям {admin, expert, viewer}. На этом алгоритм завершает свою работу.

Парсинг реализован по принципу фабрики парсеров (Parser Factory): для каждого типа документа создан специализированный парсер, наследующий общий базовый класс и переопределяющий метод разбора содержимого. Документ, не подходящий ни под одно правило маршрутизации, направляется в универсальный парсер, извлекающий ключевые слова для последующего анализа. Извлечённые записи вставляются в соответствующие таблицы хранилища пакетно. Расчётные показатели вычисляются отдельной задачей на движке Apache Spark, запускаемой по завершении загрузки данных.

Панель администратора реализована как десктопное приложение на языке Python с использованием библиотеки PyQt6, что обусловлено требованиями к автономности работы экспертов в защищённом контуре предприятия и возможностью локальной обработки больших объёмов данных без дополнительной нагрузки на серверную инфраструктуру.

Приложение подключается к хранилищу через Trino и предоставляет функции просмотра списка таблиц и их содержимого, выполнения произвольных SQL-запросов с сохранением истории, ручного редактирования значений ячеек, добавления и удаления записей с фиксацией факта удаления в истории изменений для обеспечения прозрачности процесса.

### Анализ результатов

Тестирование системы проведено на материалах расследования аварии на угольной шахте в 2023 году. Корпус включал 47 документов разных типов: акты осмотра, протоколы опросов, паспорта оборудования, журналы обслуживания, транскрипции аудиозаписей, результаты газового и воздушного анализа, сертификаты, сейсмические данные и мультимедийные материалы. Были проверены модуль загрузки и маршрутизации, парсеры извлечения фактов, модуль расчётных показателей, панель администратора и инфраструктурная часть решения.

Из 47 документов в хранилище загружено 45; два файла не обработаны из-за некорректной кодировки. Оператор маршрутизации корректно классифицировал все загруженные документы: формализованные материалы обрабатывались регулярными шаблонами, неструктурированные тексты — NLP-конвейером, медиафайлы — оператором регистрации метаданных. Среднее время обработки одного документа составило около 0,72 с.

На выборке из 10 документов проведена экспертная валидация извлечения фактов. Получено 86 верно извлечённых фактов, 8 ложных срабатываний и 11 пропусков, что соответствует точности 91,5%, полноте 88,7% и F1-мере 90,1%. Ошибки в основном связаны с нестандартными сокращениями и отдельными случаями неверной интерпретации числовых значений.

Сравнение результатов работы модуля расчётных показателей с ручным расчётом эксперта показало

полное совпадение по общим показателям инцидента. Для пожарных и вентиляционных показателей полученные значения также согласовались с выводами подкомиссий, что подтверждает корректность реализованных расчётных правил.

Функциональное тестирование панели администратора по сценариям просмотра данных, выполнения SQL-запросов, редактирования и удаления записей показало полное соответствие ожидаемому результату. Все проверяемые сценарии были отработаны успешно.

Ключевым эффектом внедрения системы является сокращение трудозатрат на формирование базы знаний по инциденту. При ручном подходе консолидация материалов, извлечение фактов, формирование хронологии и вычисление показателей занимают 8—12 часов. В предлагаемой системе автоматизируются все этапы, кроме первичного поиска и подготовки материалов, что сокращает время формирования базы знаний до 5—10 минут, то есть примерно на 97%.

К ограничениям решения относятся формирование словаря семантических шаблонов на материалах одного инцидента, фиксация для медиафайлов только метаданных без анализа содержимого и необходимость ручного формирования гипотез о причинах аварии. Перспективы развития связаны с расширением корпуса документов, интеграцией методов компьютерного зрения и автоматизацией ранжирования гипотез на основе накопленных данных.

### Выводы

В результате проведённого исследования разработана база знаний для расследования аварий и инцидентов на производственных объектах, обеспечивающая централизованное хранение и автоматизированную обработку данных из гетерогенных источников.

Разработанная математическая модель формального представления данных по инцидентам и реализация алгоритма их обработки позволяет унифицировать процесс извлечения знаний из неструктурированной информации, поступающей в процессе расследования аварии. Предложенная комбинация Lakehouse-архитектуры с модулем семантического анализа вносит вклад в методологию построения отраслевых экспертных систем.

На практике подтвердилась эффективность полученного решения, сократив время первичной обработки данных. Это позволяет ускорить рутинные процессы и заложить основу к системному подходу к расследованию аварий на производственных объектах.

Направления дальнейшего развития включают: расширение словаря семантических шаблонов на основе расширенного корпуса документов, интеграцию методов компьютерного зрения для извлечения фактов из медиаматериалов, автоматизацию ранжирования гипотез о причинах аварии на основе расчётных показателей и масштабирование базы знаний на множество инцидентов для последующего сравнительного анализа системных причин аварийности.



## **Литература**

1. Кузнецова Е.А. Столетняя история развития методов расследования несчастных случаев на производстве // Экономика, предпринимательство и право. 2021. Т. 11. № 1. С. 193—212.
2. Ahmadi Rad M., Lefsrud L., Hendry M.T. Application of systems thinking accident analysis methods: A review for railways // Safety Science. 2023. Vol. 160. P. 106066.
3. Стасева Е.В., Кузнецов С.Ю., Шаяхметов Р.Р., Идиятуллина З.Ф., Муллагалиев И.Р. Анализ характерных причин аварий и травматизма на объектах газоснабжения // Безопасность техногенных и природных систем. 2021. № 2. С. 2—7.
4. Пигилова Р.Н., Малышева Т.В., Аверьянова Ю.А., Филиппова Ф.М. Статистический анализ аварийности на производстве в результате некорректного функционирования системы энергообеспечения предприятия // Известия Самарского научного центра РАН. 2023. № 2 (112). С. 27—33.
5. Derdowski L.A., Mathisen G.E. Psychosocial factors and safety in high-risk industries: A systematic literature review // Safety Science. 2023. Vol. 157. P. 105948.
6. Ванякин О.В., Сухоруков В.В., Строилов И.А. Актуализация подхода к установлению причин возникновения аварий и инцидентов на опасных производственных объектах в условиях современной добычи и переработки (обогащения) полезных ископаемых // Уголь. 2026. № 2. С. 65—68.
7. Adumene S., Afenyo M., Salehi V., William P. An adaptive model for human factors assessment in maritime operations // International Journal of Industrial Ergonomics. 2022. Vol. 89. P. 103293.
8. Климова И.В., Сазанова Н.В., Махнева А.Н. Опыт проведения технического расследования аварии на опасном производственном объекте нефтепродуктообеспечения // Современные проблемы гражданской защиты. 2023. № 1(46). С. 93—102.
9. Маркарян А.О. Система поддержки принятия решений при расследовании авиационных происшествий // Труды МАИ. 2026. № 141.
10. Шамин Е.А., Зеленко Л.С. Разработка автоматизированного рабочего места следователя // Перспективные информационные технологии (ПИТ 2022): сб. тр. науч.-техн. конф. 2022. С. 95—97.
11. Guntupalli B. Data Lake vs. Data Warehouse: Choosing the Right Architecture // International Journal of Artificial Intelligence, Data Science, and Machine Learning. 2023. Vol. 4. № 4. P. 54—64.
12. Кудрявцев С., Емелин П., Козлов В. Анализ баз данных о техногенных чрезвычайных ситуациях в горнодобывающей отрасли // Механика және технологиялар. 2026. № 3 (89). С. 371—381.
13. Sahoo S., Mukane P., Maiti J., Tewari V.K. A framework for process risk assessment incorporating prior hazard information in text mining models using chunking // Process Safety and Environmental Protection. 2024. Vol. 189. P. 486—499.
14. Karimi Dehkordi M., Sattari F., Lefsrud L. Creating an incident investigation framework for a complex socio-technical system: Application of multi-label text classification and Bayesian network structure learning // Reliability Engineering and System Safety. 2025. Vol. 260.
15. Ерошенко С.А., Матренин П.В., Хальясмаа А.И., Клименко Д.Е., Сидорова А.В. Технология обработки данных для прогнозирования притока воды в водохранилище при использовании дистанционного зондирования Земли и сети метеорологических и гидрологических постов // Проблемы региональной энергетики. 2022. № 4 (56). С. 100—109.
16. Захаров В.Н., Клебанов Д.А., Макеев М.А., Радченко Д.Н. Анализ методов подготовки и преобразования информации, поступающей в хранилища данных для эффективного управления горнотехнической системой // Горный информационно-аналитический бюллетень. 2021. № 6. С. 120—135.
17. Machine learning-based literature review on the concept of safety barriers against hazardous events // Journal of Loss Prevention in the Process Industries. 2024. Vol. 92. P. 105470.
18. Rodriguez M., Fernandez A. Deep learning for accident report classification in high-risk industries // Safety Science. 2026. Vol. 165. P. 106210.
19. Wang H., Li J., Liu Y. Knowledge graph and machine learning for accident pattern recognition // Reliability Engineering and System Safety. 2024. Vol. 248. P. 110124.
20. Thompson M., Lee S. Interoperability in corporate safety management systems: A data integration framework // Journal of Safety Research. 2024. Vol. 90. P. 245—260.
21. Kumar A., Singh R. Implementation of investigation support systems in Indian manufacturing industries: Challenges and success factors // International Journal of Industrial Ergonomics. 2024. Vol. 99. P. 103512.
22. Потекаева Ю.В., Охотников И.В., Сибирко И.В. Формирование информационной архитектуры промышленного предприятия // Экономика: вчера, сегодня, завтра. 2021. Т. 11. № 8-1. С. 191—200.

# KNOWLEDGE BASE IN THE SYSTEM OF INVESTIGATING ACCIDENTS AND INCIDENTS AT INDUSTRIAL FACILITIES

Markarian A.O.<sup>4</sup>, Polyakhovskaya O.A.<sup>5</sup>, Yakubovskaya Yu.A.<sup>6</sup>

**Keywords:** information system, investigation, knowledge formalization, database, data processing rules, natural language processing, regular expressions, Lakehouse architecture, industrial safety, digitalization.

## Abstract

**Purpose of the study:** development of a knowledge base — a centralized system for storage and automated processing of data for investigating the causes of accidents and incidents at industrial facilities, providing unified access to heterogeneous information and reducing the time of accident analysis.

**Methods:** system analysis of the investigation process and existing information solutions in the field of industrial safety; mathematical apparatus of set theory for constructing a formal data model; natural language processing methods and regular expressions for automated fact extraction from heterogeneous documents; Lakehouse architecture design and technologies for software implementation of the system.

**Results:** an analysis of the accident investigation regulations and existing information solutions was conducted, revealing the need to develop a toolkit for centralized storage of heterogeneous investigation materials with automated fact extraction and calculation of regulatory indicators. A conceptual model was proposed and knowledge formalization of the investigation system was carried out: data marts, entities characterizing the subject area, relationships between them, and rules for traceable fact extraction from documents of various types. The database structure was defined, and an algorithm for its automated population was proposed, providing for document routing, application of specialized parsers, and calculation of indicators based on investigation materials. Software based on the Lakehouse architecture was developed, including a data processing module and an administrator panel. Testing on real investigation materials showed fact extraction precision of 91.5%, recall of 88.7%, complete coincidence of calculated indicators with manual calculations, and a reduction in the time of knowledge formation for an incident by approximately 97%.

## References

1. Kuznetsova E.A. Stoletniia istoriia razvitiia metodov rassledovaniia neschastnykh sluchaev na proizvodstve // *Ekonomika, predprinimatel'stvo i pravo*. 2021. T. 11. No. 1. S. 193—212.
2. Ahmadi Rad M., Lefsrud L., Hendry M.T. Application of systems thinking accident analysis methods: A review for railways // *Safety Science*. 2023. Vol. 160. P. 106066.
3. Staseva E.V., Kuznetsov S.Iu., Shaiakhmetov R.R., Idiatullina Z.F., Mullagaliev I.R. Analiz kharakternykh prichin aarii i travmatizma na ob'ektakh gazosnabzheniia // *Bezopasnost' tekhnogennykh i prirodnnykh sistem*. 2021. No. 2. S. 2—7.
4. Pigilova R.N., Malysheva T.V., Aver'ianova Iu.A., Filippova F.M. Statisticheskii analiz avariinosti na proizvodstve v rezul'tate nekorrektnogo funktsionirovaniia sistemy energoobespecheniia predpriiatiia // *Izvestiia Samarskogo nauchnogo tsentra RAN*. 2023. No. 2 (112). S. 27—33.
5. Derdowski L.A., Mathisen G.E. Psychosocial factors and safety in high-risk industries: A systematic literature review // *Safety Science*. 2023. Vol. 157. P. 105948.

<sup>4</sup> **Markarian Anna Ogenesovna**, Ph.D. (Technology), Associate Professor of the Department of Automated Control Systems, National University of Science and Technology MISIS, Moscow, Russian Federation. ORCID: 0009-0004-2181-2144.  
E-mail: [anestrelle@gmail.com](mailto:anestrelle@gmail.com)

<sup>5</sup> **Olga A. Polyakhovskaya**, Student, Automated Control Systems Department, National University of Science and Technology MISIS, Moscow, Russian Federation. ORCID: 0009-0005-4053-6357.  
E-mail: [plkhvskl@gmail.com](mailto:plkhvskl@gmail.com)

<sup>6</sup> **Yulia A. Yakubovskaya**, Student, Automated Control Systems Department, National University of Science and Technology MISIS, Moscow, Russian Federation. ORCID: 0009-0009-7196-0774.  
E-mail: [yakuboyulia@gmail.com](mailto:yakuboyulia@gmail.com)

6. Vaniakin O.V., Sukhorukov V.V., Stroilov I.A. Aktualizatsiia podkhoda k ustanovleniiu prichin vozniknoveniia avarii i intsidentov na opasnykh proizvodstvennykh ob"ektakh v usloviakh sovremennoi dobychi i pererabotki (obogashcheniia) poleznykh iskopaemykh // Ugol'. 2026. No. 2. S. 65—68.
7. Adumene S., Afenyo M., Salehi V., William P. An adaptive model for human factors assessment in maritime operations // International Journal of Industrial Ergonomics. 2022. Vol. 89. P. 103293.
8. Klimova I.V., Sazanova N.V., Makhneva A.N. Opyt provedeniia tekhnicheskogo rassledovaniia avarii na opasnom proizvodstvennom ob"ekte nefteproduktoobespecheniia // Sovremennye problemy grazhdanskoi zashchity. 2023. No. 1(46). S. 93—102.
9. Markarian A.O. Sistema podderzhki priniatiia reshenii pri rassledovanii aviatsionnykh proisshествii // Trudy MAI. 2026. No. 141.
10. Shamin E.A., Zelenko L.S. Razrabotka avtomatizirovannogo rabocheho mesta sledovatel'ia // Perspektivnye informat-sionnye tekhnologii (PIT 2022): sb. tr. nauch.-tekhn. konf. 2022. S. 95—97.
11. Guntupalli B. Data Lake vs. Data Warehouse: Choosing the Right Architecture // International Journal of Artificial Intelligence, Data Science, and Machine Learning. 2023. Vol. 4. No. 4. P. 54—64.
12. Kudriavtsev S., Emelin P., Kozlov V. Analiz baz dannykh o tekhnogennykh chrezvychainykh situatsiiakh v gornodobyvaishchei otrasli // Mekhanika zhāne tekhnologii. 2026. No. 3 (89). S. 371—381.
13. Sahoo S., Mukane P., Maiti J., Tewari V.K. A framework for process risk assessment incorporating prior hazard in-formation in text mining models using chunking // Process Safety and Environmental Protection. 2024. Vol. 189. P. 486—499.
14. Karimi Dehkordi M., Sattari F., Lefsrud L. Creating an incident investigation framework for a complex socio-technical system: Application of multi-label text classification and Bayesian network structure learning // Reliability Engineer-ing and System Safety. 2025. Vol. 260.
15. Eroshenko S.A., Matrenin P.V., Khal'iasmaa A.I., Klimenko D.E., Sidorova A.V. Tekhnologiya obrabotki dannykh dlia prognozirovaniia pritoka vody v vodokhranilishche pri ispol'zovanii distantsionnogo zondirovaniia Zemli i seti met-eorologicheskikh i gidrologicheskikh postov // Problemy regional'noi energetiki. 2022. No. 4 (56). S. 100—109.
16. Zakharov V.N., Klebanov D.A., Makeev M.A., Radchenko D.N. Analiz metodov podgotovki i preobrazovaniia informat-sii, postupaiushchei v khranilishcha dannykh dlia effektivnogo upravleniia gornotekhnicheskoi sistemoi // Gornyi informatsionno-analiticheskii biulleten'. 2021. No. 6. S. 120—135.
17. Machine learning-based literature review on the concept of safety barriers against hazardous events // Journal of Loss Prevention in the Process Industries. 2024. Vol. 92. P. 105470.
18. Rodriguez M., Fernandez A. Deep learning for accident report classification in high-risk industries // Safety Science. 2026. Vol. 165. P. 106210.
19. Wang H., Li J., Liu Y. Knowledge graph and machine learning for accident pattern recognition // Reliability Engineer-ing and System Safety. 2024. Vol. 248. P. 110124.
20. Thompson M., Lee S. Interoperability in corporate safety management systems: A data integration framework // Journal of Safety Research. 2024. Vol. 90. P. 245—260.
21. Kumar A., Singh R. Implementation of investigation support systems in Indian manufacturing industries: Challenges and success factors // International Journal of Industrial Ergonomics. 2024. Vol. 99. P. 103512.
22. Potekaeva Iu.V., Okhotnikov I.V., Sibirko I.V. Formirovanie informatsionnoi arkhitektury promyshlennogo predprii-atiia // Ekonomika: vchera, segodnia, zavtra. 2021. T. 11. No. 8-1. S. 191—200.



# ПОДХОД К РЕАЛИЗАЦИИ БЕЗОПАСНОГО УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ ИНФРАСТРУКТУР

Морозов Ф.А.<sup>1</sup>

**Ключевые слова:** брокеры сообщений, асинхронное взаимодействие, отказоустойчивость, обратный опрос, информационная безопасность, микросервисная архитектура, персистентные очереди, гарантии доставки, централизованный аудит.

## Аннотация

**Цель работы.** Анализ архитектурных ограничений существующих подходов к удалённому администрированию и разработка архитектурной модели защищённого механизма управления распределённой серверной инфраструктурой с гарантированной доставкой управляющих воздействий.

**Метод исследования.** В работе применены методы сравнительного анализа существующих систем удалённого администрирования, архитектурного моделирования и обобщения эксплуатационных характеристик программных решений. Рассмотрены синхронные и асинхронные модели взаимодействия, оценены их свойства в условиях сетевой сегментации и динамически изменяющегося состава узлов. Проведена систематизация требований к механизму администрирования с учётом критериев безопасности, масштабируемости и отказоустойчивости.

**Результаты исследования.** В ходе исследования обоснована целесообразность применения асинхронной архитектуры на основе брокера сообщений и модели обратного взаимодействия, при которой управляемые узлы иницируют соединение самостоятельно. Данный подход позволяет отказаться от организации входящих соединений к серверам и существенно сократить потенциальную атакующую поверхность распределённой инфраструктуры. Сформулирован формализованный подход к гарантированной доставке управляющих воздействий, учитывающий подтверждение получения, фиксацию исполнения и аудит операций. Предложенная модель описывает жизненный цикл команды через формально определённые состояния и переходы между ними, что обеспечивает сквозное отслеживание выполнения каждой операции. Полученные результаты позволяют снизить атакующую поверхность и обеспечить устойчивость механизма управления в условиях временной недоступности отдельных компонентов, что подтверждено экспериментальной апробацией разработанного прототипа.

DOI: 10.24412/1994-1404-2026-3-60-69

## Введение

Современные распределённые серверные инфраструктуры характеризуются высокой степенью территориальной и логической децентрализованности, использованием виртуализированных сред и сегментацией сетевого пространства. Такие условия предъявляют повышенные требования к механизмам удалённого администрирования, поскольку управление должно обеспечивать масштабируемость, устойчивость к сетевым ограничениям и соответствие требованиям информационной безопасности.

Традиционные синхронные модели управления предполагают установление соединения со стороны управляющего компонента к каждому узлу инфраструктуры. В распределённых средах с многоуровневой сег-

ментацией и динамически изменяющимся составом серверов подобный подход может сопровождаться усложнением контроля доступа и ростом числа входящих соединений. Это формирует необходимость поиска архитектурных решений, ориентированных на снижение атакующей поверхности и повышение устойчивости к временной недоступности узлов.

Дополнительной задачей является формализация критерия гарантированной доставки управляющего воздействия. В практических системах выполнение команды нередко трактуется как факт её отправки или получения подтверждения на уровне протокола, что не всегда отражает реальное завершение операции. Отсутствие формализованного описания жизненного

<sup>1</sup> Морозов Фёдор Андреевич, специалист отдела мониторинга и реагирования на киберугрозы ПАО «Ростелеком». E-mail: fedor-555m@yandex.ru



цикла команды затрудняет оценку корректности функционирования механизма управления.

В связи с этим в работе ставится задача разработки архитектурной модели защищённого механизма администрирования распределённой серверной инфраструктуры, обеспечивающего асинхронное взаимодействие, минимизацию входящих соединений и формализованную гарантированную доставку управляющих воздействий.

### **АНАЛИЗ ПОДХОДОВ К УПРАВЛЕНИЮ РАСПРЕДЕЛЁННЫМИ СЕРВЕРНЫМИ ИНФРАСТРУКТУРАМИ**

#### **Особенности управления распределёнными серверными средами**

Высокая территориальная и логическая распределённость современных серверных инфраструктур предъявляет дополнительные требования к управлению. Организации используют комбинацию локальных центров обработки данных, удалённых филиалов, виртуализированных платформ и облачных сервисов. Подобная архитектура позволяет повысить гибкость вычислительных ресурсов, обеспечить отказоустойчивость и адаптивность к изменяющимся нагрузкам, однако одновременно усложняет процессы администрирования.

Управление распределённой инфраструктурой предполагает координацию большого числа узлов, находящихся в различных сетевых сегментах и функционирующих в условиях неоднородных политик безопасности. В отличие от централизованных систем, где взаимодействие осуществляется в пределах единого доверенного контура, распределённая среда включает сегменты с различными уровнями доступа, сетевыми ограничениями и механизмами фильтрации трафика. Это накладывает ограничения на способы установления соединений и передачи управляющих воздействий.

Рост числа узлов прямо влияет на увеличение объёма административных операций: конфигурация программного обеспечения, обновление компонентов, контроль состояния сервисов, аудит действий и реагирование на инциденты. При использовании традиционных методов удалённого доступа увеличение масштаба приводит к росту числа активных сетевых соединений и усложнению контроля доступа, что повышает требования к управляемости и безопасности.

Дополнительным фактором является динамичность инфраструктуры. Виртуальные машины и контейнеры могут создаваться и удаляться автоматически, изменяться в процессе масштабирования или миграции между площадками. В таких условиях управление должно учитывать изменимость состава узлов и обеспечивать устойчивость к временной недоступности отдельных компонентов.

Таким образом, распределённость, сегментация и динамичность формируют совокупность ограничений, при которых традиционные синхронные модели администрирования могут демонстрировать снижение эффективности. Это обуславливает необходимость анализа архитектурных подходов, ориентированных на масштабируемость, асинхронность взаимодействия и снижение атакующей поверхности.

#### **Архитектурные факторы, влияющие на процессы администрирования**

Архитектура распределённой инфраструктуры, как правило, включает несколько уровней: центральные вычислительные ресурсы, периферийные узлы, облачные сегменты и изолированные подсети, предназначенные для размещения специализированных сервисов. Между сегментами применяются механизмы фильтрации трафика, разграничения доступа и контроля соединений.

Наличие сетевой сегментации является объективным требованием информационной безопасности. Однако с точки зрения администрирования это означает, что прямое установление входящих соединений к управляемым узлам может быть ограничено политиками межсетевых экранов или требованиями изоляции. В результате классическая модель, при которой управляющий сервер инициирует соединение к каждому узлу, становится менее универсальной.

Кроме того, различие в уровнях доверия между сегментами требует строгого контроля аутентификации и авторизации. Административные учётные записи должны использоваться в минимально необходимом объёме, а сами управляющие воздействия — протоколироваться и контролироваться. При увеличении числа узлов централизованный контроль за множеством прямых подключений усложняется.

Виртуализация и контейнеризация усиливают динамический характер инфраструктуры. Узлы могут временно отсутствовать в сети, находиться за трансляцией адресов или быть доступными только через промежуточные компоненты. В подобных условиях синхронное выполнение команд, предполагающее немедленный отклик, не всегда отражает фактическое состояние системы. В связи с этим, как отмечено в [1], асинхронное взаимодействие с использованием брокеров сообщений является ключевым средством для решения недостатков синхронных вызовов, таких как каскадные сбои и высокие задержки.

Таким образом, архитектурные особенности распределённой среды ограничивают применение моделей, основанных исключительно на постоянной доступности управляемых узлов и прямом сетевом взаимодействии. Это требует рассмотрения альтернативных схем обмена управляющими сообщениями, способных функционировать в условиях сегментации и временной недоступности отдельных компонентов.

### Сравнительный анализ существующих подходов к удалённому администрированию

На практике применяются несколько классов решений для управления серверной инфраструктурой.

Первый класс — прямые методы удалённого доступа, основанные на использовании протоколов интерактивного подключения. Их достоинством является простота реализации и оперативность выполнения задач. Однако при увеличении числа узлов возрастает количество открытых сервисов и входящих соединений, что увеличивает требования к контролю доступа и мониторингу безопасности. В условиях распределённой сегментированной сети такие методы могут требовать дополнительной настройки маршрутизации и политик фильтрации.

Второй класс — системы управления конфигурациями, ориентированные на автоматизацию развёртывания и поддержания заданного состояния узлов. Они обеспечивают централизованное описание конфигурации и позволяют выполнять массовые операции. При этом эффективность их применения зависит от сетевой доступности управляемых компонентов и корректности механизма доставки задач. В ряде сценариев выполнение операций предполагает наличие постоянного соединения между управляющим компонентом и узлами.

Третий класс — решения, использующие брокеры сообщений и асинхронную модель взаимодействия. В данной схеме узлы самостоятельно инициируют соединение к централизованному компоненту обмена сообщениями и получают задания через очереди или каналы подписки. Такой подход позволяет сократить количество входящих соединений к управляемым узлам и адаптироваться к временной недоступности отдельных сегментов. Асинхронный характер взаимодействия упрощает масштабирование и балансировку нагрузки. Как подтверждают исследования [2, 3], использование брокеров сообщений (например, Kafka,

RabbitMQ) способствует повышению отказоустойчивости и масштабируемости систем за счёт внедрения событийно-ориентированной архитектуры (EDA) и асинхронной обработки данных.

Сравнительный анализ показывает, что каждый подход имеет преимущества и ограничения в условиях высокой распределённости. Прямые методы оперативны, но требуют множества входящих соединений. Системы управления конфигурациями эффективны для поддержания состояния, однако зависят от сетевой топологии. Решения на основе брокеров сообщений гибки и асинхронны, но требуют формализации подтверждения выполнения задач.

Таким образом, ни один из подходов в изолированном виде не гарантирует одновременное выполнение требований масштабируемости, безопасности и подтверждённой доставки управляющих воздействий. Это указывает на необходимость формализации критериев корректности управления и уточнения требований к механизму доставки команд.

Для более наглядного сопоставления рассмотренных подходов проведём их сравнительный анализ по ряду обобщённых критериев, отражающих требования распределённой серверной инфраструктуры.

Результаты сравнительного анализа представлены в таблице 1.

### Обобщённые требования к механизму администрирования

На основании проведённого анализа можно сформулировать совокупность требований к механизму управления распределённой инфраструктурой.

В контексте безопасности механизм должен минимизировать количество входящих соединений к управляемым узлам и обеспечивать строгую аутентификацию участников взаимодействия. Необходимо предусмотреть разграничение прав доступа и фиксацию административных действий в журнале аудита.

Таблица 1

Сравнительный анализ подходов к администрированию

| Критерий                                     | Прямые методы удалённого доступа         | Системы управления конфигурациями       | Решения на основе брокеров сообщений              |
|----------------------------------------------|------------------------------------------|-----------------------------------------|---------------------------------------------------|
| Инициирование соединения                     | Со стороны управляющего узла             | Чаще со стороны управляющего узла       | Со стороны управляемого узла                      |
| Требования к входящим подключениям           | Наличие открытых сервисов на каждом узле | Зависит от архитектуры решения          | Минимальные, используется исходящее соединение    |
| Масштабируемость                             | Ограничена ростом числа соединений       | Поддерживается средствами автоматизации | Обеспечивается асинхронной моделью                |
| Устойчивость к временной недоступности узлов | Низкая, требуется повторное подключение  | Частично обеспечивается                 | Поддерживается механизмами очередей               |
| Подтверждение выполнения операции            | Обычно на уровне сессии                  | На уровне выполнения задания            | Может быть формализовано на уровне сообщений      |
| Централизованный аудит                       | Требует дополнительной интеграции        | Реализуется средствами системы          | Может быть встроен в механизм обработки сообщений |

В отношении доставки управляющих воздействий требуется определить формальный критерий завершённости операции. Отправка команды сама по себе не может рассматриваться как достаточное условие её выполнения. Механизм должен обеспечивать подтверждение получения, фиксацию результата исполнения и сохранение информации о состоянии операции.

С позиции масштабируемости система должна поддерживать увеличение числа узлов без пропорционального роста сложности управления. Это предполагает использование архитектурных решений, допускающих горизонтальное масштабирование и асинхронный обмен сообщениями.

Обеспечение отказоустойчивости требует сохранения корректности функционирования при временной недоступности отдельных компонентов. Управляющие воздействия не должны теряться при кратковременных сбоях связи, что может быть обеспечено за счёт применения паттернов отказоустойчивости и гарантий доставки, описанных в [2, 3].

Наконец, важным требованием является централизованный аудит, позволяющий отслеживать последовательность административных операций и обеспечивать воспроизводимость состояния системы.

Формирование указанных требований задаёт направление дальнейшего проектирования и обосновывает необходимость разработки модели, в которой процесс управления будет описан через формально определённые состояния и переходы.

## **ОБОСНОВАНИЕ АРХИТЕКТУРНЫХ РЕШЕНИЙ И ВЫБОРА ТЕХНОЛОГИЙ**

### **Анализ существующих решений и технологических подходов**

Для обоснования архитектуры разработанного механизма проведён анализ распространённых инструментов удалённого администрирования и средств

межсервисного взаимодействия с точки зрения их применимости в распределённых средах.

Прямые методы удалённого доступа обеспечивают оперативность выполнения задач, однако при масштабировании инфраструктуры увеличивается количество активных соединений и усложняется централизованный контроль доступа и аудит. Их эффективность снижается в условиях сегментированных сетей и динамически изменяющегося состава узлов.

Системы управления конфигурациями ориентированы на автоматизацию поддержания заданного состояния серверов. Они повышают управляемость инфраструктуры, однако архитектурные особенности отдельных решений предполагают зависимость от сетевой доступности узлов или периодического опроса агентов. В динамичных средах это может приводить к задержкам выполнения операций.

Отдельный класс решений представляют брокеры сообщений, обеспечивающие асинхронную доставку данных между компонентами системы [4]. Такие инструменты не являются средствами администрирования в готовом виде, однако предоставляют механизмы подтверждения получения сообщений, буферизации и устойчивости к временной недоступности участников взаимодействия.

Для более детального анализа возможностей различных архитектурных подходов рассмотрим их функциональные характеристики в контексте задач удалённого администрирования, как показано в таблице 2.

Проведённый анализ показывает, что решения на основе асинхронного обмена сообщениями в наибольшей степени соответствуют требованиям распределённой среды, однако требуют архитектурной надстройки, ориентированной на задачи администрирования. Как показано в [5], использование имитационного моделирования процессов обработки сообщений с применением брокеров позволяет оценить производительность распределённых систем ещё на этапе проектирования.

Таблица 2

Сопоставление архитектурных подходов

| Критерий                              | Прямые методы доступа (SSH)                 | Системы управления конфигурациями                  | Подход на базе брокера сообщений                     |
|---------------------------------------|---------------------------------------------|----------------------------------------------------|------------------------------------------------------|
| Гибкость выполнения команд            | Произвольные команды в интерактивном режиме | Выполнение заранее описанных сценариев             | Передача произвольных команд через очередь сообщений |
| Поддержка отложенного выполнения      | Отсутствует                                 | Ограниченно поддерживается средствами планирования | Поддерживается за счёт хранения сообщений в очередях |
| Контроль корректности команд          | Отсутствует                                 | Проверка структуры сценариев                       | Может быть реализован на уровне обработки сообщений  |
| Управление на основе метаданных узлов | Отсутствует                                 | Используются группы и инвентари                    | Требуется дополнительный механизм тегирования        |
| Централизованный аудит операций       | Ограничен журналами соединений              | Поддерживается средствами системы                  | Требуется реализации на уровне управляющего сервиса  |

### Обоснование архитектуры на основе асинхронного обмена сообщениями

Предлагаемая архитектура основана на сочетании микросервисного подхода и механизма асинхронного взаимодействия через брокера сообщений.

Ключевым принципом является модель обратного взаимодействия, при которой управляемые узлы самостоятельно инициируют соединение с компонентом обмена сообщениями и получают управляющие воздействия через выделенные каналы. Это позволяет отказать от организации входящих соединений к серверам и сократить атаковую поверхность.

Архитектура включает три логически разделённых компонента: сервер управления, реализующий прикладную логику и интерфейс взаимодействия; компонент маршрутизации, обеспечивающий распределение команд; агенты выполнения, осуществляющие обработку задач на узлах инфраструктуры.

Асинхронный обмен через брокера сообщений обеспечивает буферизацию команд и подтверждение их обработки. При временной недоступности узла управляющее воздействие сохраняется до момента восстановления соединения. Как показано в [6], такой подход позволяет формализовать жизненный цикл команды и определить критерий её завершённости.

Альтернативные архитектурные решения, основанные на монолитной структуре или прямом межсервисном взаимодействии, обладают меньшей гибкостью масштабирования и требуют дополнительных механизмов повторной передачи данных. Использование брокера сообщений обеспечивает баланс между структурной простотой и устойчивостью к отказам.

### Обоснование выбора технологического стека

Выбор технологий осуществлялся исходя из требований к масштабируемости, безопасности и сопровождаемости системы.

В качестве архитектурной основы использован микросервисный подход, обеспечивающий разделение ответственности и независимое масштабирование компонентов.

Для реализации серверной части выбран язык Python, позволяющий использовать асинхронную модель обработки запросов и развитую экосистему библиотек для сетевого взаимодействия. Применение современного веб-фреймворка обеспечивает реализацию REST-интерфейса и унифицированного механизма интеграции с внешними системами.

В качестве брокера сообщений использован инструмент, поддерживающий подтверждение получения сообщений и механизмы их сохранения. Это позволяет реализовать гарантированную доставку управляющих воздействий и обеспечить устойчивость к кратковременным сбоям связи.

Для хранения данных применена реляционная система управления базами данных с поддержкой тран-

закционности и репликации. Как показано в [7], применение архитектурного паттерна отказоустойчивого взаимодействия с брокерами сообщений (ограничение интенсивности запросов, обработка ошибок) обеспечивает гарантированную доставку управляющих воздействий и устойчивость к сбоям связи.

Выбранный стек ориентирован на использование зрелых и поддерживаемых технологий, что снижает риски внедрения и обеспечивает возможность дальнейшего развития системы.

### Формирование требований к реализации

На основании проведённого анализа сформулированы требования к реализации механизма администрирования.

Система должна обеспечивать централизованное управление узлами распределённой инфраструктуры без необходимости открытия входящих портов на управляемых серверах. Необходимо реализовать механизм разграничения доступа, журналирование действий и формализованный контроль выполнения команд.

Функционально система должна поддерживать регистрацию агентов, адресное и групповое выполнение команд, хранение истории операций и интеграцию с внешними сервисами через программный интерфейс.

Архитектурно требуется поддержка горизонтального масштабирования, асинхронной обработки сообщений и устойчивости к временной недоступности отдельных компонентов.

Эксплуатационные требования включают совместимость с гетерогенными средами, минимальные зависимости на стороне агента и возможность интеграции с существующими средствами мониторинга и управления.

Сформулированные требования определяют рамки дальнейшего проектирования и обеспечивают согласованность между архитектурными решениями и целями разработки.

### ПРОЕКТИРОВАНИЕ, РЕАЛИЗАЦИЯ И АПРОБАЦИЯ МЕХАНИЗМА АДМИНИСТРИРОВАНИЯ

#### Архитектурная модель и функциональные возможности системы

Для реализации защищённого механизма администрирования распределённой серверной инфраструктуры была разработана архитектура программного комплекса, основанная на микросервисном подходе и асинхронной модели взаимодействия компонентов. Основной задачей проектирования являлось создание системы, обеспечивающей безопасное централизованное управление серверами, гарантированную доставку управляющих воздействий и устойчивость к сетевым ограничениям распределённой инфраструктуры.

Архитектура системы включает три основных компонента: центральный сервер управления, сервис



маршрутизации команд и программный агент, устанавливаемый на управляемых узлах. Взаимодействие компонентов осуществляется через брокера сообщений, обеспечивающий асинхронную передачу управляющих команд и результатов их выполнения. Хранение состояния системы и истории операций осуществляется в реляционной базе данных.

Ключевой особенностью архитектуры является использование механизма **обратного опроса**. В отличие от традиционных систем администрирования, где управляющий сервер инициирует соединение с управляемыми узлами, в предложенном решении инициатором взаимодействия выступает агент. Управляемые серверы самостоятельно устанавливают соединение с брокером сообщений и получают команды из персональных очередей. Такой подход позволяет исключить необходимость открытия входящих сетевых портов на управляемых серверах и снижает потенциальную атакующую поверхность системы.

На рис. 1 представлена схема взаимодействия компонентов системы.

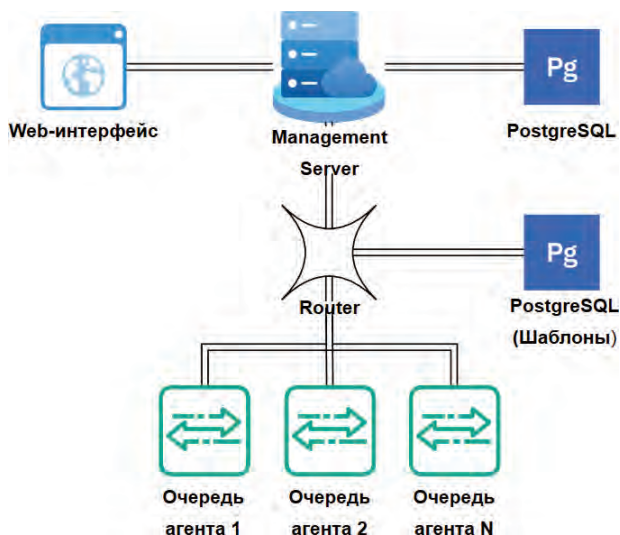


**Рис. 1. Схема взаимодействия компонентов системы**

Предложенная архитектура обеспечивает реализацию следующих функциональных возможностей:

- централизованное управление инфраструктурой, позволяющее выполнять административные операции на множестве серверов из единой точки управления;
- выполнение команд на группах серверов, формируемых динамически на основе метаданных управляемых узлов;
- система шаблонов команд, обеспечивающая создание параметризованных сценариев администрирования и повторное использование типовых операций;
- динамическое таргетирование серверов, позволяющее автоматически определять целевые узлы на основе заданных критериев;

- журналирование и аудит операций, фиксирующие историю всех выполненных административных действий;
- мониторинг состояния серверов, включая сбор базовых метрик и контроль активности агентов.

Одним из ключевых требований к системе являлось обеспечение гарантированной доставки управляющих воздействий. Для решения данной задачи используется брокер сообщений с поддержкой персистентных очередей и механизмов подтверждения обработки сообщений. Сравнительный анализ производительности RabbitMQ и Kafka [8] демонстрирует, что выбор конкретного брокера зависит от требований к пропускной способности и задержкам, что было учтено при проектировании архитектуры. Такой подход позволяет сохранять команды в очереди до момента их успешного выполнения агентом.

Асинхронная модель взаимодействия обеспечивает устойчивость системы к временной недоступности отдельных компонентов. При разрыве соединения команды сохраняются в очереди сообщений и выполняются после восстановления связи с агентом.

Предложенная архитектура обеспечивает модульность системы, независимость компонентов и возможность масштабирования при увеличении количества управляемых серверов.

### **Реализация ключевых механизмов администрирования**

В ходе реализации программного комплекса были разработаны основные механизмы управления распределённой инфраструктурой.

Ключевым элементом системы является механизм обратного опроса, обеспечивающий безопасное подключение управляемых серверов. Каждый агент при запуске автоматически регистрируется в системе и создаёт персональную очередь команд в брокере сообщений. Далее агент периодически проверяет свою очередь и получает новые задачи.

Использование брокера сообщений позволяет реализовать гарантированную доставку команд [9]. Для этого применяются персистентные очереди и подтверждение обработки сообщений. В случае временной недоступности узла команда сохраняется в очереди и будет выполнена после восстановления соединения.

В системе реализована возможность динамического таргетирования серверов. Каждый агент может иметь набор метаданных (тегов), характеризующих его назначение, роль или расположение. При отправке команды пользователь может указать фильтр по тегам, после чего система автоматически определяет набор целевых серверов.

Дополнительной функцией является система шаблонов команд, позволяющая создавать параметризованные сценарии администрирования. Шаблон представляет собой описание команды с переменными параметрами, которые подставляются при выполнении

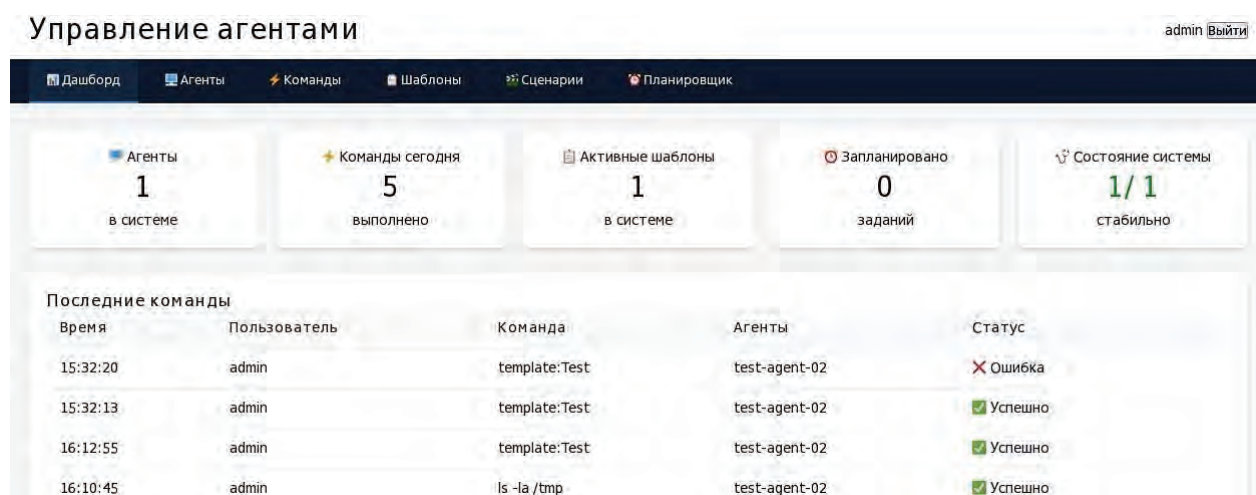


Рис. 2. Главный дашборд системы

операции. Такой подход позволяет стандартизировать типовые операции и снизить вероятность ошибок администратора.

Для предотвращения ошибочных действий реализован механизм валидации команд. Перед отправкой команда проверяется на наличие потенциально опасных операций и опечаток. Это позволяет уменьшить вероятность случайного выполнения критических команд.

Также в системе реализована подсистема аудита и мониторинга, включающая:

- журнал всех выполненных операций;
- историю выполнения команд;
- мониторинг состояния агентов;
- сбор метрик ресурсов серверов.

Интерфейс системы обеспечивает централизованное управление инфраструктурой и визуализацию состояния серверов. На рис. 2 показан главный дашборд системы, предоставляющий сводную информацию о состоянии инфраструктуры.

Использование централизованного интерфейса позволяет администратору получать сводную информацию о состоянии инфраструктуры и контролировать выполнение операций управления.

### Апробация прототипа и оценка эффективности решения

Для проверки работоспособности разработанного механизма был развернут тестовый стенд, включающий:

- одну виртуальную машину для центральных компонентов системы;
- две виртуальные машины, выступающие в роли агентов.

Использование компактного тестового стенда является распространённой практикой тестирования распределённых систем, поскольку позволяет проверить функциональные возможности системы на минимальной конфигурации с последующей экстраполяцией результатов на более крупные инфраструктуры.

В ходе тестирования проверялись следующие сценарии:

- регистрация и управление агентами;
- выполнение команд на отдельных серверах;
- выполнение команд на группах серверов;
- работа системы шаблонов;
- механизмы безопасности и аутентификации;
- отказоустойчивость системы.

Сравнительный анализ брокеров сообщений (RabbitMQ, Kafka, NATS) по задержке доставки и пропускной способности [10] обосновывает выбор архитектуры для высоконагруженных систем.

Основные временные характеристики выполнения операций представлены в таблице 3.

Таблица 3

### Временные характеристики выполнения операций

| Операция                                            | Минимальное время | Среднее время | Максимальное время |
|-----------------------------------------------------|-------------------|---------------|--------------------|
| Проверка нагрузки (uptime)                          | 10 мс             | 24 мс         | 35 мс              |
| Проверка состояния служб (ps aux   grep -c «nginx») | 12 мс             | 21 мс         | 40 мс              |
| Обновление состояния                                | 8 с               | 12 с          | 15 с               |

Дополнительно была проведена проверка механизмов безопасности системы. Результаты тестирования представлены в таблице 4.

Проведённый анализ показал, что разработанная система обеспечивает стабильную работу при типовых нагрузках и демонстрирует устойчивость к одиночным сбоям компонентов.

Сравнительный анализ с традиционными подходами администрирования представлен в таблице 5.

Таблица 4

**Эффективность механизмов безопасности**

| Механизм безопасности         | Тестовых сценариев | Успешно обработано | Эффективность |
|-------------------------------|--------------------|--------------------|---------------|
| Валидация опасных команд      | 45                 | 44                 | 97.8%         |
| Обнаружение опечаток          | 35                 | 33                 | 94.3%         |
| Доставка команд после разрыва | 25                 | 24                 | 96.0%         |

Таблица 5

**Сравнение подходов к администрированию**

| Критерий                    | Разработанная система                               | Ansible                     | Прямой SSH               |
|-----------------------------|-----------------------------------------------------|-----------------------------|--------------------------|
| Безопасность                | Обратный опрос                                      | Прямые соединения           | Открытые порты           |
| Доставка команд             | Персистентные очереди                               | Требует доступности узлов   | Нет механизма            |
| Централизованное управление | Единый Web-интерфейс<br>Динамическое таргетирование | CLI & Статические инвентари | Разрозненные подключения |
| Мониторинг                  | Встроенная система здоровья                         | Требует доп. средств        | Отсутствует              |

Полученные результаты демонстрируют преимущества предложенной архитектуры в аспектах безопасности, централизованного управления и устойчивости к сбоям.

**Выводы**

В ходе исследования разработан механизм безопасного удалённого администрирования распределённых серверных инфраструктур, основанный на асинхронной модели взаимодействия с использованием брокера сообщений и принципа обратного опроса управляемых узлов. Предложенный подход позволяет минимизировать количество входящих сетевых соединений, что снижает потенциальную атаковую поверхность инфраструктуры, и обеспечивает гарантированную доставку управляющих воздействий за счёт применения персистентных очередей и механизмов подтверждения обработки сообщений. Научная новизна работы

заключается в формализации жизненного цикла команды и критерия её завершенности, что позволяет однозначно интерпретировать состояние выполнения административных операций в условиях временной недоступности отдельных компонентов распределённой системы.

Достоверность предложенных решений подтверждена экспериментальной апробацией разработанного прототипа на тестовом стенде. В ходе тестирования подтверждена работоспособность ключевых механизмов: валидации опасных команд, обнаружения опечаток и доставки команд после разрыва связи, что свидетельствует о практической применимости разработанного подхода. Полученные результаты позволяют использовать предложенную архитектуру в качестве основы для построения систем централизованного управления распределённой инфраструктурой, обеспечивающих безопасность, масштабируемость и отказоустойчивость.

**Литература**

1. Баженов А.Э., Райков А.В., Нехаев М.В., Ореховский Н.В. Оптимизация взаимодействия микросервисов с использованием асинхронных вызовов и брокеров сообщений (Kafka, RabbitMQ) // Программные системы и вычислительные методы. 2025. № 4. С. 77—92.

2. Барабанов П.П. Исследование паттернов отказоустойчивости и гарантий доставки для высоконагруженного обмена пользовательскими метриками // Актуальные исследования. 2026. №9 (295). Ч. I. С. 26—30.

3. Сухов Д.Д., Еленев Д.В., Муравьева Е.В. Исследование методов обмена данными с помощью брокеров сообщений // Минобрнауки России, Самар. нац. исслед. ун-т им. С.П. Королева. Самара, 2025.

4. Агеев А.Е. Разработка архитектурного паттерна для отказоустойчивого взаимодействия высоконагруженных приложений с брокерами сообщений // Сборник тезисов докладов конгресса молодых ученых. СПб. : Университет ИТМО. 2025.

5. Паринов П.А., Сирота А.А. Моделирование процессов обработки сообщений в системах с микросервисной архитектурой с использованием брокера сообщений // Системный анализ и информационные технологии. 2025. № 3. С. 15—28.
6. Макаров П.С. Исследование эффективности брокеров сообщений в высоконагруженных распределённых системах // Студенческий электронный научный журнал. 2025. № 18 (314).
7. Карпович М.Н. Особенности проектирования микросервисно-событийных архитектур для высоконагруженных распределённых систем обработки информации // Труды БГТУ. Серия 3: Физико-математические науки и информатика. 2023. № 1 (266). С. 89—95.
8. Kamiński F., Kłonica R., Pańczyk B. Comparative Performance Analysis of RabbitMQ and Kafka Message Queue Systems in Spring Boot and ASP.NET Environments // Journal of Computer Sciences Institute. 2025. Vol. 37. P. 457—462. DOI: 10.35784/jcsi.7977.
9. Селезнёв А.И., Селезнёв И.Л. Брокеры сообщений в системах обработки данных // Молодой ученый. 2025. № 46 (597).
10. Зарубин В.А. Построение событийно-ориентированной архитектуры в системе кредитного скоринга // Молодежь и современные информационные технологии : сб. тр. XXII Межд. науч.-практ. конф., 15—17 апреля 2025 г., Томск. Томск : Изд-во ТПУ, 2025. С. 477—481.

SECTION:

SYSTEM ANALYSIS, MANAGEMENT, ARTIFICIAL INTELLIGENCE, AND INFORMATION PROTECTION

## A SECURE REMOTE ADMINISTRATION APPROACH FOR DISTRIBUTED COMPUTING INFRASTRUCTURES

Morozov F.A.<sup>2</sup>

**Keywords:** message brokers, asynchronous communication, fault tolerance, reverse polling, information security, microservice architecture, persistent queues, delivery guarantees, centralized audit.

### Abstract

**Objective.** The aim of the research is to analyze architectural limitations of existing approaches to remote administration and to develop an architectural model of a secure management mechanism for distributed server infrastructure with guaranteed delivery of control actions.

**Methods.** The research employs methods of comparative analysis of existing remote administration systems, architectural modeling, and generalization of operational characteristics of software solutions. Synchronous and asynchronous interaction models are considered; their properties are evaluated under conditions of network segmentation and dynamically changing node composition. The requirements for the administration mechanism are systematized considering security, scalability, and fault tolerance criteria.

**Results.** This study substantiates the feasibility of using an asynchronous architecture based on a message broker and a reverse communication model, in which controlled nodes initiate connections independently. This approach eliminates the need for incoming connections to servers and significantly reduces the potential attack surface of a distributed infrastructure. A formalized approach to guaranteed delivery of control actions is formulated, taking into account confirmation of receipt, execution logging, and operation auditing. The proposed model describes the command lifecycle through formally defined states and transitions between them, ensuring end-to-end tracking of each operation. The obtained results reduce the attack surface and ensure the resilience of the control mechanism under conditions of temporary unavailability of individual components, as confirmed by experimental validation of the developed prototype.

---

<sup>2</sup> **Fedor A. Morozov**, Specialist, Cyber Threat Monitoring and Response Department, PJSC Rostelecom.  
E-mail: [fedor-555m@yandex.ru](mailto:fedor-555m@yandex.ru)



## References

1. Bazhenov A.E., Raikov A.V., Nekhaev M.V., Orekhovskii N.V. Optimizatsiia vzaimodeistviia mikroservisov s ispol'zovaniem asinkhronnykh vyzovov i brokerov soobshchenii (Kafka, RabbitMQ) // Programmnye sistemy i vychislitel'nye metody. 2025. No. 4. S. 77—92.
2. Barabanov P.P. Issledovanie patternov otkazoustoichivosti i garantii dostavki dlia vysokonagruzhennogo obmena pol'zovatel'skimi metrikami // Aktual'nye issledovaniia. 2026. No.9 (295). Ch. I. S. 26—30.
3. Sukhov D.D., Elenov D.V., Murav'eva E.V. Issledovanie metodov obmena dannymi s pomoshch'iu brokerov soobshchenii // Minobrnauki Rossii, Samar. nats. issled. un-t im. S.P. Koroleva. Samara, 2025.
4. Ageev A.E. Razrabotka arkhitekturnogo patterna dlia otkazoustoichivogo vzaimodeistviia vysokonagruzhennykh prilozhenii s brokerami soobshchenii // Sbornik tezisev dokladov kongressa molodykh uchenykh. SPb. : Universitet ITMO. 2025.
5. Parinov P.A., Sirota A.A. Modelirovanie protsessov obrabotki soobshchenii v sistemakh s mikroservisnoi arkhitekturoi s ispol'zovaniem brokera soobshchenii // Sistemnyi analiz i informatsionnye tekhnologii. 2025. No. 3. S. 15—28.
6. Makarov P.S. Issledovanie effektivnosti brokerov soobshchenii v vysokonagruzhennykh raspredelennykh sistemakh // Studencheskii elektronnyi nauchnyi zhurnal. 2025. No. 18 (314).
7. Karpovich M.N. Osobennosti proektirovaniia mikroservisno-sobytiinykh arkhitektur dlia vysokonagruzhennykh raspredelennykh sistem obrabotki informatsii // Trudy BGTU. Seriiia 3: Fiziko-matematicheskie nauki i informatika. 2023. No. 1 (266). S. 89—95.
8. Kamiński F., Kłonica R., Pańczyk B. Comparative Performance Analysis of RabbitMQ and Kafka Message Queue Systems in Spring Boot and ASP.NET Environments // Journal of Computer Sciences Institute. 2025. Vol. 37. P. 457—462. DOI: 10.35784/jcsi.7977.
9. Seleznev A.I., Seleznev I.L. Brokery soobshchenii v sistemakh obrabotki dannykh // Molodoi uchenyi. 2025. No. 46 (597).
10. Zarubin V.A. Postroenie sobytiino-orientirovannoi arkhitektury v sisteme kreditnogo skoringa // Molodezh' i sovremennye informatsionnye tekhnologii : sb. tr. XXII Mezhd. nauch.-prakt. konf., 15—17 apreliia 2025 g., Tomsk. Tomsk : Izd-vo TPU, 2025. S. 477—481.



# АНАЛИЗ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ МОНИТОРИНГА ОБСТАНОВКИ И ПРОГРАММНЫХ КОМПЛЕКСОВ МОДЕЛИРОВАНИЯ ПОСЛЕДСТВИЙ ЧС

Мураев Н.П.<sup>1</sup>, Карапузиков А.А.<sup>2</sup>

**Ключевые слова:** дистанционное зондирование, прогнозные расчеты, поддержка управленческих решений, цифровые двойники, межведомственный обмен данными, оценка рисков, оперативное реагирование.

## Аннотация

**Цель работы:** проанализировать функциональные возможности современных цифровых решений, применяемых для наблюдения за изменением оперативной ситуации, прогнозом оценки опасных процессов и поддержки принятия решений при угрозе или возникновении чрезвычайных ситуаций.

**Метод исследования:** теоретический анализ научной и учебно-методической литературы по вопросам предупреждения чрезвычайных ситуаций, цифровизации управления рисками, геоинформационного обеспечения, дистанционного зондирования и прогнозирования опасных процессов. Также применялись методы обобщения, систематизации и сравнительного анализа функциональных возможностей программных решений, используемых для оценки обстановки, пространственного анализа, сценарного прогнозирования и информационной поддержки органов управления.

**Результаты исследования:** в ходе исследования установлено, что эффективность предупреждения и ликвидации чрезвычайных ситуаций во многом зависит от своевременного получения достоверных данных, их комплексной обработки и представления в удобной для принятия решений форме. Установлено, что наибольшую эффективность демонстрируют комплексные цифровые системы, которые интегрируют информацию, поступающую от различных датчиков, метеослужб, спутников, беспилотных аппаратов, электронных карт и ведомственных баз данных.

**Практическая ценность** проведенного исследования заключается в том, что полученные результаты могут быть использованы для совершенствования систем оповещения и реагирования на чрезвычайные ситуации, разработки мер по защите населения и территорий, анализа уязвимых элементов инфраструктуры, выбора программных средств для информационно-аналитической поддержки процессов управления.

DOI: 10.24412/1994-1404-2026-3-70-78

## Введение

Эффективное предупреждение и ликвидация последствий чрезвычайных ситуаций невозможны без своевременного получения достоверной информации об обстановке, ее аналитической обработки и прогнозирования возможного развития событий. В связи с этим особую актуальность приобретают современные информационно-аналитические системы мониторинга и программные комплексы моделирования последствий чрезвычайных ситуаций.

Такие системы позволяют осуществлять сбор, хранение, обработку, визуализацию и анализ данных, поступающих от различных источников: стационарных

датчиков, автоматизированных постов наблюдения, спутниковых систем, беспилотных летательных аппаратов, метеорологических служб, ведомственных баз данных и оперативных сообщений. На основе полученной информации формируются прогнозы развития опасных процессов, рассчитываются зоны поражения, масштабы возможного ущерба, потребность в силах и средствах, а также варианты управленческих решений [1].

Вместе с тем практическое применение информационно-аналитических систем мониторинга и программных комплексов моделирования последствий чрезвычайных ситуаций сопровождается рядом

<sup>1</sup> **Мураев Николай Павлович**, кандидат педагогических наук, доцент, профессор кафедры безопасности в ЧС Уральского института ГПС МЧС России, г. Екатеринбург, Российская Федерация.

E-mail: myrnik1967@yandex.com

<sup>2</sup> **Карапузиков Александр Анатольевич**, кандидат педагогических наук, доцент, начальник кафедры безопасности в ЧС Уральского института ГПС МЧС России, г. Екатеринбург, Российская Федерация.

E-mail: alexx-7777@mail.ru

проблем методического, технического и организационного характера. К числу наиболее существенных проблем можно отнести разнообразие исходных данных, отличия в их форматах, недостаточно высокую скорость обмена информацией между различными ведомствами, ограниченную совместимость отдельных программных продуктов, а также зависимость точности прогнозирования от полноты и достоверности исходных сведений [2]. Кроме того, при анализе последствий чрезвычайных ситуаций важно принимать во внимание множество взаимосвязанных факторов, к числу которых относятся особенности источника риска, погодные условия, специфику рельефа, плотность населения, состояние транспортных и инженерных систем, а также готовность соответствующих сил и ресурсов.

Данные обстоятельства подчеркивают необходимость комплексного изучения современных информационно-аналитических систем и программных решений, используемых для мониторинга текущей обстановки, прогнозирования динамики чрезвычайных ситуаций и оценки потенциальных последствий. Проведение такого анализа дает возможность определить их функциональные характеристики, выявить сильные и слабые стороны, а также наметить пути дальнейшего развития с учетом актуальных требований к скорости, точности и наглядности предоставляемой информации.

### **Основная часть**

Мониторинг обстановки — это непрерывный или периодический процесс наблюдения, сбора, обработки и анализа сведений о состоянии природных, техногенных и социальных объектов, которые могут представлять потенциальную опасность возникновения чрезвычайных ситуаций. Основная цель мониторинга заключается в своевременном обнаружении признаков опасных процессов и оперативном обеспечении органов управления достоверной информацией, необходимой для принятия эффективных решений по предупреждению и ликвидации ЧС.

По мнению Г.М. Абрамова, важной составляющей современных систем мониторинга является применение когнитивных технологий и систем принятия решений в реальном времени. Такие технологии позволяют не только выявлять признаки возможных угроз, но и автоматически формировать оптимальные сценарии реагирования, что в дальнейшем способствует сокращению времени, необходимого для принятия управленческих решений, повышает готовность служб реагирования к действиям в условиях чрезвычайных ситуаций и обеспечивает своевременную, адекватную реакцию, направленную на минимизацию последствий природных и техногенных опасностей [3].

М.И. Фалеев и С.В. Горбунов считают, что мониторинг быстроразвивающихся опасных природных явлений и техногенных процессов представляет собой комплексную деятельность, включающую несколько

взаимосвязанных направлений. К числу основных относятся наблюдение за воздействующими факторами, оценка фактического состояния объектов и природной среды, а также прогнозирование их дальнейшего состояния. По мнению ученых это позволяет обеспечить непрерывное получение актуальной информации об обстановке, своевременно выявлять признаки развития опасных процессов и формировать основу для принятия обоснованных управленческих решений в сфере предупреждения и ликвидации чрезвычайных ситуаций<sup>3</sup>.

По мнению Р.С. Майстерчука и М.С. Хацько, важным инструментом мониторинга чрезвычайных ситуаций является дистанционное зондирование Земли. Этот подход основан на использовании спутниковых и авиационных технологий, которые предоставляют оперативную информацию о состоянии земной поверхности и наблюдаемых изменениях. Использование методов дистанционного зондирования позволяет выявлять районы, подвергшиеся затоплению, пожарам и зонам загрязнения, а также фиксировать изменения ландшафта и оценивать уровень ущерба, причиненного чрезвычайными ситуациями [4].

С.Н. Семиглазов подчеркивает, что мониторинг направлен на выявление и фиксацию опасных природных и техногенных явлений, а также на обработку информации о них и формирование информационных ресурсов, необходимых для предотвращения чрезвычайных ситуаций и организации мероприятий по ликвидации их последствий. К основным задачам мониторинга и прогнозирования относятся наблюдение за потенциальными источниками чрезвычайных ситуаций, систематизация и анализ поступающих данных, своевременное информирование органов управления о существующих угрозах, а также ведение учета опасных процессов и оценка возможных сценариев развития чрезвычайных ситуаций [5].

Мониторинг выполняет ряд важных функций в системе предупреждения чрезвычайных ситуаций. Прежде всего, он обеспечивает своевременное выявление таких опасных факторов, как повышение уровня воды в водоемах, повышенная концентрация вредных химических веществ, сейсмическая активность, лесные пожары и аварийные работы на технических объектах. Кроме того, мониторинг позволяет отслеживать изменения ситуации с течением времени, выявлять тенденции и определять уровень вероятности возникновения чрезвычайных ситуаций. Данные, полученные в ходе мониторинга, являются основой для вычислительных моделей и прогностических программных комплексов, используемых для оценки рисков.

Современный мониторинг характеризуется комплексным подходом, предполагающим интеграцию

<sup>3</sup> Фалеев М.И., Горбунов С.В. Мониторинг и прогнозирование чрезвычайных ситуаций как составная часть системы управления рисками ЧС // Проблемы анализа риска. 2018. Т. 15. № 6. С. 8—16. DOI: 10.32686/1812-5220-2018-15-8-16.

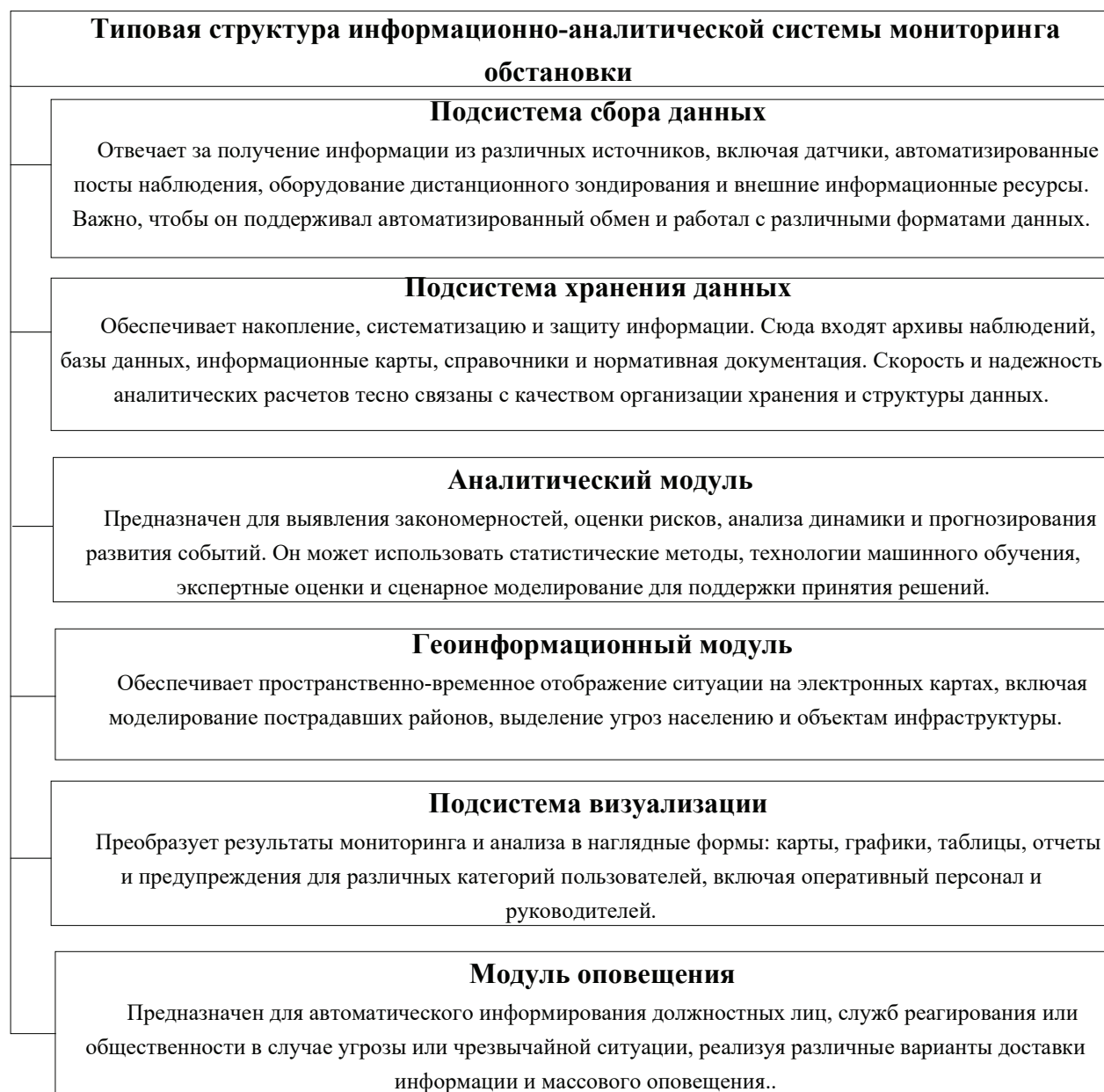


**Рис. 1. Типовая структура информационно-аналитической системы мониторинга обстановки**

различных видов наблюдений: гидрометеорологических, экологических, радиационных, химических, сейсмических, противопожарных, инженерных и санитарно-эпидемиологических. Каждый из этих типов включает в себя свои собственные методы, устройства и нормативные параметры, но для эффективного управления рисками их данные объединяются в единую информационную систему.

Примером специализированной системы является «Система мониторинга лесных пожаров», предназначенная для обнаружения очагов возгорания и оценки лесопожарной обстановки на различных территориях. Такие системы обеспечивают работу лесопожарных служб, органов исполнительной власти и дежурных оперативных подразделений, позволяя получать оперативную информацию о возможных пожарах, анали-

зировать их координаты, отслеживать подтверждение температурных точек и отслеживать реагирование на инциденты.

Другим примером может служить «Атлас опасностей и рисков МЧС России», представляющий собой информационно-аналитический инструмент для отображения и анализа информации о рисках возникновения чрезвычайных ситуаций на определенной территории. Он визуализирует различные типы угроз, такие как природные, техногенные, пожарные, гидрологические, метеорологические и др., предоставляя исчерпывающую картину существующих опасностей и их потенциального развития в конкретной области.

Оперативность получения информации имеет особое значение при мониторинге ситуации. В быстро меняющейся обстановке даже небольшая задержка



**Группы программных комплексов моделирования последствий чрезвычайных ситуаций**

| <b>ГРУППА</b>                                                                          | <b>НАЗНАЧЕНИЕ</b>                                                                                                                                                  | <b>ОСНОВНЫЕ ИСПОЛЬЗУЕМЫЕ ДАННЫЕ<br/>И ВОЗМОЖНОСТИ</b>                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Моделирование природных ЧС</b>                                                      | Для прогнозирования паводков и наводнений, лесных и ландшафтных пожаров, оползней, селей, лавин, ураганов, засух и других опасных природных процессов.             | Используются данные гидрологических и метеорологических наблюдений, цифровые модели рельефа, информация о растительном покрове, типах почв, водных объектах и хозяйственной освоенности территории.                                          |
| <b>Моделирование техногенных ЧС</b>                                                    | Для оценки последствий аварий на промышленных объектах, транспорте, объектах энергетики, химически опасных и радиационно опасных объектах.                         | Позволяют рассчитывать распространение опасных химических веществ в атмосфере, зоны теплового излучения при пожарах, параметры ударной волны при взрывах, уровни загрязнения окружающей среды, последствия разрушения инженерных сооружений. |
| <b>Комплексы оценки биолого-социальных чрезвычайных ситуаций</b>                       | Для анализа распространения инфекционных заболеваний, оценки санитарно-эпидемиологической обстановки, планирования ограничительных и профилактических мероприятий. | Применяются эпидемиологические модели, статистические данные, информация о плотности населения, транспортной мобильности и состоянии медицинской инфраструктуры.                                                                             |
| <b>Комплексные информационно-аналитические системы поддержки принятия решений в ЧС</b> | Предназначены для сбора, объединения, отображения и анализа информации о различных видах чрезвычайных ситуаций, а также для обоснования управленческих решений     | Объединяют картографические данные, результаты мониторинга, метеоданные, сведения о силах и средствах, прогнозные расчеты, маршруты эвакуации, зоны поражения и позволяют работать с ними в едином интерфейсе.                               |

может существенно повлиять на эффективность принимаемых мер. Поэтому современные системы мониторинга ориентированы на автоматизированный сбор, передачу и обработку данных в режиме реального времени.

Информационно-аналитическая система мониторинга представляет собой интегрированный комплекс технических, программных, информационных и организационных средств, предназначенных для сбора, хранения, обработки и анализа данных о состоянии объектов и территорий. В отличие от простых систем регистрации параметров, такие системы предоставляют возможности для интерпретации, выявления отклонений, составления прогнозов и подготовки рекомендаций для органов управления.

Стандартная структура информационно-аналитической системы мониторинга обычно включает в себя следующие ключевые подсистемы: подсистему сбора данных, подсистему хранения информации, аналитический модуль, геоинформационный модуль, подсистему визуализации данных, модуль оповещения и подсистему поддержки принятия решений. Схема, представленная на рисунке 1 иллюстрирует типовую структуру информационно-аналитической системы мониторинга ситуации и демонстрирует, как реализуются основные задачи мониторинга и аналитической поддержки предупреждения и ликвидации чрезвычайных ситуаций.

Программные комплексы моделирования последствий чрезвычайных ситуаций предназначены для рас-

четной оценки развития опасных процессов и определения возможных зон воздействия поражающих факторов. Их применение позволяет заранее оценить масштабы чрезвычайной ситуации, определить потенциально опасные территории, рассчитать численность населения в зоне риска, спрогнозировать ущерб и спланировать мероприятия по защите населения и территорий.

В зависимости от характера чрезвычайной ситуации программные комплексы можно условно разделить на несколько групп, которые приведены в таблице 1.

Геоинформационные системы занимают центральное место в современных системах мониторинга и моделирования чрезвычайных ситуаций. Пространственная привязка большинства чрезвычайных ситуаций требует учета географических, инфраструктурных и демографических параметров при анализе их последствий. Использование геоинформационных технологий позволяет интегрировать цифровые карты, спутниковые снимки, результаты дистанционного зондирования, данные мониторинга, предполагаемые зоны повреждения и информацию об объектах инфраструктуры в единую информационную систему. На этой основе разрабатываются тематические карты рисков, оперативные схемы обстановки, планы эвакуации и распределения необходимых ресурсов.

Существенным преимуществом геоинформационных систем является возможность отображения информации в нескольких слоях. Например, в процессе моделирования последствий наводнения на карту

одновременно наносятся элементы гидрографической сети, рельеф, административные границы, транспортная и социальная инфраструктура, а также прогнозируемые зоны затопления. Такой подход обеспечивает всестороннюю оценку масштаба угрозы и выявление наиболее уязвимых участков территории, что значительно повышает обоснованность управленческих решений.

По мнению Н.Ю. Рыженко, одним из ключевых условий эффективного применения таких систем является наличие необходимой и практически значимой функциональности, а также простота внедрения и эксплуатации. Автор отмечает, что в настоящее время существует достаточно широкий спектр универсальных ГИС, использование которых позволяет решать большой круг прикладных задач в деятельности структур МЧС России<sup>4</sup>.

Геоинформационные технологии также используются для решения задач маршрутизации. В условиях чрезвычайной ситуации необходимо оперативно определить оптимальные пути эвакуации населения, доставки гуманитарных ресурсов, перемещения аварийно-спасательных формирований и медицинских бригад. При этом учитываются состояние дорог, загруженность транспортной сети, наличие разрушений, погодные условия и другие факторы.

По мнению Г.Ю. Шамсудинова, В.Ю. Ярового, В.И. Спешилова, для эффективного внедрения и практического использования геоинформационных технологий в деятельности пожарных подразделений необходимо создание специального учебно-методического пособия, которое должно быть изложено доступным языком и разъяснять сотрудникам основные принципы работы с ГИС в подразделении. Авторы подчеркивают, что его содержание целесообразно строить на пошаговых инструкциях, примерах практического применения и рекомендациях по интеграции геоинформационных систем в повседневную служебную деятельность [6].

Качество работы информационно-аналитических систем во многом зависит от полноты, точности и актуальности исходных данных. В современных условиях используется широкий спектр источников информации [7].

Одним из основных источников являются автоматизированные датчики и посты наблюдения. Они позволяют в режиме реального времени фиксировать параметры окружающей среды и технических объектов: температуру, давление, уровень воды, скорость ветра, концентрацию загрязняющих веществ, радиационный фон, вибрации, дым, пламя и другие показатели.

Важную роль играют данные дистанционного зондирования Земли. Спутниковые снимки и аэрофото-

съемка позволяют выявлять очаги пожаров, зоны подтопления, изменения растительного покрова, разрушения инфраструктуры, загрязнение водных объектов и другие признаки чрезвычайных ситуаций. Использование беспилотных летательных аппаратов обеспечивает получение детализированной информации в труднодоступных или опасных районах.

Метеорологическая информация необходима для моделирования распространения опасных веществ, прогнозирования пожаров, паводков, штормовых явлений и других процессов. К таким данным относятся скорость и направление ветра, температура воздуха, влажность, атмосферное давление, осадки, облачность и другие параметры.

Существенное значение имеют сведения о населении и инфраструктуре [8]. Для оценки последствий чрезвычайной ситуации необходимо знать численность и плотность населения, расположение жилых районов, больниц, школ, объектов транспорта, связи, энергетики, водоснабжения и других элементов жизнеобеспечения.

Дополнительным источником могут выступать оперативные сообщения, данные социальных сетей, обращения граждан, фото- и видеоматериалы с места происшествия. Однако такая информация требует обязательной проверки достоверности и сопоставления с официальными источниками.

Моделирование последствий чрезвычайных ситуаций основано на применении математических, статистических, имитационных и экспертных методов. Выбор конкретного метода зависит от типа чрезвычайной ситуации, доступности исходных данных, требуемой точности и времени, отведенного на расчет.

Математические модели применяются для описания физических процессов: распространения загрязняющих веществ, движения водных потоков, теплопередачи, взрывных процессов, распространения пожара. Такие модели позволяют получить количественные параметры поражающих факторов и определить границы опасных зон [9].

Статистические методы используются при наличии значительного объема исторических данных и обеспечивают обоснование параметров вероятностных моделей и расчет показателей риска для различных территорий и объектов.

Имитационное моделирование позволяет протестировать различные варианты реагирования, оптимизировать использование ресурсов и повысить готовность к чрезвычайным ситуациям<sup>5</sup>.

Экспертные оценки помогают учесть специфику конкретных регионов, а также позволяют корректировать результаты автоматического анализа на основе профессионального опыта специалистов

<sup>4</sup> Фалеев М.И., Горбунов С.В. Мониторинг и прогнозирование чрезвычайных ситуаций как составная часть системы управления рисками ЧС // Проблемы анализа риска. 2018. Т. 15. № 6. С. 8—16. DOI: 10.32686/1812-5220-2018-15-8-16.

<sup>5</sup> Рыженко Н.Ю. Использование геоинформационных систем в структурах МЧС России // Современные технологии обеспечения гражданской обороны и ликвидации последствий чрезвычайных ситуаций. 2016. № 1-1(7). С. 480—484.

**Общие функциональные возможности современных информационно-аналитических систем мониторинга  
и программных комплексов моделирования последствий чрезвычайных ситуаций**

| <b>ФУНКЦИОНАЛЬНАЯ ВОЗМОЖНОСТЬ</b>              | <b>СОДЕРЖАНИЕ</b>                                                                                                                                                                           |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Интеграция разнородных данных</b>           | Эффективная система должна объединять информацию от датчиков, картографических сервисов, ведомственных баз данных, спутниковых систем, метеорологических служб и оперативных подразделений. |
| <b>Автоматизированное выявление отклонений</b> | Система должна не только отображать текущие параметры, но и сигнализировать о превышении пороговых значений или появлении опасных тенденций.                                                |
| <b>Прогнозирование развития обстановки</b>     | Значимым элементом является наличие прогнозного блока, позволяющего не только фиксировать текущую ситуацию, но и оценивать возможное будущее состояние обстановки.                          |
| <b>Пространственная визуализация данных</b>    | Современные комплексы должны обеспечивать геоинформационное отображение данных, включая зоны риска, маршруты, объекты инфраструктуры и расположение сил реагирования.                       |
| <b>Поддержка принятия решений</b>              | Может реализовываться в виде автоматизированного формирования рекомендаций, расчетов потребности в ресурсах, сравнения сценариев и подготовки отчетных документов.                          |
| <b>Масштабируемость системы</b>                | Система должна быть способна функционировать как на уровне отдельного объекта или муниципального образования, так и на региональном или национальном уровне.                                |

Внедрение методов искусственного интеллекта и машинного обучения помогает повысить точность прогнозов и автоматизировать процессы обнаружения и классификации угроз [10, 11]. Современные технологии искусственного интеллекта, интегрированные с геоинформационными и аналитическими системами, обеспечивают быстрый анализ больших объемов разнородных данных, своевременное обнаружение аномалий, динамическое обновление данных о рисках и эффективную поддержку принятия управленческих решений.

Таким образом, использование комплексного подхода, сочетающего в себе: ГИС-технологии, статистические, имитационные и экспертные методы, а также современные достижения в области искусственного интеллекта, позволяет значительно повысить эффективность систем мониторинга, предупреждения чрезвычайных ситуаций и реагирования на них, а также реализовать принцип проактивного управления рисками. Однако применение таких методов требует качественных обучающих выборок, прозрачности алгоритмов и постоянной проверки результатов.

Современные информационно-аналитические системы мониторинга и программные комплексы моделирования последствий чрезвычайных ситуаций различаются по назначению, масштабу применения, точности расчетов, способам визуализации и степени автоматизации. Однако можно выделить ряд общих функциональных возможностей, характерных для наиболее развитых решений (таблица 2).

Использование информационно-аналитических систем и программных комплексов моделирования последствий чрезвычайных ситуаций имеет ряд существенных преимуществ. К ним относятся повышение оперативности получения информации, улучшение качества прогнозирования, снижение влияния человеческого фактора, возможность анализа сложных сценариев, наглядность представления данных и повышение обоснованности управленческих решений.

Кроме того, такие системы позволяют проводить предварительное планирование мероприятий по предупреждению и ликвидации чрезвычайных ситуаций. С их помощью можно заранее оценивать уязвимость территорий, определять зоны повышенного риска, разрабатывать планы эвакуации, рассчитывать потребность в силах и средствах, проводить обучение персонала на основе моделируемых сценариев.

Вместе с тем современные программные комплексы имеют и определенные ограничения. Одной из главных проблем является зависимость результатов моделирования от качества исходных данных. Ошибки в данных о рельефе, погодных условиях, технических характеристиках объектов или численности населения могут привести к существенным искажениям прогнозов.

Еще одной проблемой является сложность моделирования многофакторных процессов. Реальное развитие чрезвычайной ситуации часто зависит от большого числа взаимосвязанных факторов, часть из которых трудно заранее учесть. Поэтому результаты расчетов

должны рассматриваться как вероятностная оценка, а не как абсолютно точное предсказание.

Кроме того, существуют трудности, связанные с интеграцией различных информационных систем. На практике информация может храниться в различных форматах, управляться разными организациями и иметь разный уровень доступности, что затрудняет формирование единой информационной среды.

Также, важным аспектом остается профессиональная подготовка. Даже самые передовые программные решения не обеспечат высокой эффективности без специалистов, обладающих необходимыми знаниями для правильной интерпретации результатов анализа и понимания ограничений используемых моделей.

### **Заключение**

На сегодняшний день современные системы анализа и мониторинга обстановки, а также программные

средства моделирования последствий чрезвычайных ситуаций занимают ведущее место среди средств прогнозирования и управления рисками. Внедрение этих технологий позволяет быстро выявлять потенциальные угрозы, анализировать возможные сценарии, проводить пространственную оценку ситуации и обеспечивать эффективную поддержку управленческих решений. Исследования подтверждают, что наилучшие результаты достигаются при использовании интегрированных платформ, которые автоматизируют сбор информации, используют геоинформационные сервисы, используют методы вычислительного моделирования, выполняют глубокую аналитическую обработку данных и используют системы оповещения.

Особое значение имеет интеграция данных из различных источников и формирование единой цифровой среды, что создает условия для перехода от отдельных специализированных программ к комплексным информационно-аналитическим комплексам.

### **Литература**

1. Мураев Н.П., Карапузиков А.А., Белкин Д.С., Башаев С.М. Мониторинг природных пожаров // Информационно-вычислительные технологии и их приложения : сб. ст. XXVIII Межд. науч.-тех. конф., Пенза, 26—27 августа 2024 года. Пенза: Пензенский государственный аграрный университет, 2024. С. 195—198.
2. Балобанов А.А., Самохвалов Д.Н. Анализ информационных систем, используемых в ЦУКС МЧС России Архангельской области // Сервис безопасности в России: опыт, проблемы, перспективы. Мониторинг, предотвращение и ликвидация чрезвычайных ситуаций природного и техногенного характера : мат. межд. науч.-практ. конф., Санкт-Петербург, 28 октября 2021 г. СПб. : Санкт-Петербургский университет ГПС МЧС России, 2021. С. 798—800.
3. Абрамов Г.М. Мониторинг, моделирование и прогнозирование опасных природных явлений и чрезвычайных ситуаций // Вестник науки. 2025. Т. 5. № 11 (92). С. 1324—1336.
4. Майстерчук Р.С., Хацько М.С. Мониторинг, моделирование и прогнозирование чрезвычайных ситуаций в современных условиях // Актуальные проблемы обеспечения пожарной безопасности и защиты от чрезвычайных ситуаций : мат. VII Всерос. науч.-практ. конф., Красноярск, 24 апреля 2025 г. Железногорск : Сибирская пожарно-спасательная академия ГПС МЧС России, 2025. С. 96—100.
5. Семиглазов С.Н. Мониторинг, моделирование и прогнозирование чрезвычайных ситуаций // Актуальные проблемы обеспечения пожарной безопасности и защиты от чрезвычайных ситуаций : сб. мат. Всерос. науч.-практ. конф., Железногорск, 22 апреля 2022 г. Железногорск : Сибирская пожарно-спасательная академия ГПС МЧС России, 2022. С. 171—175.
6. Шамсудинов Г.Ю., Яровой В.Ю., Спешиллов В.И. Применение геоинформационных технологий в пожарной охране // Информационные технологии в сфере РСЧС и ГО : сб. тр. секции № 12 XXXV Межд. науч.-практ. конф., Химки, 26 февраля 2025 г. Химки : Академия гражданской защиты МЧС России им. генерал-лейтенанта Д.И. Михайлика, 2025. С. 132—136.
7. Тюрин А.Р., Семенов А.О., Разумова Е.Ф. Обзор информационных систем и ресурсов, применяемых в деятельности Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций // Актуальные вопросы пожаротушения : сб. мат. IV Всерос. науч.-практ. конф., Иваново, 27 марта 2025 г. Иваново : Ивановская пожарно-спасательная академия ГПС МЧС России, 2025. С. 632—638.
8. Нехорошев С.Н., Кудрявцев А.Н., Попов А.П., Свентская Н.В. О цифровом развитии единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций // Технологии гражданской безопасности. 2021. Т. 18. № 5. С. 60—67. DOI: 10.54234/CST.19968493.2021.18.5.8.60.
9. Кузнецова Н.Н. Геоинформационные технологии в решении задач прогнозирования и устранения ЧС подразделениями МЧС России // Пожарная и аварийная безопасность : сб. мат. XV межд. науч.-практ. конф., посвященной 30-й годовщине МЧС России, Иваново, 17—18 ноября 2020 г. Иваново : Ивановская пожарно-спасательная академия ГПС МЧС России, 2020. С. 491—493.



10. Третьяков Н.А. Возможность применения алгоритмов машинного обучения для анализа чрезвычайных ситуаций // Материалы межд. науч.-тех. конф. «Системы безопасности». 2020. № 29. С. 64—67.
11. Матвеев А.В., Колеров Д.А. Перспективы применения искусственного интеллекта при реагировании на ЧС // Сервис безопасности в России: опыт, проблемы, перспективы. Мониторинг, предотвращение и ликвидация чрезвычайных ситуаций природного и техногенного характера : мат. межд. науч.-практ. конф., Санкт-Петербург, 28 октября 2021 г. СПб. : Санкт-Петербургский университет ГПС МЧС России, 2021. С. 726—730.

**SECTION:**

*SYSTEM ANALYSIS, MANAGEMENT, ARTIFICIAL INTELLIGENCE, AND INFORMATION PROTECTION*

# **ANALYSIS OF INFORMATION AND ANALYTICAL SYSTEMS FOR MONITORING THE SITUATION AND SOFTWARE COMPLEXES FOR MODELING THE CONSEQUENCES OF EMERGENCIES**

*Muraev N.P.<sup>6</sup>, Karapuzikov A.A.<sup>7</sup>*

**Keywords:** *remote sensing, predictive calculations, management decision support, digital twins, interagency data exchange, risk assessment, rapid response.*

**Abstract**

**The purpose of the work:** *to analyze the functionality of modern digital solutions used to monitor changes in the operational situation, predictive assessment of dangerous processes and support decision-making in the event of a threat or emergency.*

**Research method:** *theoretical analysis of scientific and educational literature on emergency prevention, digitalization of risk management, geoinformation support, remote sensing and forecasting of dangerous processes. The methods of generalization, systematization and comparative analysis of the functionality of software solutions used for situation assessment, spatial analysis, scenario forecasting and information support of management bodies were also applied.*

**Research results:** *the study found that the effectiveness of emergency prevention and response largely depends on the timely receipt of reliable data, their complex processing and presentation in a convenient form for decision-making. It has been established that complex digital systems that integrate information from various sensors, weather services, satellites, unmanned vehicles, electronic maps and departmental databases demonstrate the greatest efficiency.*

**Practical value:** *the practical value of the conducted research lies in the fact that the results obtained can be used to improve emergency warning and response systems, develop measures to protect the population and territories, analyze vulnerable infrastructure elements, and select software tools for information and analytical support of management processes.*

**References**

1. Muraev N.P., Karapuzikov A.A., Belkin D.S., Bashaev S.M. Monitoring prirodnikh pozharov // Informatsionno-vychislitel'nye tekhnologii i ikh prilozheniia : sb. st. XXVIII Mezhd. nauch.-tekhn. konf., Penza, 26—27 avgusta 2024 goda. Penza: Penzenskii gosudarstvennyi agrarnyi universitet, 2024. S. 195—198.
2. Balobanov A.A., Samokhvalov D.N. Analiz informatsionnykh sistem, ispol'zuemykh v TsUKS MChS Rossii Arkhangel'skoi oblasti // Servis bezopasnosti v Rossii: opyt, problemy, perspektivy. Monitoring, predotvrashchenie

<sup>6</sup> **Nikolai P. Muraev**, Ph.D. (Pedagogy), Associate Professor, Professor of the Department of Safety in Emergency Situations of the Ural Institute of the State Emergency Service of the Ministry of Emergency Situations of Russia, Ekaterinburg, Russian Federation.  
E-mail: [myrnik1967@yandex.com](mailto:myrnik1967@yandex.com)

<sup>7</sup> **Aleksandr A. Karapuzikov**, Ph.D. (Pedagogy), Associate Professor, Head of the Department of Safety in Emergency Situations at the Ural Institute of the State Emergency Service of the Ministry of Emergency Situations of Russia, Associate Professor of the Department of Technosphere and Environmental Safety at the Ural State Agrarian University, Ekaterinburg, Russian Federation.  
E-mail: [alexx-7777@mail.ru](mailto:alexx-7777@mail.ru)

- i likvidatsiia chrezvychainykh situatsii prirodnogo i tekhnogenogo kharaktera : mat. mezhd. nauch.-prakt. konf., Sankt-Peterburg, 28 oktiabria 2021 g. SPb. : Sankt-Peterburgskii universitet GPS MChS Rossii, 2021. S. 798—800.
3. Abramov G.M. Monitoring, modelirovanie i prognozirovanie opasnykh prirodnykh iavlenii i chrezvychainykh situatsii // Vestnik nauki. 2025. T. 5. No. 11 (92). S. 1324—1336.
  4. Maisterchuk R.S., Khats'ko M.S. Monitoring, modelirovanie i prognozirovanie chrezvychainykh situatsii v sovremennykh usloviakh // Aktual'nye problemy obespecheniia pozharnoi bezopasnosti i zashchity ot chrezvychainykh situatsii : mat. VII Vseros. nauch.-prakt. konf., Krasnoiarsk, 24 apreliia 2025 go. Zheleznogorsk : Sibirskaia pozharно-spasatel'naia akademiia GPS MChS Rossii, 2025. S. 96—100.
  5. Semiglazov S.N. Monitoring, modelirovanie i prognozirovanie chrezvychainykh situatsii // Aktual'nye problemy obespecheniia pozharnoi bezopasnosti i zashchity ot chrezvychainykh situatsii : sb. mat. Vseros. nauch.-prakt. konf., Zheleznogorsk, 22 apreliia 2022 g. Zheleznogorsk : Sibirskaia pozharно-spasatel'naia akademiia GPS MChS Rossii, 2022. S. 171—175.
  6. Shamsudinov G.Iu., Iarovoi V.Iu., Speshilov V.I. Primenenie geoinformatsionnykh tekhnologii v pozharnoi okhrane // Informatsionnye tekhnologii v sfere RSChS i GO : sb. tr. sektsii No. 12 XXXV Mezhd. nauch.-prakt. konf., Khimki, 26 fevralia 2025 g. Khimki : Akademiia grazhdanskoi zashchity MChS Rossii im. general-leitenanta D.I. Mikhailika, 2025. S. 132—136.
  7. Tiurin A.R., Semenov A.O., Razumova E.F. Obzor informatsionnykh sistem i resursov, primeniaemykh v deiatel'nosti Edinoi gosudarstvennoi sistemy preduprezhdeniia i likvidatsii chrezvychainykh situatsii // Aktual'nye voprosy pozharotusheniia : sb. mat. IV Vseros. nauch.-prakt. konf., Ivanovo, 27 marta 2025 g. Ivanovo : Ivanovskaia pozharно-spasatel'naia akademiia GPS MChS Rossii, 2025. S. 632—638.
  8. Nekhoroshev S.N., Kudriavtsev A.N., Popov A.P., Svetskaia N.V. O tsifrovom razvitii edinoi gosudarstvennoi sistemy preduprezhdeniia i likvidatsii chrezvychainykh situatsii // Tekhnologii grazhdanskoi bezopasnosti. 2021. T. 18. No. S. 60—67. DOI: 10.54234/CST.19968493.2021.18.S.8.60.
  9. Kuznetsova N.N. Geoinformatsionnye tekhnologii v reshenii zadach prognozirovaniia i ustraneniia ChS podrazdeleniiami MChS Rossii // Pozharnaia i avariinaia bezopasnost' : sb. mat. XV mezhd. nauch.-prakt. konf., posviashchennoi 30-i godovshchine MChS Rossii, Ivanovo, 17—18 noiabria 2020 g. Ivanovo : Ivanovskaia pozharно-spasatel'naia akademiia GPS MChS Rossii, 2020. S. 491—493.
  10. Tret'iakov N.A. Vozmozhnost' primeneniia algoritmov mashinnogo obucheniia dlia analiza chrezvychainykh situatsii // Materialy mezhd. nauch.-tekhn. konf. "Sistemy bezopasnosti". 2020. No. 29. S. 64—67.
  11. Matveev A.V., Kolerov D.A. Perspektivy primeneniia iskusstvennogo intellekta pri reagirovanii na ChS // Servis bezopasnosti v Rossii: opyt, problemy, perspektivy. Monitoring, predotvrashchenie i likvidatsiia chrezvychainykh situatsii prirodnogo i tekhnogenogo kharaktera : mat. mezhd. nauch.-prakt. konf., Sankt-Peterburg, 28 oktiabria 2021 g. SPb. : Sankt-Peterburgskii universitet GPS MChS Rossii, 2021. S. 726—730.



# МЕТОДИКА ОПТИМИЗАЦИИ СЛОЖНОЙ ЧЕЛОВЕКО-МАШИННОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С УЧЁТОМ УГЛЕРОДНОЙ ИНТЕНСИВНОСТИ

Исаев Н.А.<sup>1</sup>

**Ключевые слова:** мониторинг, корреляция, реагирование, тревоги, ресурсоёмкость, энергоэффективность, телеметрия, параметризация, конфигурация, детектирование.

## Аннотация

**Цель работы:** состоит в разработке воспроизводимой методики оптимизации человеко-машинного контура мониторинга и реагирования на инциденты информационной безопасности (аналитик центра мониторинга безопасности и программная система поддержки принятия решений) по трём группам критериев: уровень киберзащищённости, когнитивная нагрузка оператора и углеродная интенсивность эксплуатации вычислительной инфраструктуры.

**Методы исследования:** системный анализ архитектуры и процессов реагирования, математическое и имитационное моделирование энергопотребления и выбросов в CO<sub>2</sub>-эквиваленте, статистическая обработка эксплуатационных данных и экспертная оценка операторских факторов. В качестве формализованного ядра вводятся нормированный показатель защищённости, метрики времени обнаружения и нагрузки на оператора, а также расчёт углеродной интенсивности конфигурации через энергопотребление ИТ-нагрузки и параметры энергоэффективности площадки.

**Результаты.** Сформулированы модели роста экологической стоимости при экстенсивной параметризации и модель насыщения при ограничении сложности. Разработан спиральный алгоритм конфигурационного управления с правилом останова по предельной эффективности (соотношению прироста защищённости и «углеродной цены» усложнения). Практический эффект заключается в снижении доли низкоэффективных правил и избыточной телеметрии при сохранении требований по времени обнаружения и качеству детектирования, что применимо для обоснования модернизации корпоративных центров мониторинга безопасности и включения экологических показателей в регламентную отчётность. Экспериментальная верификация на данных трёх корпоративных СППР (5—20 тыс. узлов) подтвердила работоспособность моделей: при экстенсивном наращивании параметров зафиксирован суперлинейный рост углеродного следа ( $\beta \approx 1,6—2,2$ ), а спиральная схема позволила сократить выбросы CO<sub>2</sub>-эквивалента на 20—30% за два года без ухудшения ключевых метрик киберзащищённости (MTTD, FNR/FPR).

DOI: 10.24412/1994-1404-2026-3-79-87

## Введение

Ускоренная цифровизация экономики усилила нагрузку на центры обработки данных, коммуникационную инфраструктуру и средства киберзащиты. По оценкам ряда исследований<sup>2</sup> доля информа-

ционно-коммуникационных технологий в глобальных выбросах парниковых газов уже сопоставима с вкладом авиации и продолжает расти. При этом энергоэф-

<sup>2</sup> Belkhir, L. Assessing ICT global emissions footprint: Trends to 2040 & recommendations / L. Belkhir, A. Elmelig // Journal of Cleaner Production. 2018. Vol. 177. P. 448–463. DOI: 10.1016/j.jclepro.2017.12.239.

Horner, N. C. Known unknowns: indirect energy effects of information and communication technology / N. C. Horner, A. Shehabi, I. L. Azevedo // Environmental Research Letters. 2016. Vol. 11, № 10. 103001. DOI: 10.1088/1748-9326/11/10/103001.

<sup>1</sup> Исаев Николай Александрович, аспирант Московского университета им. С.Ю. Витте, Москва, Россия. ORCID: 0009-0007-3987-1670.

E-mail: [supercopen@yandex.ru](mailto:supercopen@yandex.ru)

фективность и углеродный след<sup>3</sup> подсистем информационной безопасности остаются слабо изученными по сравнению с вычислительными и сетевыми сервисами общего назначения.

К исследованиям, формирующим методическую базу оценки и снижения экологической стоимости вычислений, относятся работы по выбросам информационно-коммуникационных технологий и динамике энергопотребления центров обработки данных<sup>4</sup> [1], а также публикации по воспроизводимым подходам к расчёту CO<sub>2</sub>-эквивалента вычислительных задач [2—5]. Для предметной области мониторинга безопасности важны также результаты по метрикам эффективности центров мониторинга и обзоры по системам управления событиями безопасности [6, 7].

В организации информационной безопасности широко применяются системы поддержки принятия решений (СППР): системы управления событиями и инцидентами (SIEM), платформы управления уязвимостями, средства корреляции событий, аналитические панели для центров мониторинга безопасности (SOC) и др. Эти системы обрабатывают большие объёмы журналов, телеметрии и сетевого трафика, что приводит к росту потребляемой энергии и, как следствие, углеродного следа.

Для данной предметной области характерны две взаимосвязанные проблемы. Первая связана с ограниченностью ресурсов (вычислительных, энергетических, бюджетных): рост объёма данных и числа корреляционных правил требует масштабирования инфраструктуры и увеличивает углеродный след. Вторая проблема состоит в оценке эффективности работы СППР с точки зрения человека: результативность мониторинга определяется не только точностью алгоритмов, но и тем, насколько оператор способен интерпретировать рекомендации, фильтровать ложные срабатывания и соблюдать целевые значения MTTD. Поэтому СППР целесообразно рассматривать как сложную человеко-машинную систему, а оптимизацию вести в многокритериальной постановке.

В практике построения СППР можно выделить две крайние методологические линии. Первая опирается на экстенсивную параметризацию: добавление всё новых правил корреляции, сигнатур, групп политик и пользовательских индикаторов, — подход, подробно описанный, в частности, А.В. Лукацким<sup>5</sup>. Вторая следует логике оптимальной сложности и минимально достаточного набора контролируемых параметров, подчёркивая ограниченные возможности оператора и риски перегрузки информацией (в духе подхода R. Anderson к инженерии безопасности [8]).

С точки зрения системного анализа обе линии задают различные траектории развития архитектуры СППР и по-разному влияют на энергопотребление компонентов, плотность размещения задач в ЦОД и, в конечном счёте, на углеродный след. В настоящей работе предлагается сопоставить эти подходы на формализованном уровне и построить гибридную «спиральную» схему, позволяющую совместно учитывать требования к кибербезопасности и устойчивому развитию.

Рассматривается класс корпоративных СППР, используемых в центрах мониторинга безопасности (SOC) для поддержки решений при выявлении и реагировании на инциденты в распределённой инфраструктуре. СППР функционирует в окружении динамической угрозовой среды и реализует процессы сбора и нормализации событий, корреляции и аналитики, хранения и представления результатов, после чего оператор принимает решение и запускает регламент реагирования. В экстенсивной практике перечень факторов и правил, на которые реагирует система, расширяется практически без верхней границы, что усиливает ресурсоёмкость и повышает риск перегрузки оператора.

Цель исследования состоит в разработке воспроизводимой методики оценки и оптимизации углеродного следа СППР как элемента человеко-машинной системы SOC, пригодной для использования как при проектировании новых решений, так и при модернизации действующих центров мониторинга. Методика опирается на метрики энергоэффективности ЦОД (PUE, CUE, WUE), региональные коэффициенты углеродоёмкости электроэнергии (CIF), а также эксплуатационные показатели киберзащищённости и операторской эффективности.

Для достижения цели решаются следующие задачи:

- 1) описать СППР как человеко-машинную систему и определить ключевые ограничения по ресурсам инфраструктуры и когнитивной нагрузке операторов;
- 2) определить набор энергетических, углеродных и эксплуатационных метрик, релевантных для оптимизации СППР (включая PUE, CUE, WUE, CIF, интегральный показатель защищённости  $S$ , MTTD и нагрузку операторов  $N$ );
- 3) сформулировать модели роста углеродного следа и деградации операторской эффективности при экстенсивной параметризации и при ограничении сложности конфигурации;
- 4) предложить «спиральный» алгоритм конфигурационного управления СППР и оценить его эффект с точки зрения критерия оптимальности, учитывающего как экологические, так и защитные и операторские показатели.

## **ОСНОВНАЯ ЧАСТЬ**

### **Показатель защищённости и критерий оптимальности**

Для связи углеродных метрик с качеством обеспечения безопасности введём интегральный показатель

<sup>3</sup> Wiedmann, T. A definition of 'carbon footprint' / T. Wiedmann, J. Minx; ed. by C. C. Pertsova // Ecological Economics Research Trends. New York: Nova Science Publishers, 2007. P. 1—11.

<sup>4</sup> Shehabi, A. United States Data Center Energy Usage Report / A. Shehabi, S. J. Smith, D. A. Sartor [et al.]. 2016. DOI: 10.2172/1372902.

<sup>5</sup> Лукацкий А.В. Обнаружение атак. СПб.: БХВ Петербург, 2001. 624 с.



защищённости  $S \in [0; 1]$ , трактуемый как нормированная полезность системы мониторинга и реагирования. В простейшей линейной форме

$$S = w_d \cdot DC + w_f \cdot (1 - FNR) + w_p \cdot (1 - FPR) + w_t \cdot \max(0, 1 - \frac{MTTD}{T_{det}}).$$

где  $DC$  — доля покрытых классов инцидентов;  $FNR$  и  $FPR$  — доли пропусков и ложных срабатываний соответственно;  $MTTD$  — среднее время обнаружения инцидента;  $T_{det}$  — согласованная целевая граница для  $MTTD$ ;  $w_d, w_f, w_p, w_t \geq 0$  — весовые коэффициенты, удовлетворяющие условию:

$$w_d + w_f + w_p + w_t = 1.$$

Показатель  $S$  дополняется метрикой нагрузки на операторов  $H$  (количество алертов на одного сотрудника SOC за смену) и ограничениями на  $MTTD$ , используемыми при оценке эффективности центров мониторинга безопасности [9].

Среднее время обнаружения ( $MTTD$ ) за период наблюдения  $T$  по множеству инцидентов  $I$  определяется как

$$MTTD = \frac{1}{|I|} \cdot \sum_{i \in I} (t_{det}(i) - t_{start}(i)),$$

где  $t_{start}(i)$  — момент первого события, включённого в инцидент  $i$ ,  $t_{det}(i)$  — время первой валидной тревоги по этому инциденту. На практике  $t_{start}$  извлекается из корреляционных графов SIEM/EDR-средств,  $t_{det}$  — из журналов оповещений;  $MTTD$  нормируется в системе управления инцидентами.

Критерий оптимальности формулируется как задача условной оптимизации при выборе конфигурации  $x$  (включая число контролируемых параметров  $n$ , число агрегированных индикаторов  $k$  и инфраструктурные параметры). Требуется минимизировать совокупную «углеродную стоимость»:

$$CS_{tot}(x) = E_{IT}(x) \cdot PUE \cdot CIF$$

при ограничениях:

$$S(x) \geq S_{min}, MTTD(x) \leq T_{det}, H(x) \leq H_{max}.$$

Эквивалентная безусловная постановка вводится через функцию штрафов:

$$J(x) = CS_{tot}(x) + \lambda_s \cdot \max(0, S_{min} - S(x)) + \lambda_t \cdot \max(0, MTTD(x) - T_{det}) + \lambda_h \cdot \max(0, H(x) - H_{max}),$$

где  $\lambda_s, \lambda_t, \lambda_h \geq 0$  — коэффициенты штрафов.

Конфигурация считается близкой к оптимальной сложности по  $k$ , если предельный прирост защищённости равен предельной «углеродной цене» добавления индикатора:

$$\frac{\partial S}{\partial k} \sim \omega \cdot \frac{\partial CS_{tot}}{\partial k}.$$

В дискретном виде используется правило останова: добавление нового индикатора допустимо, пока  $\frac{\Delta S}{\Delta CS_{tot}} \geq \omega^*$ , после чего запускается фаза упрощения.

## Методологические основы и модели оценки углеродного следа

### Энергетические и углеродные метрики

В соответствии с современными подходами к оценке экологической эффективности центров обработки данных в качестве базовых используются показатели PUE (Power Usage Effectiveness), CUE (Carbon Usage Effectiveness) и WUE (Water Usage Effectiveness)<sup>6</sup> [10, 11]. Для СППР, размещённой в ЦОД, углеродный след за расчётный период  $T$  можно оценить по формуле:

$$CS_{tot} = E_{IT} \cdot PUE \cdot CIF,$$

где  $E_{IT}$  — потреблённая ИТ-оборудованием электрическая энергия за период  $T$ ,  $PUE$  — отношение полной энергии ЦОД к энергии ИТ-нагрузки,  $CIF$  — коэффициент углеродоёмкости электроэнергии региона [13].  $WUE$  используется для отдельной оценки водного следа ЦОД и непосредственно не входит в базовую формулу расчёта углеродного следа. Учёт выбросов, связанных с водоснабжением и водоотведением, возможен только при введении отдельного коэффициента углеродной интенсивности воды.

В рамках системного анализа СППР рассматривается как совокупность подсистем с разной динамикой нагрузки (сбор логов, анализ, хранение, визуализация). Для каждой подсистемы оценивается *удельный углеродный след на единицу полезного функционала* (например, на один обработанный инцидент или на единицу времени мониторинга заданного множества показателей), что позволяет сопоставлять различные архитектурные решения.

### Параметры калибровки и источники данных

Для калибровки моделей углеродного следа используются агрегированные эксплуатационные данные трёх корпоративных СППР, обслуживающих от 5 до 20 тыс. узлов наблюдения. В регистре входных данных формируются почасовые или посуточные ряды за период наблюдения:

$$\{n_t, k_t, E_{IT_t}, PUE_t, CIF_t, WUE_t, Inc_t, MTTD_t, FNR_t, FPR_t, H_t\},$$

где  $Inc_t$  — число инцидентов за интервал  $t$ .

Для каждого интервала  $t$  вычисляется совокупный углеродный след:

$$CS_t = E_{IT_t} \cdot PUE_t \cdot CIF_t,$$

после чего выполняется оценивание параметров моделей.

Источники данных:

<sup>6</sup> Kern, E. Sustainable software products—towards assessment criteria for resource and energy efficiency / E. Kern, L. M. Hilty, A. Guldner, Y. V. Maksimov, A. Filler, J. Gröger, S. Naumann // Future Generation Computer Systems. 2018. Vol. 86. P. 199—210. DOI: 10.1016/j.future.2018.02.044.

$E_{IT,t}$  — электрическая энергия, потреблённая относимым к СППР ИТ-оборудованием за интервал  $t$ , включая серверы, системы хранения данных и сетевое оборудование; определяется по счётчикам на выходе PDU, питающего соответствующую ИТ-нагрузку, либо по агрегированной телеметрии всех относимых к СППР ИТ-ресурсов. Энергопотребление систем охлаждения, освещения, ИБП и иной инженерной инфраструктуры ЦОД  $E_{it}$ , не включается.

$PUE_t$  — показатель энергетической эффективности, получаемый из отчётности и системы мониторинга ЦОД;  $WUE_t$  — показатель водоиспользования ЦОД, применяемый для отдельной оценки водного следа и не входящий непосредственно в базовую формулу расчёта углеродного следа  $CS_t$ .

$CIF_t$  — региональные коэффициенты углеродоёмкости электроэнергии по открытым статистическим источникам [13]; эксплуатационные метрики  $MTTD_t, FNR_t, FPR_t$  и  $H_t$  — журналы SIEM/SOC и системы управления инцидентами.

#### Степенная модель экстенсивной параметризации

Для степенной модели

$$CS_L(n) = \alpha \cdot n^\beta + \gamma$$

используется два варианта оценивания параметров:

(а) при малом  $\gamma$  применяется лог-линейная регрессия:

$$\log CS_t = \log \alpha + \beta \log n_t + \varepsilon_t.$$

(б) в общем случае используются нелинейные наименьшие квадраты по  $(\alpha, \beta, \gamma)$  с робастной функцией потерь (Huber, Tukey), устойчивой к выбросам.

#### Асимптотическая модель оптимальной сложности

Для асимптотической модели

$$CS_A(k) = \lambda(1 - e^{-\varphi k}) + \theta$$

параметры  $(\lambda, \varphi, \theta)$  оцениваются по парам  $(k_i, CS_i)$ , полученным при последовательном укрупнении и агрегировании индикаторов.

В качестве начальных приближений принимаются:

$$\begin{aligned} \lambda &\approx \max(CS) - \min(CS), \theta \approx \\ &\approx \min(CS), \varphi \approx -\frac{\ln(1 - 0.63)}{k_0}, \end{aligned}$$

где  $k_0$  — точка, в которой достигается  $\approx 1 - e^{-1}$  насыщения.

#### Калибровка коэффициента операционной эффективности

Коэффициент операционной эффективности  $OEA(k) \in (0; 1]$  калибруется по наблюдаемым зависимостям  $MTTD$  и  $FNR$  от числа активных индикаторов  $k$ . В простейшей параметризации используется экспоненциальное убывание эффективности:

$$OEA(k) = \exp(-\eta \cdot \max(0, k - k^*)). \quad (6)$$

где  $k^*$  — операторский порог когнитивной нагрузки,  $\eta$  — коэффициент снижения эффективности, оцениваемый регрессией.

#### Инфраструктурный сглаживающий коэффициент «зелёных» практик

Инфраструктурный сглаживающий коэффициент  $SF(n, k) \in (0; 1]$  отражает эффекты «зелёных» практик эксплуатации: виртуализации, авто-масштабирования и повторного использования энергии (heat reuse) [6, 7, 9, 14]. Возможная факторная форма:

$$\begin{aligned} SF(n, k) &= \\ &= (1 - a \cdot VR)(1 - b \cdot AS)(1 - c \cdot ERE_{norm}), \end{aligned} \quad (7)$$

где  $VR$  — доля виртуализированных/контейнеризованных нагрузок,  $AS$  — доля времени с активным авто-масштабированием,  $ERE_{norm}$  — нормированная эффективность утилизации тепла; коэффициенты  $a, b, c \in [0, 1]$  подбираются по данным.

#### Экспоненциальное сглаживание временного ряда углеродного следа

Для подавления краткосрочных всплесков в отчётности используется экспоненциальное сглаживание временного ряда углеродного следа:

$$\begin{aligned} CS(t) &= \rho CS(t-1) + \\ &+ (1 - \rho) CS(t), \rho \in [0; 1] \end{aligned} \quad (8)$$

Здесь  $CS(t)$  — сглаженный углеродный след, а  $\rho$  задаёт «память» сглаживания; типичные значения  $\rho$  находятся в диапазоне 0,2—0,4.

#### **Модели оценки углеродного следа** **Модель экстенсивной параметризации**

При экстенсивном подходе операторы и аналитики постепенно увеличивают число контролируемых факторов  $n$ : источников событий, правил корреляции, сигнатур, пользовательских показателей, фильтров и отчётов. В такой логике развития набор факторов, на которые реагирует СППР, практически не имеет верхней границы и определяется преимущественно локальными потребностями и «гипотезами» аналитиков. Это приводит к росту объёма обрабатываемых данных, числа вычислительных операций и обращений к хранилищам, а также к усложнению панелей мониторинга.

На основе аппроксимации эксплуатационных данных трёх корпоративных СППР получена степенная модель углеродного следа:

$$CS_L(n) = \alpha \cdot n^\beta + \gamma. \quad (9)$$

где  $CS_L(n)$  — совокупный углеродный след СППР;  $\alpha$  и  $\gamma$  — параметры калибровки;  $\beta$  — показатель степени. В большинстве наблюдений  $\beta$  лежит в диапазоне 1,6—2,2, что свидетельствует о суперлинейном характере роста экологической нагрузки при увеличении числа параметров. Иначе говоря, каждое новое правило корреляции в среднем «стоит» больше, чем предыдущее, с точки зрения углеродного следа.

Суперлинейность  $\beta > 1$  отражает не только линейный рост объёма данных, но и комбинаторное усложнение корреляции: увеличение числа соединений потоков, размеров окон анализа, требуемых объёмов оперативной памяти и операций ввода-вывода. При росте  $n$  растут очереди заданий, увеличивается частота конфликтов за ресурсы и объём кэшируемых состояний, что приводит к росту энергопотребления быстрее, чем линейно. Эмпирически полученные значения  $\beta \approx 1,6—2,2$  при среднем относительном отклонении модели от наблюдений не более 8% подтверждают суперлинейный характер роста.

#### Концепция оптимальной сложности

Альтернативный подход исходит из того, что оператор способен эффективно работать лишь с ограниченным числом агрегированных индикаторов  $k$ , отражающих ключевые аспекты защищённости инфраструктуры. При этом расширение набора индикаторов после некоторого порога приводит к снижению понимаемости картин инцидентов и росту вероятности операторских ошибок.

Для описания зависимости приведённого углеродного следа от числа агрегированных индикаторов  $k$  используется асимптотическая модель:

$$CS_A(k) = \lambda(1 - \exp(-\phi k)) + \theta. \quad (10)$$

где  $CS_A(k)$  — приведённый углеродный след при фиксированном уровне информационной достаточности панелей мониторинга;  $\lambda$  и  $\theta$  — параметры масштаба;  $\phi$  — коэффициент нарастания полезной нагрузки. Модель отражает эффект насыщения: по мере увеличения  $k$  достигается плато, при котором добавление новых индикаторов не даёт существенной дополнительной информации, но требует ресурсов ЦОД и увеличивает когнитивную нагрузку оператора.

С учётом  $OEA(k)$  интегральная «эффективная» полезная нагрузка панели может быть описана как:

$$S_{eff}(k) = S(k) \cdot OEA(k).$$

В окрестности порогового значения  $k^*$  достигается максимум  $S_{eff}(k)$  при умеренных значениях  $k$ , что согласуется с концепцией оптимальной сложности.

#### **Спиральная модель эволюции СППР**

Для объединения сильных сторон обоих подходов предлагается рассматривать жизненный цикл СППР

как последовательность «витков спирали»<sup>7</sup>, на каждом из которых реализуются фазы расширения и упрощения конфигурации. На фазе расширения осуществляется интенсивное накопление правил и индикаторов с целью повышения полноты контроля (рост  $n$  и  $k$ ), на фазе упрощения выполняются агрегирование, укрупнение и удаление низкоэффективных элементов.

Совокупный углеродный след на  $i$ -м витке спиральной эволюции описывается выражением:

$$CS_S(i) = CS_L(n_i) \cdot OEA(k_i) \cdot SF(n_i, k_i). \quad (11)$$

Здесь  $OEA(k_i) \in (0; 1]$  характеризует операционную эффективность при числе агрегированных индикаторов  $k_i$  а  $SF(n_i, k_i)$  — сглаживающий коэффициент, учитывающий эффекты переиспользования инфраструктуры и внедрения «зелёных» практик.

Алгоритм управления конфигурацией СППР в такой модели включает регулярные (например, квартальные) циклы пересмотра перечня правил и индикаторов с оценкой их вклада как в показатели безопасности (доля предотвращённых инцидентов, MTDD, FNR/FPR), так и в углеродный след. Правила, дающие минимальный прирост защищённости при значимых ресурсных затратах, подлежат укрупнению или исключению.

Фазовый переход от расширения к упрощению инициируется при достижении порога:

$$\frac{\Delta S}{\Delta CS} < \omega^*,$$

и/или при нарушении ограничений по MTDD и Н.

#### **Перспективы работы с результатами исследования**

На основе собранных эксплуатационных данных о трёх корпоративных СППР, обслуживающих от 5 до 20 тыс. узлов, была проведена калибровка моделей (9)—(11). Для сценариев экстенсивной параметризации коэффициент  $\beta$  в (9) принимал значения в диапазоне 1,6—2,2, а среднее относительное отклонение модели от наблюдений не превышало 8%. Это подтверждает гипотезу о суперлинейном росте углеродного следа при добавлении новых правил корреляции и источников событий.

Для сценариев ограничения сложности и агрегирования показателей выявлено, что зависимость полезной функциональности от числа индикаторов хорошо описывается асимптотической моделью (10): начиная с  $k \approx 25—30$  прирост информативности панелей мониторинга становится пренебрежимо малым по сравнению с ростом ресурсопотребления и нагрузки на операторов. Практически это означает, что расширение наборов метрик выше указанного порога не оправдано ни с точки зрения операторской эффективности, ни с точки зрения углеродного следа.

<sup>7</sup> Boehm, B. A Spiral Model of Software Development and Enhancement // Computer. 1988. Vol. 21, № 5. P. 61—72. DOI: 10.1109/2.59.



Имитационные эксперименты со спиральной схемой (11) показали, что чередование фаз расширения и последующей оптимизации конфигурации позволяет снизить совокупный углеродный след СППР в среднем на 20—30% за двухлетний горизонт планирования по сравнению с вариантом монотонной экстенсивной параметризации при сопоставимых метриках защищённости. Дополнительно наблюдалось снижение доли потерянных пакетов и отказов в обслуживании при пиковой нагрузке, рост эффективной пропускной способности инфраструктуры примерно на 15%, а также сокращение доли успешно реализованных атак на 20—25% за счёт улучшения видимости и снижения MTTD.

С точки зрения эксплуатационных практик важным результатом является формирование набора ориентиров для эксплуатации СППР: целевые значения  $PUE \leq 1,4$  для площадок, обслуживающих центры мониторинга безопасности; учёт CUE и WUE при планировании модернизаций и выборе площадок размещения; регламенты квартального пересмотра правил и панелей мониторинга с включением углеродных показателей в отчётность по информационной безопасности [10]. Такие регламенты естественным образом интегрируются в существующие системы менеджмента информационной безопасности и корпоративные системы устойчивого развития.

Сопоставление моделей  $CS_L(n)$  и  $CS_A(k)$ , а также спиральной схемы  $CS_S(i)$  (Сопоставление степенной модели (9), асимптотической модели (10) и спиральной схемы (11)) с учётом оценённых параметров  $\beta, \lambda, \varphi, \theta$  и эксплуатационных метрик  $S$ , MTTD и  $H$  позволяет выделить области применимости каждого подхода и дать количественную оценку компромисса между уровнем защищённости и углеродным следом.

Преимущества экстенсивной параметризации ( $CS_L$ ):

- высокая полнота покрытия и гибкость настройки за счёт большого числа правил, источников событий и детализированных индикаторов;
- возможность включения редких и сложных сценариев атак, что позволяет увеличивать показатель  $S$  при сохранении заданных ограничений по MTTD;
- сравнительно простая организационная модель развития системы (подход «добавлять всё, что может быть полезно»), не требующая на первых этапах сложных процедур агрегирования и регламентов регулярного пересмотра конфигурации.

Риски и ограничения экстенсивного подхода: суперлинейный рост углеродного следа и затрат ресурсов ЦОД при увеличении  $n$ : в модели

$$CS_L(n) = \alpha \cdot n^\beta + \gamma, \beta > 1,$$

что приводит к ускоренному росту  $CS_{tot}$  и необходимости опережающих инвестиций в инфраструктуру; деградация операционной эффективности OEA( $k$ ) вследствие перегрузки панелей мониторинга и увели-

чения MTTD, когда оператор вынужден обрабатывать избыточный объём сигналов и отчётов; рост FPR и FNR при превышении когнитивного порога  $k^*$ , обусловленный «шумом» в потоке оповещений и снижением внимания к слабым, но значимым индикаторам.

Преимущества подхода оптимальной сложности ( $CS_A$ ):

управляемая когнитивная нагрузка на операторов и предсказуемое насыщение информативности: асимптотическая модель

$$CS_A(k) = \lambda(1 - e^{-\varphi k}) + \theta$$

показывает, что после достижения диапазона  $k \approx 25$ —30 дальнейшее расширение набора индикаторов практически не увеличивает полезную функциональность панелей мониторинга;

возможность формализованного выбора числа индикаторов  $k$  на основе критерия  $\frac{\Delta S}{\Delta CS}$  и порога  $\omega^*$ , что позволяет количественно обосновывать решения о включении новых показателей с точки зрения их «углеродной цены».

Риски чрезмерной агрегации:

- потенциальное недообнаружение редких и сложных сценариев атак при слишком сильном укрупнении показателей и сокращении исходного множества правил;
- необходимость высококвалифицированной аналитической поддержки и наличия репрезентативных эмпирических данных для построения устойчивых агрегированных индексов и регулярной перенастройки моделей.

Синтетическая спиральная схема, объединяющая фазы расширения и упрощения конфигурации, компенсирует перечисленные недостатки: экстенсивный этап обеспечивает накопление статистики и тестирование новых правил, а этап оптимизации, опирающийся на уравнения (9)—(11) настоящей работы, позволяет удерживать  $CS_{tot}$  в целевом диапазоне за счёт исключения низкоэффективных правил и ограничения  $k$  вблизи значений, обеспечивающих максимум эффективной полезной нагрузки:

$$S_{eff}(k) = S(k) \cdot OEA(k).$$

Имитационные эксперименты показывают, что такая схема даёт выигрыш по углеродному следу при сохранении требуемых эксплуатационных метрик.

## Заключение

Выполнен системный анализ СППР как сложной человеко-машинной системы в контуре SOC и сопоставлены две траектории её эволюции — экстенсивная параметризация и концепция оптимальной сложности — с точки зрения их влияния на углеродный след, загрузку инфраструктуры и требования к оператору.

Предложен комплекс формализованных моделей оценки углеродного следа СППР:

степенная модель  $CS_L(n)$  для сценариев экстенсивного наращивания числа параметров,



$$CS_L(n) = \alpha \cdot n^\beta + \gamma;$$

асимптотическая модель  $CS_A(k)$  для сценариев ограничения сложности,

$$CS_A(k) = \lambda(1 - e^{-\varphi k}) + \theta;$$

спиральная модель  $CS_S(i)$ , учитывающая чередование фаз расширения и упрощения, операционную эффективность OEA(k) и инфраструктурный коэффициент SF(n, k),

$$CS_S(i) = CS_L(n_i) \cdot OEA(k_i) \cdot SF(n_i, k_i).$$

Введён интегральный показатель защищённости S и критерий оптимальности, позволяющий совместно учитывать S, MTTD, H и совокупный углеродный след  $CS_{tot}$ .

На основе аппроксимации эксплуатационных данных трёх корпоративных СППР и имитационных экспериментов показано, что при экстенсивной параметризации зависимость  $CS_L(n)$  характеризуется суперлинейным ростом с показателем степени  $\beta \approx 1,6$ —2,2, а в парадигме оптимальной сложности информативность панелей мониторинга насыщается при  $k \approx 25$ —30. Моделирование спиральной схемы продемонстрировало снижение совокупного углеродного следа на 20—30% на двухлетнем горизонте по сравнению с монотонной экстенсивной параметризацией при сопоставимых значениях S и MTTD.

Сформулированы практические рекомендации по внедрению предложенной методики в эксплуатацию центров мониторинга безопасности: включение показателей PUE, CUE, WUE и CIF в регламентную отчётность SOC; проведение регулярных циклов пересмотра правил и панелей мониторинга с учётом углеродной «цены» новых индикаторов; использование ограничений по MTTD и нагрузке H для предотвращения операторской перегрузки. Такой подход согласует задачи

кибербезопасности, экономии ресурсов и устойчивого развития в едином контуре управления  $\frac{\Delta S}{\Delta CS}$  и пороговых значений MTTD и H для принятия решений о добавлении или укрупнении индикаторов. Такой подход обеспечивает согласование задач кибербезопасности и целей устойчивого развития в едином контуре управления.

Достоверность результатов подтверждается сопоставлением моделей с эксплуатационными данными нескольких реальных СППР и их согласованностью с опубликованными исследованиями по энергопотреблению ИКТ-инфраструктуры и рекомендациями The Green Grid по метрикам PUE/CUE/WUE. Ограничением работы является фокус на корпоративных системах мониторинга с определённым масштабом нагрузки; дальнейшие исследования могут быть направлены на расширение выборки систем, учёт распределённых облачных архитектур [13—15] и уточнение моделей учёта косвенных выбросов. Тем не менее предложенная методика уже может служить основой для формирования корпоративных стандартов «зелёной» эксплуатации СППР в области информационной безопасности.

### Практическое подтверждение/достоверность

Достоверность и практическая применимость предложенных научных решений подтверждаются сопоставлением моделей с эксплуатационными данными корпоративных систем мониторинга и реагирования, а также согласованностью используемых метрик и подходов с актуальными рецензируемыми публикациями, по оценке углеродной интенсивности вычислений и эффективности центров мониторинга безопасности.

### Литература

1. Lannelongue, L. Green Algorithms: Quantifying the Carbon Footprint of Computation / L. Lannelongue, J. Grealey, M. Inouye // Advanced Science. 2021. Vol. 8, № 12. 2100707. DOI: 10.1002/adv.202100707.
2. Lannelongue, L. Ten simple rules to make your computing more environmentally sustainable / L. Lannelongue, J. Grealey, A. Bateman, M. Inouye // PLoS Computational Biology. 2021. Vol. 17, № 9. e1009324. DOI: 10.1371/journal.pcbi.1009324.
3. Lannelongue, L. GREENER principles for environmentally sustainable computational science / L. Lannelongue, H.-E. G. Aronson, A. Bateman [et al.] // Nature Computational Science. 2023. Vol. 3, № 6. P. 514—521. DOI: 10.1038/s43588-023-00461-y.
4. Lannelongue, L. Carbon footprint estimation for computational research / L. Lannelongue, M. Inouye // Nature Reviews Methods Primers. 2023. Vol. 3. Article 1. DOI: 10.1038/s43586-023-00202-5.
5. Nazare, T. Green computing for energy transition: a survey / T. Nazare, J. Gadelha, E. Nepomuceno, R. Lozi // IEEE Latin America Transactions. 2023. Vol. 21, № 9. P. 937—948. DOI: 10.1109/TLA.2023.10251799.
6. González Granadillo, G. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures / G. González Granadillo, S. González Zarzosa, R. Diaz // Sensors. 2021. Vol. 21, № 14. 4759. DOI: 10.3390/s21144759.
7. Forsberg, J. Technical performance metrics of a security operations center / J. Forsberg, T. Frantti // Computers & Security. 2023. Vol. 135. 103529. DOI: 10.1016/j.cose.2023.103529.
8. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. 3rd ed. Hoboken: Wiley, 2020. 1232 p. DOI: 10.1002/9781119644682.

9. Masanet, E. Recalibrating global data center energy use estimates / E. Masanet, A. Shehabi, N. Lei, S. J. Smith, J. Koomey // Science. 2020. Vol. 367, № 6481. P. 984—986. DOI: 10.1126/science.aba3758.
10. Siddik, M. A. B. The environmental footprint of data centers in the United States / M. A. B. Siddik, A. Shehabi, L. Marston // Environmental Research Letters. 2021. Vol. 16, № 6. 064017. DOI: 10.1088/1748-9326/abfba1.
11. Gupta, U. Chasing Carbon: The Elusive Environmental Footprint of Computing / U. Gupta, Y. G. Kim, S. Lee, J. Tse, H. H. S. Lee, G.-Y. Wei, D. Brooks, C.-J. Wu // Proc. IEEE HPCA. 2021. P. 854—867. DOI: 10.1109/HPCA51647.2021.00076.
12. Dallel, H. Modeling the Green Cloud Continuum: integrating energy considerations into Cloud–Edge models / H. Dallel, A. Ksentini [et al.] // Cluster Computing. 2024. Vol. 27. P. 4095—4125. DOI: 10.1007/s10586-024-04383-w.
13. Hankendi C., Coskun A. K., Sovacool B. K. Why transparency matters for sustainable data centers and carbon-neutral artificial intelligence (AI) // iScience. 2025. Vol. 28, № 11. 113705. DOI: 10.1016/j.isci.2025.113705
14. Schwartz, R. Green AI / R. Schwartz, J. Dodge, N. A. Smith, O. Etzioni // Communications of the ACM. 2020. Vol. 63, № 12. P. 54—63. DOI: 10.1145/3381831.
15. Strubell, E. Energy and policy considerations for deep learning in NLP / E. Strubell, A. Ganesh, A. McCallum // Proc. ACL. 2019. P. 3645—3650. DOI: 10.18653/v1/P19-1355.

SECTION:

SYSTEM ANALYSIS, MANAGEMENT, ARTIFICIAL INTELLIGENCE, AND INFORMATION PROTECTION

## A METHODOLOGY FOR OPTIMIZING A COMPLEX HUMAN–MACHINE DECISION SUPPORT SYSTEM IN INFORMATION SECURITY CONSIDERING CARBON INTENSITY

Isaev N.A.<sup>8</sup>

**Keywords:** monitoring, correlation, response, alerts, resource intensity, energy efficiency, telemetry, parametrisation, configuration, detection.

### Abstract

**Purpose of work** is to develop a reproducible methodology for optimising the human-machine monitoring and incident response loop in information security (a security monitoring centre analyst and a decision support software system) according to three groups of criteria: the level of cybersecurity, the operator's cognitive load, and the carbon intensity of computing infrastructure operation.

**Research methods:** system analysis of architecture and response processes, mathematical and simulation modelling of energy consumption and CO<sub>2</sub>-equivalent emissions, statistical processing of operational data, and expert assessment of operator factors. As a formal core, the study introduces a normalised security index, metrics for detection time and operator workload, as well as a calculation of configuration carbon intensity based on IT load energy consumption and site energy efficiency parameters.

**Results of the study.** Models of environmental cost growth under extensive parametrisation and a saturation model under complexity constraints have been formulated. A spiral configuration management algorithm has been developed, featuring a stopping rule based on marginal efficiency (the ratio of security gain to the “carbon cost” of increased complexity). The practical effect consists in reducing the share of low-efficiency rules and excess telemetry while maintaining detection time and detection quality requirements, which can be used to justify the modernisation of corporate security monitoring centres and to include environmental indicators in routine reporting. Experimental verification using data from three corporate DSSs (5—20 thousand nodes) confirmed the models' operability: under extensive parameter expansion, a superlinear growth of the carbon footprint was recorded ( $\beta \approx 1.6—2.2$ ), and the spiral scheme made it possible to reduce CO<sub>2</sub>-equivalent emissions by 20—30% over two years without degrading key cybersecurity metrics (MTTD, FNR/FPR).

---

<sup>8</sup> **Nikolay A. Isaev**, Ph.D. student, Moscow Witte University, Moscow, Russia. ORCID: 0009-0007-3987-1670.  
E-mail: [supercopen@yandex.ru](mailto:supercopen@yandex.ru)

## References

1. Lannelongue, L. Green Algorithms: Quantifying the Carbon Footprint of Computation / L. Lannelongue, J. Grealey, M. Inouye // *Advanced Science*. 2021. Vol. 8, № 12. 2100707. DOI: 10.1002/advs.202100707.
2. Lannelongue, L. Ten simple rules to make your computing more environmentally sustainable / L. Lannelongue, J. Grealey, A. Bateman, M. Inouye // *PLoS Computational Biology*. 2021. Vol. 17, № 9. e1009324. DOI: 10.1371/journal.pcbi.1009324.
3. Lannelongue, L. GREENER principles for environmentally sustainable computational science / L. Lannelongue, H.-E. G. Aronson, A. Bateman [et al.] // *Nature Computational Science*. 2023. Vol. 3, № 6. P. 514—521. DOI: 10.1038/s43588-023-00461-y.
4. Lannelongue, L. Carbon footprint estimation for computational research / L. Lannelongue, M. Inouye // *Nature Reviews Methods Primers*. 2023. Vol. 3. Article 1. DOI: 10.1038/s43586-023-00202-5.
5. Nazare, T. Green computing for energy transition: a survey / T. Nazare, J. Gadelha, E. Nepomuceno, R. Lozi // *IEEE Latin America Transactions*. 2023. Vol. 21, № 9. P. 937—948. DOI: 10.1109/TLA.2023.10251799.
6. González Granadillo, G. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures / G. González Granadillo, S. González Zarzosa, R. Diaz // *Sensors*. 2021. Vol. 21, № 14. 4759. DOI: 10.3390/s21144759.
7. Forsberg, J. Technical performance metrics of a security operations center / J. Forsberg, T. Frantti // *Computers & Security*. 2023. Vol. 135. 103529. DOI: 10.1016/j.cose.2023.103529.
8. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. 3rd ed. Hoboken: Wiley, 2020. 1232 p. DOI: 10.1002/9781119644682.
9. Masanet, E. Recalibrating global data center energy use estimates / E. Masanet, A. Shehabi, N. Lei, S. J. Smith, J. Koomey // *Science*. 2020. Vol. 367, № 6481. P. 984—986. DOI: 10.1126/science.aba3758.
10. Siddik, M. A. B. The environmental footprint of data centers in the United States / M. A. B. Siddik, A. Shehabi, L. Marston // *Environmental Research Letters*. 2021. Vol. 16, № 6. 064017. DOI: 10.1088/1748-9326/abfba1.
11. Gupta, U. Chasing Carbon: The Elusive Environmental Footprint of Computing / U. Gupta, Y. G. Kim, S. Lee, J. Tse, H. H. S. Lee, G.-Y. Wei, D. Brooks, C.-J. Wu // *Proc. IEEE HPCA*. 2021. P. 854—867. DOI: 10.1109/HPCA51647.2021.00076.
12. Dallel, H. Modeling the Green Cloud Continuum: integrating energy considerations into Cloud–Edge models / H. Dallel, A. Ksentini [et al.] // *Cluster Computing*. 2024. Vol. 27. P. 4095—4125. DOI: 10.1007/s10586-024-04383-w.
13. Hankendi C., Coskun A. K., Sovacool B. K. Why transparency matters for sustainable data centers and carbon-neutral artificial intelligence (AI) // *iScience*. 2025. Vol. 28, № 11. 113705. DOI: 10.1016/j.isci.2025.113705.
14. Schwartz, R. Green AI / R. Schwartz, J. Dodge, N. A. Smith, O. Etzioni // *Communications of the ACM*. 2020. Vol. 63, № 12. P. 54—63. DOI: 10.1145/3381831.
15. Strubell, E. Energy and policy considerations for deep learning in NLP / E. Strubell, A. Ganesh, A. McCallum // *Proc. ACL*. 2019. P. 3645—3650. DOI: 10.18653/v1/P19-1355.



# ИНТЕРПРЕТАЦИОННАЯ МОДЕЛЬ НАБЛЮДЕНИЯ И ДИАГНОСТИРОВАНИЯ СОСТОЯНИЯ ЭЛЕМЕНТОВ БЛОКЧЕЙН-СИСТЕМ ПО РЕШЕНИЯМ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ

Лисов Д.Н.<sup>1</sup>

**Ключевые слова:** объяснимый искусственный интеллект, локальные атрибуции признаков, бинарная классификация угроз, качество объяснения, диагностический профиль, доверие к прогнозу, подозрительная активность, аналитическая проверка, новые угрозы безопасности, сетевые вторжения.

## Аннотация

**Цель работы:** разработать интерпретационную модель наблюдения и диагностирования состояния элементов блокчейн-систем при появлении угроз нового типа путем совместного анализа прогнозов моделей машинного обучения и результатов их локальной интерпретации.

**Методы исследования:** выполнена функциональная декомпозиция наблюдения, включающего получение прогноза, построение локального объяснения, количественную оценку его свойств и формирование диагностического заключения. Для количественной оценки локального объяснения использованы две метрики качества: верность и устойчивость. Метрика верности показывает, насколько замена выделенных объяснителем признаков изменяет выход модели по сравнению с заменой случайного набора, а метрика устойчивости характеризует сохранение состава значимых признаков у близких объектов с сопоставимым прогнозом. Значения метрик определялись путем контролируемой замены входных признаков и сопоставления локальных объяснений, а их диагностическая информативность оценивалась с помощью характеристических кривых. При экспериментальном воспроизведении угрозы нового типа один тип атаки исключался из обучающих данных и сохранялся в тестовой выборке, после чего проверялись методы объяснения и их сочетания.

**Результаты исследования:** предложена интерпретационная модель, в которой результат локального объяснения включается в наблюдение за решением ML-модели и формирование диагностического состояния объекта. Измеримые свойства объяснения преобразуются в вектор показателей, по которому определяется уровень доверия. Если диагностический профиль объяснения не соответствует характерным профилям известных корректных решений, объект получает промежуточное состояние «подозрительное» и сохраняется для дополнительной проверки. Экспериментальное исследование показало, что показатели качества объяснения содержат диагностическую информацию, не представленную в выходном классе модели, однако ее выраженность зависит от данных и применяемого объяснителя. При поступлении активности, отсутствовавшей в обучающих данных, интерпретационный контур позволил сохранить в области наблюдения часть объектов, пропущенных базовой моделью. Совместное использование нескольких методов объяснения оказалось полезным только при взаимном дополнении получаемых атрибуций и не обеспечило универсального преимущества. Полученные результаты подтверждают возможность выделять решения, требующие дополнительной проверки при появлении ранее не наблюдавшихся угроз. Базовый классификатор при этом не изменяется, а подозрительное состояние не отождествляется с атакой.

DOI: 10.24412/1994-1404-2026-3-88-99

## Введение и постановка задачи

Национальные блокчейн-системы и платформы экономики данных представляют собой распределенные цифровые инфраструктуры, объединяющие узлы хранения и обработки данных, сетевые

и интеграционные сервисы, средства удостоверения, механизмы исполнения транзакций, смарт-контракты и прикладные приложения. Взаимозависимость перечисленных компонентов приводит к тому, что локаль-

<sup>1</sup> Лисов Дмитрий Николаевич, аспирант, младший научный сотрудник центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус», пгт Сириус, Краснодарский край, Российская Федерация. ORCID: 0000-0002-8214-4109.

E-mail: lisov.dn@talantiuspeh.ru



ное нарушение способно повлиять на выполнение функций всей системы. Поэтому ее защищенность определяется не только стойкостью отдельных механизмов безопасности, но и способностью продолжать функционирование при изменении условий и характера деструктивных воздействий [1]. Необходимость обеспечения такой способности обоснована в концепции киберустойчивости национальных цифровых платформ и блокчейн-экосистем [2], а возможные направления воздействия на элементы блокчейн-инфраструктуры конкретизированы в модели квантовых угроз [3]. Систематический учет изменения угроз и появления новых сценариев их реализации предусмотрен также Методикой оценки угроз безопасности информации ФСТЭК России<sup>2</sup>. В этих условиях противодействие угрозам нового типа требует не только совершенствования предотвращающих мер, но и развития средств наблюдения, позволяющих обнаруживать изменения состояния элементов системы при неполноте предварительных сведений о возможном воздействии.

Источниками сведений о состоянии блокчейн-системы могут служить сетевой трафик, параметры транзакций, обращения к программным интерфейсам, события интеграционных сервисов и результаты выполнения прикладных функций. В исследованиях эти данные используются при разработке средств обнаружения аномалий, мошенничества и вредоносной активности на основе машинного обучения. Основные направления объединения блокчейн-технологий и ML систематизированы в работе [4], а в исследовании [5] классификаторы применены для выявления аномальных транзакций с последующим объяснением полученных решений. ML-модель в таких разработках выступает одним из возможных средств распознавания угроз, применимость которого определяется архитектурой и назначением конкретного элемента. Поэтому настоящее исследование ограничено теми элементами блокчейн-системы, для которых решение задачи распознавания угроз предусматривает использование ML-модели.

При включении ML-модели в контур, связанный с безопасностью, возникает вопрос о контролируемости сформированных ею решений [6]. Выходной класс показывает результат распознавания, но не раскрывает, какие свойства объекта определили этот результат и соответствует ли поведение модели изученным закономерностям. Методы объяснимого искусственного интеллекта частично устраняют эту неопределенность и позволяют установить влияние отдельных признаков на прогноз [7, 8]. В существующих системах обнаружения вторжений объяснение преимущественно сопровождает уже полученное решение. В XAI-XGBoost методы SHAP и LIME используются для глобального и локального анализа прогнозов модели [9]. В рабо-

те [10] угрозы нулевого дня распознаются специализированной ML-моделью, а LIME и SHAP применяются для последующего анализа результата. Аналогичная последовательность используется в системе X-CBA [11]. Рассмотренные решения повышают прозрачность обнаружения и позволяют специалисту проверить содержательные основания прогноза, однако результат интерпретации не участвует в определении состояния объекта и не показывает, насколько свойства полученного объяснения согласуются с решением классификатора.

Попытки включить XAI непосредственно в дальнейшую обработку данных привели к появлению более сложных архитектур. В работе [12] атрибуции первой модели поступают на вход дополнительному классификатору, благодаря чему выявленные XAI зависимости используются при повторном распознавании DDoS-атак. Другой способ операционного применения объяснений предложен в работе [13]. В разработанной авторами федеративной системе SHAP обеспечивает прослеживаемость решений агентов, используется для выявления нестабильного поведения и участвует в ограничении влияния потенциально скомпрометированных узлов на обновление общей модели. Обе работы подтверждают, что результаты интерпретации могут применяться не только для представления прогноза. Вместе с тем в первом случае создается дополнительный обучаемый детектор, а во втором изменяется политика федеративного обновления. Следовательно, XAI встраивается в механизм обучения или адаптации, тогда как задача независимого наблюдения за уже сформированным прогнозом остается нерешенной.

Наиболее близкий к указанной задаче подход предложен Mougan и соавторами [14]. Авторы исходят из того, что изменение поступающих данных может проявляться не только в распределении входных признаков или прогнозов, но и в распределении объяснений. Атрибуции, рассчитанные для исходной и новой выборки, передаются бинарному классификатору, результат которого характеризует наличие сдвига объяснений. XAI здесь уже участвует в формировании показателя мониторинга, а не только сопровождает готовый прогноз. Тем не менее единицей наблюдения остается совокупность новых данных: подход устанавливает факт изменения взаимодействия модели с потоком объектов, но не формирует диагностическое заключение для каждого объекта, не оценивает качество его локального объяснения и не связывает полученную оценку с исходным классом. Смежная работа [15] посвящена оценке изменения производительности ML-модели и установлению входных признаков, связанных с предполагаемым ухудшением ее качества. XAI в этом случае объясняет результат мониторинга и помогает определить возможные причины деградации, однако также не используется для диагностирования отдельного объекта. Таким образом, существующие исследования содержат отдельные предпосылки интерпретационного наблюдения — локальное объяснение

<sup>2</sup> Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021). Пп. 2.4, 2.14 // СПС «КонсультантПлюс».

прогноза, использование атрибуций при дополнительном распознавании и обнаружение сдвига объяснений, но не устанавливают единой связи между прогнозом конкретного объекта, измеримыми свойствами его объяснения и диагностическим состоянием.

Для построения такой связи недостаточно использовать непосредственно значения атрибуций. Они характеризуют вклад признаков, но не позволяют установить, действительно ли выделенные признаки определяют поведение модели и сохраняется ли полученная структура объяснения относительно сопоставимых объектов. Необходимость количественной оценки XAI обоснована в систематическом обзоре [16], где показано, что качество объяснения оценивается с помощью групп метрик, характеризующих его верность, устойчивость, сложность и локализацию. Инструментарий Quantus предоставляет унифицированные процедуры вычисления соответствующих показателей [17], однако их значения зависят от модели, данных, объяснителя и способа проверки, что подтверждается критическим анализом современного состояния XAI [18]. В существующих исследованиях такие показатели преимущественно используются для сравнения объяснителей на выборке. Для наблюдения за состоянием объекта требуется иное применение: свойства объяснения должны оцениваться для конкретного прогноза, сохраняться в виде отдельных диагностических признаков и рассматриваться совместно с исходным выходом модели. Поскольку разные XAI-методы используют неодинаковые способы определения вклада признаков, сформированные ими объяснения и оценки их свойств могут различаться для одного объекта. Это различие создает основание для проверки как отдельных объяснителей, так и их совместного использования. При этом низкое качество объяснения не доказывает ошибочность прогноза и потому не должно приводить к его автоматической инверсии.

Научная проблема состоит в отсутствии формальной связи между бинарным прогнозом ML-модели, количественными свойствами его локального объяснения и диагностическим состоянием наблюдаемого элемента блокчейн-системы. Вследствие этого объяснение либо предъявляется после принятия решения, либо используется для изменения обучаемого механизма, но не обеспечивает независимое диагностирование конкретного объекта в рабочем цикле наблюдения. Гипотеза исследования заключается в том, что локальное объяснение содержит измеримые свойства решения классификатора, не представленные в его бинарном выходе, а их совместное рассмотрение с прогнозом позволяет выделять объекты, для которых принятое решение не получает достаточного интерпретационного подтверждения. Предполагается, что такие отклонения могут сопровождать появление ранее не наблюдавшихся угроз, однако сами по себе не являются доказательством атаки и требуют отдельного диагностического состояния. Дополнительно проверяется частное предположение о том, что совместное использование

результатов нескольких XAI-методов может повысить диагностическую информативность описания по сравнению с отдельным объяснителем за счет учета различий в определении значимости признаков.

Цель работы состоит в разработке интерпретационной модели наблюдения и диагностирования состояния элементов блокчейн-систем, для которых распознавание угроз выполняется с применением ML-моделей. Для достижения цели необходимо определить состав результатов ML и XAI анализа, доступных при наблюдении за отдельным объектом, установить способ количественного представления свойств локального объяснения, формализовать их использование совместно с решением классификатора при формировании диагностического состояния, определить связь состояния с сигналом и объяснимым отчетом, а также экспериментально оценить поведение модели при поступлении активности, отсутствовавшей в обучающих данных.

Научная новизна состоит в разработке модели интерпретационного наблюдения, в которой количественные свойства локального объяснения используются как диагностические признаки отдельного объекта. В отличие от постфактум-интерпретации предлагаемая модель учитывает не только содержание объяснения, но и степень подтверждения им прогноза. В отличие от решений, передающих атрибуции дополнительному классификатору, исходная ML-модель не заменяется и не переобучается. В отличие от мониторинга сдвига объяснений диагностический результат формируется для каждого объекта, а недостаточное интерпретационное подтверждение представляется самостоятельным состоянием, требующим аналитической проверки.

### **Интерпретационная модель наблюдения и диагностирования состояния элемента блокчейн-системы**

Предлагаемая модель строится вокруг среды национального блокчейна. Под такой средой понимается не только распределенный реестр, но и связанные с ним сетевые узлы, валидаторы, сервисы доступа, средства обработки транзакций, механизмы исполнения смарт-контрактов, прикладные модули и интерфейсы взаимодействия с внешними системами<sup>3</sup>. Обозначим совокупность наблюдаемых элементов как  $B = \{B_1, \dots, B_n\}$ . Данные об их работе поступают последовательно, поэтому введем множество моментов времени  $\mathcal{T} = \{t_1, \dots, t_\delta\}$ . Для каждого элемента  $B_i$  в момент  $t \in \mathcal{T}$  формируется вектор входных данных  $X_{(B_i)}(t) = (x_1, x_2, \dots, x_k) \in \mathbb{R}^k$ . В зависимости от назначения элемента этот вектор может описывать сетевое поведение, параметры транзакции, обращение

<sup>3</sup> Recommendation ITU-T X.1413 (05/2025). Security controls for distributed ledger technology. URL: <https://www.itu.int/rec/T-REC-X.1413/en> (дата обращения: 08.08.2026)

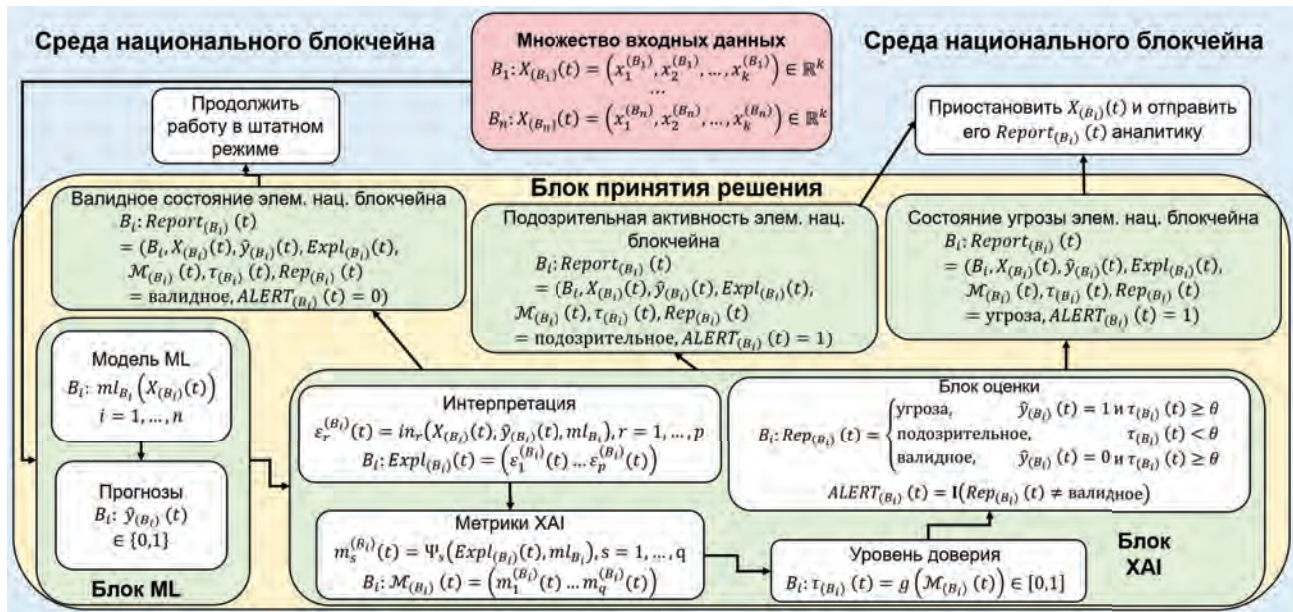


**Рис. 1. Интерпретационная модель наблюдения и диагностирования состояния элемента блокчейн-системы**

к программному интерфейсу, событие интеграционного сервиса, выполнение смарт-контракта или другую наблюдаемую активность.

Такая постановка имеет два следствия. Во-первых, модель сохраняет применимость на разных уровнях блокчейн-платформы. Во-вторых, наблюдение не сводится только к анализу финансовых транзакций. Оно может быть организовано для любого элемента, состояние которого влияет на безопасность, доверие, непрерывность работы или корректность предоставляемых сервисов. При этом состав входных признаков и применяемые средства машинного обучения могут различаться: сетевой узел, механизм обработки транзакций и прикладной сервис решают разные задачи и оставляют разные наблюдаемые следы. На рис. 1 представлена общая схема интерпретационной модели наблюдения и диагностирования состояния элемента блокчейн-системы.

Как видно из рис. 1, обработка начинается с получения прогноза ML-модели. Интерпретационный контур не заменяет этот прогноз и не создает вместо исходной модели новый классификатор. Его задача состоит в том, чтобы дополнить полученный ответ сведениями о том, какие признаки определили решение и насколько свойства сформированного объяснения соответствуют условиям его дальнейшего использования.

Пусть  $ML = \{ml_1, \dots, ml_n\}$  — множество обученных бинарных моделей машинного обучения, применяемых для наблюдаемых элементов. Каждому элементу  $B_i$  сопоставляется модель  $ml_{B_i}$ , которая получает вектор  $X_{(B_i)}(t)$  и формирует прогноз:

$$\hat{y}_{(B_i)}(t) = ml_{B_i}(X_{(B_i)}(t)) \in \{0, 1\}, \quad (1)$$

где значение 0 соответствует прогнозу нормы, значение 1 — прогнозу угрозы. Здесь важно различать прогноз и фактическое состояние объекта. Бинарная модель должна выбрать один из предусмотренных

классов даже тогда, когда поступившие данные отличаются от наблюдавшихся при ее обучении. Поэтому значение  $\hat{y}_{(B_i)}(t)$  показывает решение классификатора, но само по себе не позволяет установить, насколько уверенно это решение подтверждается особенностями конкретного объекта.

Дополнительные сведения о сформированном прогнозе получают с помощью локальной интерпретации. Для рассматриваемого элемента задается конфигурация  $In = \{in_1, \dots, in_p\}$ , совместимая с его ML-моделью и представлением входных данных. При  $p = 1$  она включает один XAI-метод, а при  $p > 1$  может объединять несколько совместимых методов, описывающих один и тот же прогноз. Конкретный состав конфигурации и способ совместного представления ее результатов зависят от реализации интерпретационного контура. Каждый метод  $in_r$  применяется к объекту  $X_{(B_i)}(t)$ , прогнозу  $\hat{y}_{(B_i)}(t)$  и соответствующей модели  $ml_{B_i}$ :

$$\varepsilon_r^{(B_i)}(t) = in_r(X_{(B_i)}(t), \hat{y}_{(B_i)}(t), ml_{B_i}), \quad r = 1, \dots, p. \quad (2)$$

Результат  $\varepsilon_r^{(B_i)}(t)$  представляет локальное объяснение прогноза и характеризует направление и относительную силу влияния входных признаков на решение ML-модели. Результаты выбранной XAI-конфигурации образуют набор  $Expl_{(B_i)}(t) = (\varepsilon_1^{(B_i)}(t), \dots, \varepsilon_p^{(B_i)}(t))$ .

Таким образом, для каждого наблюдаемого элемента используется подходящее ему средство локальной интерпретации либо выбранная совместимая комбинация.

На следующем этапе осуществляется переход от результата локальной интерпретации к измеряемым показателям качества объяснения. Атрибуции показывают, какие признаки и в каком направлении повлияли



на прогноз, однако сами по себе не позволяют количественно охарактеризовать свойства полученного объяснения. Поэтому в модель вводится множество метрик  $\Psi = \{\Psi_1, \dots, \Psi_q\}$ . Каждая метрика  $\Psi_s$  оценивает отдельное свойство объяснения с учетом поведения соответствующей ML-модели и возвращает значение  $m_s^{(B_i)}(t)$ :

$$m_s^{(B_i)}(t) = \Psi_s(Expl_{(B_i)}(t), ml_{B_i}), s = 1, \dots, q. \quad (3)$$

В зависимости от рассматриваемого элемента и выбранной ХАИ-конфигурации вектор может включать метрики верности, устойчивости, согласованности и другие характеристики локального объяснения, для которых определены воспроизводимые процедуры расчета. При этом метрики не заменяют атрибуты и не формируют новый класс объекта. Они переводят свойства объяснения в измеряемую форму, необходимую для их последующего совместного учета.

Полученные значения метрик образуют вектор показателей качества объяснения

$$\mathcal{M}_{(B_i)}(t) = (m_1^{(B_i)}(t), \dots, m_q^{(B_i)}(t)), \text{ который пред-}$$

ставляет количественное описание свойств объяснения, сформированного для текущего прогноза. Каждая его компонента сохраняет смысл соответствующей метрики, а весь вектор используется как единое диагностическое описание свойств объяснения при дальнейшем формировании уровня доверия.

Для совместного учета рассчитанных показателей вводится правило  $g$ , преобразующее вектор  $\mathcal{M}_{(B_i)}(t)$  в скалярный уровень доверия:

$$\tau_{(B_i)}(t) = g(\mathcal{M}_{(B_i)}(t)) \in [0,1]. \quad (4)$$

Правило  $g$  устанавливает связь между совокупностью измеренных свойств объяснения и итоговой оценкой. Модель не ограничивает его одной заранее заданной математической операцией, поскольку характер связи зависит от наблюдаемого элемента, ML-модели и используемой ХАИ-конфигурации. При этом  $\tau_{(B_i)}(t)$  не является вероятностью угрозы и не заменяет прогноз  $\hat{y}_{(B_i)}(t)$ . Эти значения описывают разные стороны рассматриваемого объекта: прогноз указывает выбранный ML-моделью класс, а уровень доверия характеризует свойства объяснения этого прогноза.

Для перехода от прогноза и уровня доверия к диагностическому состоянию вводится порог  $\theta \in [0,1]$ . Состояние наблюдаемого элемента определяется выражением:

$$Rep_{(B_i)}(t) = \begin{cases} \text{угроза, } \hat{y}_{(B_i)}(t) = 1 \text{ и } \tau_{(B_i)}(t) \geq \theta, \\ \text{подозрительное, } \tau_{(B_i)}(t) < \theta, \\ \text{валидное, } \hat{y}_{(B_i)}(t) = 0 \text{ и } \tau_{(B_i)}(t) \geq \theta. \end{cases} \quad (5)$$

Значение  $Rep_{(B_i)}(t)$  является диагностическим заключением интерпретационного контура и не рассматривается как достоверно известная фактическая метка объекта.

Состояние «угроза» формируется при совпадении двух условий: ML-модель обнаружила признаки угрозы, а свойства объяснения соответствуют установленному уровню доверия. Такое заключение сохраняет исходный прогноз модели и одновременно дополняет его результатами интерпретационного контроля.

«Подозрительное состояние» возникает при недостаточном уровне доверия независимо от значения бинарного прогноза. В данном случае прогноз не отменяется и не заменяется противоположным, однако его автоматическое применение ограничивается. Тем самым состояние отражает недостаточность основания для однозначного отнесения объекта к валидному состоянию или угрозе.

«Валидное состояние» соответствует прогнозу нормы, объяснение которого удовлетворяет установленному условию. Такой объект может продолжить обработку в штатном режиме, поскольку интерпретационный контур не выявил оснований для дополнительной проверки.

Для передачи результата во внешний контур вводится бинарный сигнал:

$$ALERT_{(B_i)}(t) = I(Rep_{(B_i)}(t) \neq \text{валидное}), \quad (6)$$

где  $I(\cdot)$  обозначает индикатор выполнения условия. Значение  $ALERT = 1$  означает необходимость передачи результата во внешний контур, а основание формирования сигнала сохраняется в  $Rep$ .

Итогом обработки объекта является отчет:

$$Report_{(B_i)}(t) = (B_i, X_{(B_i)}(t), \hat{y}_{(B_i)}(t), Expl_{(B_i)}(t), \mathcal{M}_{(B_i)}(t), \tau_{(B_i)}(t), Rep_{(B_i)}(t), ALERT_{(B_i)}(t)) \quad (7)$$

Отчет последовательно объединяет исходные сведения об объекте, прогноз ML-модели, результаты локальной интерпретации, значения метрик, уровень доверия и сформированное диагностическое состояние. Такое представление позволяет не только передать сигнал о необходимости реагирования, но и сохранить сведения, объясняющие причину принятого решения.

Поскольку модель предназначена для применения в действующей системе защиты, интерпретация и оценка ее результатов должны выполняться в пределах установленных ограничений:

$$T_{Expl_{(B_i)}} + T_{\tau_{(B_i)}} \leq T_{max}, \quad (8)$$

$$R(Expl_{(B_i)}) + R(\tau_{(B_i)}) \leq R_{max}. \quad (9)$$

Здесь  $T_{Expl_{(B_i)}}$  обозначает время получения локального объяснения, а  $T_{\tau_{(B_i)}}$  — время расчета метрик и уровня доверия. Аналогично  $R(\cdot)$  характеризует используемые вычислительные ресурсы.

Таким образом, модель формализует включение результатов локальной интерпретации в наблюдение за решением ML-модели и диагностирование состояния поступившего объекта. Свойства объяснения



представляются вектором  $\mathcal{M}$ , из которого правило  $g$  формирует уровень доверия  $\tau$ . Совместный учет решения  $\hat{y}$  и уровня доверия определяет состояние  $Rep$ , на основе которого формируются сигнал  $ALERT$  и отчет  $Report$ . Такая последовательность позволяет использовать локальное объяснение не только для последующего ознакомления аналитика, но и как источник сведений при формировании диагностического результата. Конкретные способы вычисления метрик, построения правила  $g$  и настройки порога  $\theta$  моделью не фиксируются.

### Экспериментальное исследование интерпретационной модели

Экспериментальное исследование проведено на наборе сетевого трафика CICIDS2017 [19]<sup>4</sup>. Для воспроизведения поступления данных, отсутствовавших при обучении ML-модели, записи с выбранным видом вредоносной активности полностью исключались из обучающей части и сохранялись в тестовой. Исследование включало три сценария: DDoS, PortScan и совместное появление DoS GoldenEye, FTP-Patator и SSH-Patator. Остальные данные разделялись на обучающую, эталонную и тестовую части. Обучающая часть использовалась для построения бинарной ML-модели, эталонная — для расчета распределений показателей объяснения и выбора порога, тестовая — для итогового сравнения исходного решения модели с результатом интерпретационного контроля. Во всех сценариях сохранялись одинаковые предобработка и структура классификатора.

Для каждого объекта вычислялись прогноз ML-модели и локальные атрибуции признаков методами Integrated Gradients, Feature Ablation, DeepLift, GradientSHAP и LIME. Рассматривались одиночные методы, их попарные сочетания и общая конфигурация из пяти объяснителей. В конфигурациях, объединяющих несколько объяснителей, абсолютные атрибуции каждого метода отдельно приводились к диапазону от 0 до 1 относительно 95-го перцентиля значений текущего объекта, после чего соответствующие оценки признаков усреднялись. Такое преобразование обеспечивало сопоставимость результатов методов, исходные масштабы атрибуций которых различаются.

Диагностический профиль объяснения формировался из показателей верности и устойчивости. Показатель верности характеризует, насколько изменение наиболее значимых по объяснению признаков воздействует на выход модели сильнее, чем изменение случайно выбранных признаков того же количества:

$$\Delta_{\text{знач}}(X_{(B_i)}(t)) = \left| z(X_{(B_i)}(t)) - z(\tilde{X}_{\text{знач}}^{(B_i)}(t)) \right|, \quad (10)$$

$$\Delta_{\text{контр}}(X_{(B_i)}(t)) = \frac{1}{5} \sum_{q=1}^5 \left| z(X_{(B_i)}(t)) - z(\tilde{X}_{\text{контр}, q}^{(B_i)}(t)) \right|, \quad (11)$$

$$m_{\text{верн}}(X_{(B_i)}(t)) = \frac{\Delta_{\text{знач}}(X_{(B_i)}(t))}{\Delta_{\text{знач}}(X_{(B_i)}(t)) + \Delta_{\text{контр}}(X_{(B_i)}(t)) + \varepsilon}, \quad (12)$$

где  $z(X_{(B_i)}(t))$  обозначает выход базовой модели, а  $\tilde{X}_{\text{знач}}^{(B_i)}$  и  $\tilde{X}_{\text{контр}, q}^{(B_i)}$  представляют измененные варианты

анализируемого объекта. Для формирования  $\tilde{X}_{\text{знач}}^{(B_i)}$  выбирались 30% признаков с наибольшими абсолютными атрибуциями, но не менее пяти признаков. Их исходные значения заменялись медианами соответствующих признаков эталонной выборки. Контрольное воздействие рассчитывалось аналогичным образом для пяти случайных наборов той же мощности. Вызванные ими изменения выхода модели усреднялись и сопоставлялись с результатом замены значимых признаков. Поэтому показатель верности отражает, насколько признаки, выделенные объяснителем, влияют на решение модели сильнее случайного набора.

Показатель устойчивости характеризует сохранение состава значимых признаков в локальной окрестности анализируемого объекта. Для этого в эталонной выборке находился ближайший по евклидову расстоянию объект с тем же прогнозируемым классом, после чего множества значимых признаков сопоставлялись с помощью коэффициента Жаккара. Полученное сходство учитывалось при различии прогнозируемых вероятностей не более 0,15. В противном случае показатель устойчивости принимал нулевое значение. Тем самым сравнивались объекты, близкие не только в пространстве входных признаков, но и по выходу ML-модели.

$$m_{\text{уст}}(X_{(B_i)}(t)) = \frac{\left| \mathbb{T}_{(B_i)}(t) \cap \mathbb{T}_{\text{ближ}}^{(B_i)}(t) \right|}{\left| \mathbb{T}_{(B_i)}(t) \cup \mathbb{T}_{\text{ближ}}^{(B_i)}(t) \right|} \cdot \mathbf{I} \left( \left| z(X_{(B_i)}(t)) - z(X_{\text{ближ}}^{(B_i)}(t)) \right| \leq 0.15 \right), \quad (13)$$

где  $\mathbb{T}_{(B_i)}(t)$  — маска значимых признаков анализируемого объекта, а  $\mathbb{T}_{\text{ближ}}^{(B_i)}(t)$  — маска ближайшего сопоставимого объекта из эталонной выборки известных состояний.  $\mathbf{I}(\cdot)$  принимает значение 1 при выполнении указанного условия и 0 в противном случае.

Полученные значения образуют вектор показателей качества объяснения  $\mathcal{M}_{(B_i)}(t) = (m_{\text{верн}}^{(B_i)}(t), m_{\text{уст}}^{(B_i)}(t))$ . В эксперимен-

тальной реализации уровень доверия  $\tau_{(B_i)}$  определялся как среднее арифметическое значений метрик верности и устойчивости:

<sup>4</sup> Canadian Institute for Cybersecurity. Intrusion Detection Evaluation Dataset (CIC-IDS2017). URL: <https://www.unb.ca/cic/datasets/ids-2017.html> (дата обращения: 08.08.2026).

Таблица 1

## Показатели бинарного распознавания

| Целевой сценарий                                                     | Accuracy    | Balanced accuracy | Precision   | Recall      | F1          |
|----------------------------------------------------------------------|-------------|-------------------|-------------|-------------|-------------|
| DDoS (базовая модель)                                                | 0,889       | 0,926             | 0,995       | 0,870       | 0,929       |
| DDoS (интерпретационный контур)                                      | 0,915—0,939 | 0,821—0,873       | 0,934—0,961 | 0,936—0,993 | 0,948—0,965 |
| PortScan (базовая модель)                                            | 0,700       | 0,817             | 0,997       | 0,641       | 0,781       |
| PortScan (интерпретационный контур)                                  | 0,695—0,769 | 0,693—0,757       | 0,916—0,950 | 0,683—0,788 | 0,789—0,850 |
| DoS GoldenEye + FTP-Patator + SSH-Patator (базовая модель)           | 0,790       | 0,871             | 0,998       | 0,7514      | 0,857       |
| DoS GoldenEye + FTP-Patator + SSH-Patator (интерпретационный контур) | 0,800—0,842 | 0,739—0,798       | 0,924—0,952 | 0,805—0,878 | 0,873—0,903 |

$$\tau_{(B_i)}(t) = g\left(\mathcal{M}_{(B_i)}(t)\right) = \frac{m_{\text{верн}}^{(B_i)}(t) + m_{\text{уст}}^{(B_i)}(t)}{2}. \quad (14)$$

Порог  $\theta$  определялся отдельно для каждой ХАИ-конфигурации по корректно классифицированным объектам эталонной выборки и соответствовал 10-му процентилю эмпирического распределения  $\tau$ . Значения ниже этой границы указывали на нетипичный для известных корректных решений профиль объяснения и приводили к формированию подозрительного состояния.

Для каждого целевого сценария исследовались пять одиночных ХАИ-методов, десять их попарных сочетаний и общий ансамбль из пяти объяснителей. Поскольку введение подозрительного состояния изменяет итоговый сигнал, полученные варианты сначала сопоставлялись с базовой ML-моделью по общим показателям бинарного распознавания. Диапазоны значений по ХАИ-конфигурациям приведены в табл. 1.

Результаты показывают, что интерпретационный контур меняет не только число правильных решений, но и соотношение разных видов ошибок. Объекты атак, пропущенные базовой моделью, частично переходят в подозрительное состояние, вследствие чего повышаются Recall и F1. Одновременно в дополнительную проверку попадает часть объектов нормы, что отражается на Precision и Balanced accuracy. Такое изменение нельзя однозначно характеризовать как улучшение или ухудшение классификации. Оно соответствует переходу от полностью автоматического бинарного решения к диагностированию случаев, в которых прогноз недостаточно подтверждается свойствами локального объяснения.

Стандартные показатели не позволяют установить, связано ли формирование подозрительного состояния с содержательными различиями объяснений. Поэтому отдельно исследовалась способность метрик верности и устойчивости, а также их совместной оценки различать правильные и ошибочные решения ML-модели. Чтобы исключить случайный характер обнаруженных различий, значения показателей сравнивались с по-

мощью критерия Манна — Уитни. При проверке нескольких ХАИ-конфигураций применялась поправка Бенджамини — Хохберга, уменьшающая вероятность ложного вывода о наличии различий. Диагностическая информативность показателей представлена в табл. 2.

Таблица 2

## Диагностическая информативность показателей объяснения

| Целевой сценарий                          | AUC верности | AUC устойчивости | AUC итоговой оценки $\tau$ |
|-------------------------------------------|--------------|------------------|----------------------------|
| DDoS                                      | 0,715—0,901  | 0,479—0,896      | 0,769—0,932                |
| PortScan                                  | 0,485—0,558  | 0,545—0,765      | 0,543—0,710                |
| DoS GoldenEye + FTP-Patator + SSH-Patator | 0,466—0,542  | 0,567—0,903      | 0,532—0,800                |

Полученные результаты подтверждают, что метрики верности и устойчивости характеризуют разные стороны локального объяснения. Метрика верности оказалась наиболее информативной в сценарии DDoS, но слабее разделяла правильные и ошибочные решения в двух других сценариях. Метрика устойчивости, напротив, сохраняла диагностическую ценность для части конфигураций PortScan и совместного сценария. Следовательно, ни одну из этих метрик нельзя считать универсальной. Их совместная оценка позволяет учитывать как влияние значимых признаков на прогноз, так и сохранение состава этих признаков в локальной окрестности объекта.

Для всех проверенных ХАИ-конфигураций различия итоговой оценки между правильными и ошибочными решениями сохранили статистическую значимость после поправки на множественные сравнения. Вместе с тем заметный разброс AUC показывает, что практическая сила такого разделения зависит от входных данных и объяснителя. Тем самым гипотеза об информативности измеримых свойств объяснения получила

Таблица 3

**Охват целевой активности сигналом и дополнительная аналитическая проверка**

| Целевой сценарий                                                     | Охват целевой активности | Дополнительная доля на проверке | Доля нормы на проверке |
|----------------------------------------------------------------------|--------------------------|---------------------------------|------------------------|
| DDoS (базовая модель)                                                | 0,630                    | 0,000                           | 0,000                  |
| DDoS (интерпретационный контур)                                      | 0,822—0,994              | 0,083—0,157                     | 0,174—0,334            |
| PortScan (базовая модель)                                            | 0,0014                   | 0,000                           | 0,000                  |
| PortScan (интерпретационный контур)                                  | 0,110—0,434              | 0,069—0,176                     | 0,178—0,324            |
| DoS GoldenEye + FTP-Patator + SSH-Patator (базовая модель)           | 0,289                    | 0,000                           | 0,000                  |
| DoS GoldenEye + FTP-Patator + SSH-Patator (интерпретационный контур) | 0,452—0,683              | 0,077—0,163                     | 0,204—0,360            |

подтверждение, однако результаты не дают оснований рассматривать отдельную метрику или XAI-метод как одинаково эффективные во всех условиях.

Установленная различимость профилей объяснения показывает, что они содержат сведения, дополняющие выходной класс ML-модели. Практический эффект этой информации оценивался путем сопоставления исходного режима и режима с интерпретационным контуром. Пусть  $\Omega_{\text{цел}}$  обозначает множество объектов целевой вредоносной активности, сохраненной в тестовой выборке, но отсутствовавшей при обучении. В исходном режиме доля объектов этого множества, вызвавших сигнал, определяется выражением:

$$\rho_{ML} = \frac{1}{|\Omega_{\text{цел}}|} \sum_{j \in \Omega_{\text{цел}}} I(\hat{y}_j = 1). \quad (15)$$

После включения интерпретационного контура сигнал формируется как для состояния «угроза», так и для состояния «подозрительное». Поэтому охват целевой активности принимает вид:

$$\begin{aligned} \rho_{ML+XAI} &= \frac{1}{|\Omega_{\text{цел}}|} \sum_{j \in \Omega_{\text{цел}}} I(Rep_j \in \\ &\in \{\text{угроза, подозрительное}\}) = \\ &= \frac{1}{|\Omega_{\text{цел}}|} \sum_{j \in \Omega_{\text{цел}}} ALERT_j. \end{aligned} \quad (16)$$

Различие между  $\rho_{ML}$  и  $\rho_{ML+XAI}$  характеризует не число подтвержденных атак, а изменение доли целевой активности, сохранившейся в области наблюдения. Расширение этой области сопровождается дополнительной проверкой объектов, которым базовая модель присвоила прогноз нормы:

$$\begin{aligned} \rho_{\text{доп}} &= \frac{1}{N_{\text{test}}} \sum_{j=1}^{N_{\text{test}}} I(\hat{y}_j = \\ &= 0 \wedge Rep_j = \text{подозрительное}). \end{aligned} \quad (17)$$

Влияние такой проверки на штатные данные определяется отдельно:

$$\rho_{\text{норм}} = \frac{\sum_{j=1}^{N_{\text{test}}} I(y_j = 0 \wedge Rep_j = \text{подозрительное})}{\sum_{j=1}^{N_{\text{test}}} I(y_j = 0)}. \quad (18)$$

Здесь  $N_{\text{test}}$  обозначает объем тестовой выборки,  $\hat{y}$  — прогноз базовой ML-модели, а  $y_j$  фактическая метка. Полученные значения приведены в табл. 3.

Сопоставление двух режимов показало, что интерпретационный контур изменяет наблюдаемость целевой активности. Часть объектов, не вызвавших сигнал базовой модели, после оценки свойств объяснения получила подозрительное состояние и была сохранена для дальнейшего анализа. Этот эффект наблюдался во всех сценариях, хотя его выраженность зависела от XAI-конфигурации. Вместе с целевой активностью на дополнительную проверку направлялась и часть штатных объектов. Таким образом, промежуточное состояние расширяет область наблюдения, но не подтверждает наличие атаки. Выявленное соотношение между охватом целевой активности и объемом проверки необходимо учитывать при разработке метода формирования диагностического профиля и настройки порогов.

Отдельно проверялось предположение о том, что совместное использование XAI-методов способно повысить диагностическую информативность по сравнению с отдельным объяснителем. Для этого сопоставлялись одиночные методы, попарные конфигурации и общий ансамбль, объединяющий все пять объяснителей. Результаты представлены в табл. 4.

Попарное объединение атрибуций не обеспечило одинакового преимущества во всех сценариях. Для DDoS и PortScan лучшие попарные конфигурации несколько превосходили отдельные XAI-методы, тогда как в совместном сценарии наиболее информативным оказался Feature Ablation. Ансамбль из пяти объяснителей также не показал устойчивого преимущества. Полученный результат означает, что диагностическая информативность совместной конфигурации определяется взаимным дополнением объяснений, а не числом объединяемых методов. Поэтому частная гипотеза о преимуществе совместного использования XAI-методов получила частичное подтверждение.

Результативность совместного использования XAI-методов

| Целевой сценарий                          | AUC одиночного XAI | AUC парной конфигурации | AUC ансамбля из пяти XAI |
|-------------------------------------------|--------------------|-------------------------|--------------------------|
| DDoS                                      | 0,769—0,923        | 0,833—0,932             | 0,900                    |
| PortScan                                  | 0,586—0,708        | 0,543—0,710             | 0,568                    |
| DoS GoldenEye + FTP-Patator + SSH-Patator | 0,580—0,800        | 0,532—0,794             | 0,594                    |

Проведенное исследование подтвердило, что локальное объяснение обладает измеримыми свойствами, которые не представлены в выходном классе ML-модели. Включение показателей верности и устойчивости в диагностическое описание позволило сохранить для дополнительной проверки часть целевой активности, не вызвавшей сигнал базовой модели. При этом подозрительное состояние не использовалось как фактическая метка угрозы. Результаты также показали, что информативность совместного использования XAI-методов определяется взаимным дополнением объяснений и не возрастает автоматически при увеличении числа объяснителей.

### Заключение

В работе разработана интерпретационная модель наблюдения и диагностирования состояния элементов блокчейн-систем на основе применения моделей машинного обучения в условиях появления угроз нового типа. Основное отличие модели состоит во включении результата локальной интерпретации в формирование диагностического состояния отдельного объекта. Свойства объяснения получают количественное представление, после чего используются совместно с решением классификатора. Исходная ML-модель при этом не изменяется, а решения с нетипичным диагностическим профилем сохраняются для дополнительной проверки.

Экспериментальная проверка показала, что метрики верности и устойчивости отражают разные свойства локального объяснения. Их совместное рассмотрение позволяет различать характерные и нетипичные сочетания прогноза и объяснения. При поступлении вредоносной активности, признаки которой не были представлены в обучающих данных, часть объектов, отнесенных базовой моделью к норме, переводилась в подозрительное состояние. Вместе с ними на проверку направлялась часть объектов нормы. Поэтому результат интерпретационного контроля не заменяет заклю-

чение аналитика, а выделяет решения, для которых имеющихся оснований недостаточно для продолжения полностью автоматической обработки.

Проведенное исследование позволило установить три основных результата. Во-первых, измеримые свойства локального объяснения образуют дополнительное диагностическое описание решения ML-модели, которое не сводится к предсказанному классу. Во-вторых, промежуточное диагностическое состояние позволяет сохранить наблюдаемость объектов при несоответствии прогноза характеру его объяснения, не вводя новый класс атаки и не изменяя базовую модель. В-третьих, информативность совместного использования XAI-методов определяется взаимным дополнением объяснений, а не числом объединяемых методов. Парные конфигурации и ансамбль из пяти объяснителей в отдельных случаях превосходили одиночные методы, но не обеспечили устойчивого преимущества во всех сценариях.

Научный результат работы состоит в формализации связи между решением ML-модели и результатом его локальной интерпретации в задаче наблюдения и диагностирования состояния элемента блокчейн-системы. Предложенная модель определяет переход от объяснения к его измеримому описанию, а затем к диагностическому состоянию, сигналу и объяснимому отчету. Благодаря этому сведения XAI участвуют в формировании результата наблюдения, не подменяя прогноз классификатора и заключение аналитика.

В дальнейшем предполагается разработать метод интерпретационного диагностирования состояния элементов блокчейн-систем. Метод должен представить установленные моделью отношения в виде последовательности действий по формированию диагностического профиля, настройке порогов и определению состояния наблюдаемого элемента. При его экспериментальном исследовании необходимо оценить влияние выбранных правил на охват угроз нового типа и объем дополнительной проверки.

*Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение от 27.09.2024 г. № 23-03).*



## Литература

1. Ларина М.В., Скиба В.Ю. Модель цифровой платформы для анализа устойчивости к квантовым угрозам // Правовая информатика. 2025. № 3. С. 12—26.
2. Skiba V.Yu. et al. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunication and Control. 2025. T. 18, № 2. С. 56—73.
3. Петренко С.А., Балябин А.А. Модель квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 1 (65). С. 7—17.
4. Kayikci S., Khoshgoftaar T.M. Blockchain meets machine learning: a survey // Journal of Big Data. 2024. T. 11, № 1. Article 9.
5. Hasan M. et al. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis // Blockchain: Research and Applications. 2024. T. 5, № 3. Article 100207.
6. Петренко С.А., Сундеев П.В. Контроль требований к защите информации на основе модели логического вывода и графовой нейронной сети // Правовая информатика. 2026. № 2. С. 85—94.
7. Бирюков Д.Н., Дудкин А.С. Объяснимость и интерпретируемость — важные аспекты безопасности решений, принимаемых интеллектуальными системами (обзорная статья) // Научно-технический вестник информационных технологий, механики и оптики. 2025. T. 25, № 3. С. 373—386.
8. Gnidko K., Lisov D. Public Dataset and Explainable AI for Cognitive Cybersecurity: Grad-CAM Insights into Negative Visual Stimuli Detection // 2025 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT). 2025. С. 17—20.
9. Hosain Y., Çakmak M. XAI-XGBoost: an innovative explainable intrusion detection approach for securing internet of medical things systems // Scientific reports. Nature Publishing Group UK London, 2025. T. 15, № 1. Article 22278.
10. Krishnan D., Singh S., Sugumaran V. Explainable AI for zero-day attack detection in IoT networks using attention fusion model // Discover Internet of Things. 2025. T. 5, № 1. Article 83.
11. Kaya K. et al. X-cba: Explainability aided catboosted anomal-e for intrusion detection system // ICC 2024-IEEE International Conference on Communications. IEEE, 2024. С. 2288—2293.
12. Senevirathna T. et al. From Insight to Action: XAI-Enhanced Detection of DDoS Attacks in Software Defined Networks // 2025 IEEE 36th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2025. С. 1—6.
13. Villegas-Ch W. et al. Autonomous federated defense for zero-day threats in IIoT: explainable agents with real-time edge inference // Frontiers in Communications and Networks. 2026. T. 6. Article 1697204.
14. Mougan C. et al. Explanation Shift: How Did the Distribution Shift Impact the Model? // Transactions on Machine Learning Research. 2025.
15. Decker T. et al. Explanatory Model Monitoring to Understand the Effects of Feature Shifts on Performance // Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, KDD 2024, Barcelona, Spain, August 25—29, 2024 / под ред. Baeza-Yates R., Bonchi F. ACM, 2024. С. 550—561.
16. Nauta M. et al. From Anecdotal Evidence to Quantitative Evaluation Methods: A Systematic Review on Evaluating Explainable AI // ACM Comput. Surv. 2023. T. 55, № 13s. С. 1—42.
17. Hedström A. et al. Quantus: An Explainable AI Toolkit for Responsible Evaluation of Neural Network Explanations and Beyond // Journal of Machine Learning Research. 2023. T. 24, № 34. С. 1—11.
18. Weber R.O. et al. XAI is in trouble // AI Magazine. 2024. T. 45, № 3. С. 300—316.
19. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISp. 2018. T. 1, № 2018. С. 108—116.

# AN INTERPRETATIVE MODEL FOR MONITORING AND DIAGNOSING THE STATUS OF BLOCKCHAIN SYSTEM COMPONENTS USING MACHINE LEARNING MODELS

Lisov D.N.<sup>5</sup>

**Keywords:** explainable artificial intelligence, local feature attributions, binary threat classification, explanation quality, diagnostic profile, prediction confidence, suspicious activity, analytical verification, new security threats, network intrusions.

## Abstract

**Purpose of work:** to develop an interpretative model for monitoring and diagnosing the status of blockchain system components when new types of threats emerge, by jointly analysing the predictions of machine learning models and the results of their local interpretation.

**Research method:** functional decomposition was performed for the monitoring process, which includes obtaining a prediction, constructing a local explanation, quantitatively assessing its properties, and forming a diagnostic conclusion. Two quality metrics, faithfulness and robustness, were used to quantitatively assess the local explanation. The faithfulness metric shows how much replacing the features identified by the explainer changes the model output compared with replacing a random set of features, while the robustness metric characterizes the preservation of the set of important features in nearby objects with comparable predictions. Metric values were determined by the controlled replacement of input features and comparison of local explanations, and their diagnostic informativeness was assessed using receiver operating characteristic curves. To reproduce a new type of threat experimentally, one attack type was excluded from the training data and retained in the test set, after which individual explanation methods and their combinations were evaluated.

**Results of the study:** an interpretative model is proposed in which the result of a local explanation is incorporated into the observation of the ML model's decision and the determination of the object's diagnostic status. The measurable properties of the explanation are transformed into a vector of indicators, which is used to determine the confidence level. If the diagnostic profile of the explanation does not correspond to the characteristic profiles of known correct decisions, the object is assigned an intermediate 'suspicious' status and retained for further verification. An experimental study has shown that the explanation quality metrics contain diagnostic information not present in the model's output class; however, the extent of this information depends on the data and the explainer used. When an activity not present in the training data was encountered, the interpretation loop made it possible to retain within the observation domain some of the objects that had been missed by the base model. The combined use of several explanation methods proved useful only when the resulting attributions complemented one another and did not provide a universal advantage. The results obtained confirm that it is possible to identify decisions requiring further verification when previously unobserved threats arise. The base classifier remains unchanged, and a suspicious state is not equated with an attack.

## References

1. Larina M.V., Skiba V.Iu. Model' tsifrovoy platformy dlia analiza ustoychivosti k kvantovym ugrozam // Pravovaya informatika. 2025. No. 3. S. 12—26.
2. Skiba V.Yu. et al. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunication and Control. 2025. T. 18. No. 2. S. 56—73.
3. Petrenko S.A., Baliabin A.A. Model' kvantovykh ugroz bezopasnosti informatsii dlia natsional'nykh blokchein-ekosistem i platform // Voprosy kiberbezopasnosti. 2025. No. 1 (65). S. 7—17.
4. Kayikci S., Khoshgoftaar T.M. Blockchain meets machine learning: a survey // Journal of Big Data. 2024. T. 11. No. 1. Article 9.

<sup>5</sup> **Dmitry N. Lisov**, Ph.D. student, Junior Researcher at the Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sirius, Krasnodar region, Russian Federation. ORCID: 0000-0002-8214-4109.  
E-mail: [lisov.dn@talantiuspeh.ru](mailto:lisov.dn@talantiuspeh.ru)

5. Hasan M. et al. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis // Blockchain: Research and Applications. 2024. T. 5. No. 3. Article 100207.
6. Petrenko S.A., Sundeev P.V. Kontrol' trebovaniy k zashchite informatsii na osnove modeli logicheskogo vyvoda i grafovoi neironnoi seti // Pravovaia informatika. 2026. No. 2. S. 85—94.
7. Biriukov D.N., Dudkin A.S. Ob"iasnimost' i interpretiruemost' — vazhnye aspekty bezopasnosti reshenii, prinimaemykh intellektual'nymi sistemami (obzornaia stat'ia) // Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki. 2025. T. 25. No. 3. S. 373—386.
8. Gnidko K., Lisov D. Public Dataset and Explainable AI for Cognitive Cybersecurity: Grad-CAM Insights into Negative Visual Stimuli Detection // 2025 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT). 2025. S. 17—20.
9. Hosain Y., Çakmak M. XAI-XGBoost: an innovative explainable intrusion detection approach for securing internet of medical things systems // Scientific reports. Nature Publishing Group UK London, 2025. T. 15. No. 1. Article 22278.
10. Krishnan D., Singh S., Sugumaran V. Explainable AI for zero-day attack detection in IoT networks using attention fusion model // Discover Internet of Things. 2025. T. 5. No. 1. Article 83.
11. Kaya K. et al. X-cba: Explainability aided catboosted anomal-e for intrusion detection system // ICC 2024-IEEE International Conference on Communications. IEEE, 2024. S. 2288—2293.
12. Senevirathna T. et al. From Insight to Action: XAI-Enhanced Detection of DDoS Attacks in Software Defined Networks // 2025 IEEE 36th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2025. S. 1—6.
13. Villegas-Ch W. et al. Autonomous federated defense for zero-day threats in IIoT: explainable agents with real-time edge inference // Frontiers in Communications and Networks. 2026. T. 6. Article 1697204.
14. Mougan C. et al. Explanation Shift: How Did the Distribution Shift Impact the Model? // Transactions on Machine Learning Research. 2025.
15. Decker T. et al. Explanatory Model Monitoring to Understand the Effects of Feature Shifts on Performance // Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, KDD 2024, Barcelona, Spain, August 25—29, 2024 / pod red. Baeza-Yates R., Bonchi F. ACM, 2024. S. 550—561.
16. Nauta M. et al. From Anecdotal Evidence to Quantitative Evaluation Methods: A Systematic Review on Evaluating Explainable AI // ACM Comput. Surv. 2023. T. 55. No. 13s. S. 1—42.
17. Hedström A. et al. Quantus: An Explainable AI Toolkit for Responsible Evaluation of Neural Network Explanations and Beyond // Journal of Machine Learning Research. 2023. T. 24. No. 34. S. 1—11.
18. Weber R.O. et al. XAI is in trouble // AI Magazine. 2024. T. 45. No. 3. S. 300—316.
19. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISp. 2018. T. 1. No. 2018. S. 108—116.



# К ЮБИЛЕЮ СОЗДАТЕЛЯ СВОДА ЗАКОНОВ СССР ТЕРЕБИЛОВА ВЛАДИМИРА ИВАНОВИЧА

Морозов А.В.<sup>1</sup>

**Ключевые слова:** история государства и права, систематизация нормативных правовых актов, правовая информатика, информационно-правовое обеспечение, Свод законов СССР, Министерство юстиции, Научный центр правовой информации, историко-правовое исследование, информационное право.

## Аннотация

Статья представляет собой историко-биографическое исследование, посвящённое Владимиру Ивановичу Теребилову — Министру юстиции СССР, председателю Верховного Суда СССР и одному из организаторов создания Свода законов СССР. На основе личных воспоминаний, свидетельств коллег и членов семьи раскрываются основные этапы профессиональной и общественной деятельности В.И. Теребилова, а также ключевые направления его работы на посту Министра юстиции СССР, включая развитие законодательства, адвокатуры, нотариата, правовой информатизации и международного правового сотрудничества.

Особое внимание уделяется созданию Научного центра правовой информации и систематизации советского законодательства. Сделан вывод о необходимости изучения и использования исторического опыта В.И. Теребилова при совершенствовании современной системы систематизации законодательства. Статья представляет интерес для исследователей истории государства и права, информационного права, правовой информатики, а также работников системы юстиции.

DOI: 10.24412/1994-1404-2026-3-100-103

В этом году исполнилось 110 лет со дня рождения создателя Свода законов СССР Министра юстиции СССР, затем Председателя Верховного суда СССР Теребилова Владимира Ивановича.

Мне, прослужившему в системе Минюста в разных должностях с 1988 по 2022 годы, неоднократно пришлось сталкиваться с воспоминаниями об этом незаурядном человеке, подобно Сперанскому Михаилу Михайловичу, создавшему Свод законов государства, возродившему в 1970 году Министерство юстиции, после его ликвидации, создавшему в 1975 году уникальное учреждение нашей страны — Научный центр правовой информации (далее — НЦПИ<sup>2</sup>), где я прослужил 7 лет директором с 1993 по 2000 годы [1].

Создание НЦПИ положило начало новой сферы деятельности — правовой информатике. Это, во-первых, активное внедрение средств информационно-вычислительной техники в юридическую деятельность<sup>3</sup>,

во-вторых, развитие правовых норм в информационной сфере, что привело к возникновению новой отрасли юриспруденции — информационного права<sup>4</sup>.

Последнее десятилетие XX века явилось периодом бурного развития баз данных правовой информации, в создании которых существенно преуспели известные коммерческие структуры, а также в построения государственной системы правовой информации<sup>5</sup>, где значительных результатов добились государственные органы и учреждения, одно из которых НЦПИ. НЦПИ, созданный в 1975 году Министром юстиции СССР Владимиром Ивановичем Теребиловым, в 80-е годы прошлого века, стал информационной и технологической базой для создания Свода законов СССР.

Мне посчастливилось 15 лет назад снять интернет-фильм по воспоминаниям коллег и детей Владимира Ивановича Теребилова о нем, и я считаю возможным поде-

<sup>2</sup> Морозов А.В. Уникальное учреждение. Труды НЦПИ. Страницы истории Научного центра правовой информации. К 35-летию НЦПИ. Выпуск 6 / Под ред. Н.С. Козленко. М.: ФГУ НЦПИ при Минюсте России, 2010. 56 с.

<sup>3</sup> Морозов А.В. Основные задачи программы информатизации судов и органов юстиции на 1996—1997 годы. Правовая

информатика: Сборник № 1. М.: Министерство юстиции Российской Федерации, НЦПИ, 1996.

<sup>4</sup> Морозов А.В. Информационное право как самостоятельная научная специальность. Юридическое образование и наука. 2013. № 1. М.: ИГ «ЮРИСТ», 2013. 40 с.

<sup>5</sup> Морозов А.В. Система правовой информации Минюста России: монография. М.: Триумф, 1999. 464 с.; ил. ISBN 5-89392-026-0.

<sup>1</sup> **Морозов Андрей Витальевич**, профессор кафедры компьютерного права и информационной безопасности Высшей школы государственного аудита МГУ имени М.В. Ломоносова, доктор юридических наук, профессор, кандидат технических наук, академик РАЕН, действительный государственный советник юстиции 2 класса, Москва, Российская Федерация.  
E-mail: [av\\_morozov@list.ru](mailto:av_morozov@list.ru)



литься некоторыми историческими сведениями о Владимире Ивановиче, которые, мне кажется, будут интересны молодым ученым юристам не только по специальности «Теоретико-исторические правовые науки», но по всем направлениям развития юриспруденции как науки.

Я сам неоднократно видел Владимира Ивановича уже в преклонном возрасте на ежегодных традиционных встречах Совета отечественных Министров юстиции в центральном аппарате Минюста, но последняя наша встреча было необычной.

Она состоялась в 2002 году в Кремле, во Дворце съездов, на торжественном мероприятии, посвященном 200-летию Министерства юстиции. Праздник был долгим и содержательным, и мы с коллегой спустились в гардероб очень поздно. И вдруг я увидел на выключенном эскалаторе с двумя палочками в руках Владимира Ивановича, который с неимоверно тяжелыми усилиями пытался подняться наверх. Мы с коллегой подхватили его и помогли подняться.

Это была наша последняя встреча. Впоследствии, в дни его юбилеев, я приходил на его могилу на Новодевичьем кладбище вместе со студентами ВГУЮ (РПА Минюста России), где я проработал заведующим кафедры 23 года.

Заслуги этого человека перед страной трудно переоценить. При В.И. Теребилове в должности Министра юстиции СССР и под его непосредственным руководством было воссоздано Министерство юстиции, разработан и принят ряд важных правовых актов, в частности, Закон СССР «Об адвокатуре», который проработал 30 лет, Положение о министерстве юстиции СССР, а также началась работа над изданием Собрания действующего законодательства СССР (50 томов) и Свода законов СССР (11 томов).

Каждое зрелое в законодательном смысле государство должно иметь свой Свод законов. Российская империя в XIX веке создала Свод законов под руководством Сперанского Михаила Михайловича, а в XX веке Свод законов СССР был создан под руководством Владимира Ивановича Теребилова.

Притом, что это чисто бумажный документ книжного формата, в него была заложена возможность его актуализации. Из темно-вишневых папок извлекались устаревшие тексты и вставлялись новые. И самое главное, что это был документ, носивший достоверную информацию, имеющую государственный статус.

С конца девяностых годов прошлого века<sup>6</sup> я неоднократно возвращался к теме создания Свода законов Российской Федерации в электронном (машиночитаемом) виде, и Министерство юстиции могло бы взять на себя эту важнейшую государственную задачу, в рам-

ках осуществления функции мониторинга правоприменения<sup>7</sup>.

Сегодня опыт создания Свода законов СССР должен быть детально изучен и использован при создании Свода законов Российской Федерации в электронной форме.

Владимир Иванович вел и очень значимую международную деятельность. В качестве одного из важных результатов — разработка проекта Конституции Индии. Известная Премьер-министр Индии Индира Ганди была очень благодарна за оказанную помощь и поддержку. Особенно тесные и доброжелательные отношения у Владимира Ивановича сложились с Финляндией, что было связано, в частности, с финским происхождением его супруги.

Но возвращаясь к воспоминаниям сослуживцев о Владимире Ивановиче Теребилове — многие из них рассказывали, что «это был авторитарный человек». С другой стороны, надо понимать, какое время и какие задачи его сформировали: Великая Отечественная война, блокада, задача возрождения Министерства юстиции. Надо найти достойные кадры, помещение, оборудование, наладить деятельность во всех республиках Советского Союза и, как сейчас говорят, в субъектах РСФСР (территориальных органах и учреждениях юстиции) по всем направлениям деятельности Министерства юстиции — от военных трибуналов (специальных судов) и систематизации законодательства до адвокатуры и нотариата.

В бытность директором НЦПИ [2] я втыкал флажки в те столицы субъектов Российской Федерации, где появлялись специалисты по правовой информатизации и была установлена модемная связь для оперативного обмена правовой информацией. Они получали от нас производственные программные продукты и обновление к базе данных правовой информации «Эталон» (авторские права)<sup>8</sup>, а нам передавали отчеты и статистическую информацию. Самой большой радостью был флажок, воткнутый в поселке Палана Камчатской области. И я понимаю, что самое важное в работе любого начальника найти кадры, которые способны решить поставленные задачи. К сожалению, во время подготовки этой статьи пришло печальное известие: не дожив до шестидесяти лет, скончался один из авторов «Эталона» — бывший первый заместитель директора НЦПИ Игорь Георгиевич Иванов.

<sup>6</sup> Морозов А.В., Филатова Л.В. Научно-педагогическая деятельность в сфере создания Свода законов Российской Федерации на базе Единого федерального регистра нормативных правовых актов. Сборник докладов VII Всероссийской научно-практической конференции «Ведение федеральных регистров и государственных реестров в системе „НПА РФ“ ЕСИТО МЮ РФ». М.: ФГУ НЦПИ при Минюсте России, 2016. 43 с.

<sup>7</sup> Морозов А.В. Актуальные проблемы ведения Единого регистра нормативных правовых актов в целях мониторинга правоприменения. Сборник материалов международной научно-практической конференции «Актуальные проблемы систематизации законодательства, информационного права и информационной безопасности». М.: ФГУ НЦПИ при Минюсте России, 2014. С. 50—62.

<sup>8</sup> Герцев К.Н., Иванов И.Г., Морозов А.В. и др. Программный комплекс «Эталон». Свидетельство об официальной регистрации программы для ЭВМ № 960424 от 23.09.1996 Российского агентства по правовой охране программ, баз данных и топологий микросхем (РосАПО).

По воспоминанию ветерана юстиции начальника управления специальных судов Белоусова Льва Вячеславовича, он высказал Теребилову претензию о манере общения: «Мы с вами, Владимир Иванович, работаем уже много лет, а я от вас ласкового слова ни разу не слышал». Владимир Иванович нахмурился, но затем улыбнулся и сказал: «Но ты же не девушка!».

Но его тогда молодой помощник Голубов Николай Васильевич, позже работавший у меня в Департаменте правовой информатизации и научно-технического обеспечения заместителем начальника отдела, считает, что мнение подчиненных о жесткости Теребилова — это попытка объяснить требовательность Владимира Ивановича к результатам выполнения поставленной задачи.

В Министерстве юстиции Российской Федерации при его первом министре Федорове Николае Васильевиче сложилась интересная традиция. Все вновь назначенные министры прежде всего встречались с Владимиром Ивановичем Теребиловым.

О Владимире Ивановиче написано немало воспоминаний, но я бы хотел рассказать о неизвестных фактах его биографии. Например, он дважды встречался с Владимиром Ильичем Лениным. Для современных молодых людей сейчас это малозначительное событие, а во времена Советского Союза эта встреча была подобно встрече с богом.

А как Владимир Иванович встретился с Лениным? Все очень просто — Ленин поселился перед революцией у одной революционерки в доме, где в 1916 году родился и жил Владимир Иванович Теребилов. Будущий вождь мирового пролетариата повстречал маленького Володю, которого выгуливала няня. Будучи в хорошем настроении, вождь решил поприветствовать малыша. А когда он узнал, что малыш имеет такое же имя, попытался с ним пообщаться поближе. Это было весной, а осенью уже подросший Володя смог самостоятельно ответить на приветствие вождя.

Но у Владимира Ивановича были и страшные воспоминания. Ленинградская блокада, которую он пережил, в некоторые месяцы уносившая по 10 тысяч жизней в день, наложила на Теребилова В.И. свой отпеча-

ток. По рассказам его детей, «он до последнего дня на подоконнике хранил коробку с сухарями, регулярно обновляя ее содержимое». Чтобы молодежь понимала: это делал человек, обеспеченный всем на свете по высшему разряду, тем более любым продовольствием.

Наслушавшись в постсоветские годы историй о страшных событиях во время блокады, дети Теребилова пытались обсуждать поведение ленинградцев, но Владимир Иванович строго запретил им это делать, сказав, что «мирные люди в мирное время не могут в полной мере оценить ту чудовищную ситуацию, на фоне которой совершались преступления», некоторые страшные истории надо обязательно рассматривать только в контексте блокадных условий.

Когда я поинтересовался у детей, в чем секрет долголетия их отца, они рассказали, что летом в свободное от работы время они ходили в походы на байдарках, а зимой в Подмосковье — на лыжах. Дочь Светлана, которая, к сожалению, недавно ушла из жизни, вспоминала, как папа во время школьных лыжных соревнований бежал по параллельной лыжне и погонял их с подругой лыжной палкой.

Наши судьбы в чем-то похожи. После долгой службы в системе Минюста, я, как и Владимир Иванович, попал на преподавательскую работу в МГУ имени М.В. Ломоносова, где и тружусь по сей день [3].

Мне в жизни повезло, я встречал очень известных и талантливых людей, с которых брал пример отношения к работе [4]. В советское время все знали стихотворение Маяковского с вопросом «сделать бы жизнь с кого». На этот вопрос я хотел бы рекомендовать молодежи брать пример с Владимира Ивановича Теребилова! Так полезно и содержательно прожить жизнь, оставаясь до конца в работоспособном состоянии!

В заключение прошу прощения у родственников и коллег, если мои воспоминания были не такими «корректными», как представляется их участникам. Это моя личная трактовка исторических событий, связанных с почти тридцатипятилетним периодом работы в Министерстве юстиции. Желаю всем коллегам мира, здоровья, спокойствия души, долгих лет жизни и новых творческих успехов!

## Литература

1. Морозов А.В. Некоторые страницы истории Научного центра правовой информации // Правовая информатика. 2025. № 2. С. 6—10. DOI: 10.24412/1994-1404-2025-2-6-9.
2. History of legal informatization in Russia. Международная конференция «Высокие технологии: история и развитие». Институт истории естествознания и техники РАН. М., 2022. IEEE — Authors Rights and Responsibilities. ORCID: 0000-0002-5016-0833. RSCI Web of Science. С. 22—25. IEEE Catalog Number: CFP22DF7-POD ISBN (Print-On-Demand): 979-8-3503-2015-2 ISBN (Online): 979-8-3503-2014-5. 10.1109/HISTHIGHTECH57099.2022.10038185. Издатель: IEEE. Место проведения конференции: Москва, Российская Федерация.
3. Морозов А.В. Научно-педагогическая деятельность кафедры компьютерного права и информационной безопасности ВШГА им. М.В. Ломоносова // Вестник Московского университета. Серия 26: Государственный аудит. Издательство МГУ, 2024. № 4. С. 53—68.

4. Морозов А.В. К 100-летию со дня рождения великого ученого информационного права России Илларию Лаврентьевну Бачило // Вестник Московского университета. Серия 26: Государственный аудит. Издательство МГУ, 2026. № 1. С. 101—114. DOI: 10.55959/MSU2413-631X-27-16-1-08.

**SECTION:**  
CONSTITUTIONAL LAW

## TO THE ANNIVERSARY OF THE CREATOR OF THE CODE OF LAWS OF THE USSR, VLADIMIR IVANOVICH TEREBILOV

**Morozov A.V.<sup>9</sup>**

**Keywords:** history of state and law, systematization of regulatory legal acts, legal informatics, information and legal support, Code of Laws of the USSR, Ministry of Justice, Scientific Centre for Legal Information, historical and legal research, information law.

### **Abstract**

The article presents a historical and biographical study devoted to Vladimir Ivanovich Terebilov, Minister of Justice of the USSR, Chairman of the Supreme Court of the USSR, and one of the organizers of the creation of the Code of Laws of the USSR. Based on personal recollections and testimonies of colleagues and family members, the main stages of V.I. Terebilov's professional and public activities are examined, as well as the key areas of his work as Minister of Justice of the USSR, including the development of legislation, the bar, notarial services, legal informatization, and international legal cooperation.

Particular attention is paid to the establishment of the Scientific Centre for Legal Information and the systematization of Soviet legislation. The article concludes that it is necessary to study and apply V.I. Terebilov's historical experience in improving the modern system of legislation systematization. The article is of interest to researchers of the history of state and law, information law, legal informatics, as well as employees of the justice system.

### **References**

1. Morozov A.V. Nekotorye stranitsy istorii Nauchnogo tsentra pravovoi informatsii // Pravovaia informatika. 2025. No. 2. S. 6—10. DOI: 10.24412/1994-1404-2025-2-6-9.
2. History of legal informatization in Russia. Mezhdunarodnaia konferentsiia "Vysokie tekhnologii: istoriia i razvitie". Institut istorii estestvoznaniia i tekhniki RAN. M., 2022. IEEE — Authors Rights and Responsibilities. ORCID: 0000-0002-5016-0833. RSCI Web of Science. S. 22—25. IEEE Catalog Number: CFP22DF7-POD ISBN (Print-On-Demand): 979-8-3503-2015-2 ISBN (Online): 979-8-3503-2014-5. 10.1109/HISTHIGHTECH57099.2022.10038185. Izdatel': IEEE. Mesto provedeniia konferentsii: Moskva, Rossiiskaia Federatsiia.
3. Morozov A.V. Nauchno-pedagogicheskaia deiatel'nost' kafedry komp'iuternogo prava i informatsionnoi bezopasnosti VShGA im. M.V. Lomonosova // Vestnik Moskovskogo universiteta. Seriya 26: Gosudarstvennyi audit. Izdatel'stvo MGU, 2024. No. 4. S. 53—68.
4. Morozov A.V. K 100-letiiu so dnia rozhdeniia velikogo uchenogo informatsionnogo prava Rossii Illarii Lavrent'evny Bachilo // Vestnik Moskovskogo universiteta. Seriya 26: Gosudarstvennyi audit. Izdatel'stvo MGU, 2026. No. 1. S. 101—114. DOI: 10.55959/MSU2413-631X-27-16-1-08.



<sup>9</sup> **Andrei V. Morozov**, Dr.Sc. (Law), Ph.D. (Technology), Professor, Academician of the Russian Academy of Natural Sciences, Professor at the Department of Computer Law and Information Security of the Higher School of Public Audit of the Lomonosov Moscow State University, 2nd class Active State Councillor of Justice, Moscow, Russian Federation.

E-mail: [av\\_morozov@list.ru](mailto:av_morozov@list.ru)

# СИСТЕМА ФИНАНСОВЫХ ОБЯЗАТЕЛЬСТВ КАК АЛГОРИТМ РАЗВИТИЯ ФИНАНСОВО-ПРАВОВЫХ ИНСТИТУТОВ

Васянина Е.Л.<sup>1</sup>

**Ключевые слова:** финансовое право, налоги, бюджет, расходы, кредит, государственный долг, обязательства, финансы.

## Аннотация

**Цель:** заключается в определении системы финансовых обязательств, составляющей существо финансового права, а также в формулировании ряда обоснованных и взаимосогласованных предложений, направленных на переориентацию технико-юридического аппарата кредитных, фискальных, расходных и долговых обязательств на достижение целей финансово-правового регулирования, отвечающим современным экономическим вызовам.

**Метод исследования:** общенаучные методы анализа и синтеза, сравнительно-правовой, формально-юридический методы.

**Результат:** сделан вывод о том, что развитие теории финансовых обязательств должно идти по пути разработки как общих положений о финансовых обязательствах, включая вопросы исполнения финансовых обязательств, положения об ответственности за нарушение финансовых обязательств, о перемене лиц в обязательстве и т. д., так и особенной части, охватывающей отдельные виды финансовых обязательств, обеспечивающих функционирование финансовой системы государства. Обосновывается, что эмиссионная деятельность государства имеет в своей основе кредитные обязательства, сторонами которых являются держатели денежных знаков, с одной стороны, и их эмитент, реализующий функцию по обеспечению устойчивости курса национальной валюты, — с другой. Такой подход, способствующий развитию двусторонней связи финансового кредитора и финансового должника, позволяет задать параметры осуществления права требования держателей денежных знаков к их эмитенту в случае ненадлежащей реализации последней функции по обеспечению устойчивости курса рубля. Требуется развития сформированная в бюджетном законодательстве совокупность финансовых обязательств, обеспечивающих сбалансированность бюджетов. Учитывая централизованный порядок распределения налоговых доходов между бюджетами разных уровней бюджетной системы, во избежание роста коммерческого долга субъектов Российской Федерации целесообразно рассмотреть вопрос о создании и применении централизованного механизма осуществления займов и распределения их среди регионов.

**Научная новизна:** заключается в определении системы финансовых обязательств, составляющих существо финансового права, и служащих ориентиром для развития финансового законодательства, а также в разработке обоснованных предложений, направленных на переориентацию технико-юридического аппарата финансовых обязательств на достижение национальных целей развития государства.

DOI: 10.24412/1994-1404-2026-3-00-11

## Введение

Изменение парадигмы будущего правовой модели финансовых отношений, вызванное обострением геополитических противоречий и структурной перестройкой экономики, должно происходить с учетом выработанных в финансово-правовой науке подходов к пониманию сущности финансового права, финансовой системы государства, позволяю-

щим создать необходимый правовой инструментарий, обеспечивающий наполнение экономики государства деньгами в объеме, достаточном для достижения поставленных Президентом Российской Федерации национальных целей развития страны<sup>2</sup>.

<sup>2</sup> Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собрание законодательства РФ. 2024. № 20. Ст. 2584.

<sup>1</sup> Васянина Елена Леонидовна, доктор юридических наук, доцент, ведущий научный сотрудник сектора административного права и административного процесса Института государства и права РАН, г. Москва, Российская Федерация.

E-mail: [elenavasianina@yandex.ru](mailto:elenavasianina@yandex.ru)



На сегодняшний день в юридической литературе разработаны и представлены: функциональный подход, характеризующий финансовую систему как совокупность звеньев финансовых отношений<sup>3</sup>; фондовый, рассматривающий сферу публичных финансов через призму совокупности денежных фондов; институциональный, сфокусированный на развитии устойчивых финансово-правовых институтов; субъектно-организационный, в рамках которого во главу угла ставятся органы и организации, участвующие в управлении финансами [1].

Следование указанным подходам в процессе формирования структурной модели построения правового материала, обеспечивающего развитие финансовой системы, до сих пор не позволило достигнуть уровня правового регулирования финансово-денежных отношений, отвечающего новым экономическим вызовам. Сформированные финансово-правовые институты получили обособленное развитие в виду слабой проработки общей части финансового права и отсутствия юридических конструкций, обеспечивающих достижение баланса целей денежно-кредитной, бюджетно-налоговой и таможенно-тарифной политики, закрепляющих ключевые направления развития финансового законодательства. Отсутствие алгоритма взаимодействия финансово-правовых институтов, развитие которых продолжает строиться вокруг не имеющей законодательного закрепления категории «финансовая деятельность», приводят к искажениям финансовой системы, не дающим возможность перейти на траекторию устойчивого экономического роста.

Учитывая изложенное, настоятельной необходимостью является поиск правового инструментария, позволяющего задать параметры развития механизма финансово-правового регулирования в нужном для укрепления финансового суверенитета государства ключе.

### **Правовые вопросы исполнения финансовых обязательств**

В настоящее время перенастройка правовых контуров финансовой системы происходит преимущественно в фокусе совершенствования правового регулирования контрольно-организационных отношений, которые, обеспечивая развитие финансово-кредитного механизма, имеют ярко выраженную административно-правовую природу. На фоне многочисленных корректировок, которым подвергаются акты финансового законодательства, в части реформирования порядка осуществления финансового (бюджетного) контроля, фискального администрирования, бюджетного процесса и иных аспектов управленческой деятельности в сфере финансов, крайне мало внимания законодатель

уделяет развитию финансовых обязательств, являющихся инструментом реализации единой финансовой и денежно-кредитной политики государства. Например, на фоне расширения управленческих полномочий Банка России в финансовой сфере и придания ему статуса мегарегулятора в Федеральном законе «О Центральном банке Российской Федерации (Банке России)» наблюдается фрагментарное закрепление обязательств, возникающих из сделок, совершаемых Банком России с кредитными организациями в целях реализации единой государственной денежно-кредитной политики.

В части регулирования фискального обложения периодически принимаемые федеральные законы о внесении изменений и дополнений в НК РФ касаются, как правило, установления и введения новых налогов и сборов, корректировки элементов юридического состава налога по поводу изменения ставки, налогового периода, сроков уплаты, установления (отмены) налоговых льгот и т. д. Вопросы же, касающиеся существа фискального обязательства, конкретизации условий его исполнения в случае изменения экономических параметров сделки, цены контракта, перемены лиц в обязательстве при том, что законодатель не исключает исполнение налоговой обязанности третьими лицами, выведены из поля зрения законодателя и отданы на откуп правоприменителю.

Хаос, происходящий в финансовом правотворчестве, привел к тому, что развитие финансового законодательства и складывающейся на его основе правоприменительной практики пошло по пути переориентации на применение альтернативных правовых инструментов регулирования финансовых отношений. Например, вне рамок НК РФ сложилась финансово-правовая модель реструктуризации налоговой задолженности, в рамках которой исполнение налоговых обязательств фискальными должниками происходит посредством деятельности Фонда содействия реструктуризации задолженности, созданного на основе Меморандума о содействии реабилитации бизнеса, подписанного представителями предпринимательского сообщества и федеральных органов власти, в числе которых ФНС России. А спорные вопросы, связанные с исполнением налоговых обязательств, разрешаются на основании налоговой оговорки в договоре.

В контексте изложенного уместно вспомнить недавно сформированный Конституционным Судом РФ подход<sup>4</sup>, в рамках которого споры, касающиеся исчисления и уплаты НДС, в случае изменения законодательства Российской Федерации о налогах и сборах в части увеличения фискального бремени в течение исполнения

<sup>3</sup> Пятковская Ю.В. Систематизация финансового законодательства: состояние и перспективы // Финансовое право. 2016. № 9. С. 12—15.

<sup>4</sup> Постановление Конституционного Суда РФ от 25. 11. 2025 № 41-П «По делу о проверке конституционности п. 1 и 2 ст. 424 Гражданского кодекса Российской Федерации, п. 1 ст. 168 Налогового кодекса Российской Федерации, пп. «а» п. 1 ст. 1 Федерального закона от 31 июля 2020 года № 265-ФЗ „О внесении изменений в часть вторую Налогового кодекса Российской Федерации“ в связи с жалобой публичного акционерного общества „Банк ВТБ“» // Собрание законодательства РФ. 2025. № 48 (Часть IV). Ст. 7476.

длящихся хозяйственных договоров, предложено разрешать с учетом положения ст. 451 ГК РФ об изменении и расторжении договора в связи с существенным изменением обстоятельств.

Иными словами, развивается тактика, направленная на отказ от конкретизации в НК РФ элементов юридического состава налога в пользу включения в хозяйственный договор налоговой оговорки, позволяющей участникам гражданского оборота предусмотреть риски, влияющие на издержки, связанные с предпринимательской деятельностью, включая порядок формирования цены. Кроме того, вместо корректировки положений НК РФ в части регламентации порядка исполнения налоговых обязательств получила развитие практика издания меморандумов по поводу правовой квалификации хозяйственных операций для целей налогообложения [2].

Возникают проблемы, связанные с исполнением кредитных обязательств, обеспечивающих развитие бюджетной системы. Речь, в частности, идет об обязательствах в сфере банковского и бюджетного кредитования. На фоне предусмотренной БК РФ развитой системы бюджетного кредитования, охватывающей как собственно бюджетный кредит, так и специальные казначейские кредиты, казначейские инфраструктурные кредиты, займы, предоставляемые за счет привлеченных средств Фонда национального благосостояния (ФНБ) и т. д., активное развитие получил коммерческий кредит, доля которого в структуре государственного долга регионов вновь начала возрастать. По данным Счетной палаты РФ, предусмотренные бюджетным законодательством кредитные инструменты используются недостаточно эффективно. При этом в условиях роста государственного долга субъектов РФ в структуре их долговых обязательств значительно увеличилась доля кредитов, полученных субъектами Российской Федерации от кредитных организаций, с 7,2 % на 1 января 2025 года до 19,4 % на 1 января 2026 года (почти в 3 раза)<sup>5</sup>.

Изложенное свидетельствует о том, что в государстве сформирован не поддающийся никакому логическому объяснению кредитный механизм, обеспечивающий формирование и погашение государственного долга субъектов РФ, суть которого состоит в том, что рост коммерческих кредитов в структуре долга регионов сопровождается, с одной стороны, предоставлением бюджетных кредитов регионам (муниципальным образованиям) для погашения долговых обязательств по кредитам, полученным ими от кредитных организаций<sup>6</sup>, а с другой — списанием задолженности субъ-

ектов РФ по бюджетным кредитам, предоставленным из федерального бюджета<sup>7</sup>. Иными словами, созданная в государстве правовая модель погашения государственного долга регионов обеспечивает удовлетворение коммерческих целей банковского сектора за счет средств бюджетной системы.

### **О развитии теории финансовых обязательств**

Поскольку правовое регулирование как разновидность управленческого процесса может осуществляться только с помощью «двоичности информации», выраженной в соответствующих субъективных правах и обязанностях<sup>8</sup>, обязательство, обеспечивающее двустороннюю связь финансового кредитора и финансового должника, является ключевым инструментом развития финансово-кредитного механизма государства, а разрабатываемая в юридической науке теория финансовых обязательств должна стать ориентиром в процессе совершенствования финансового законодательства.

В литературе, до сих пор ориентированной на изучение категории «финансовая деятельность», а также в финансовом законодательстве пока не выстроена система финансовых обязательств, корреспондирующая финансово-правовым институтам, регулирующим финансово-денежный механизм, отправной точкой в развитии которого являются кредитные обязательства, направленные на создание платежеспособности участников гражданского оборота, на смену которым приходят фискальные обязательства, обеспечивающие трансформацию частной денежной массы в публичный доход, а затем расходные обязательства, посредством которых происходит распределение бюджетных средств между их получателями и долговые обязательства, возникающие в целях финансирования дефицита бюджета.

Несформированность системы финансовых обязательств, составляющих существо финансово-денежного механизма, во много обусловлена тем, что под влиянием получившего активное развитие метода одностороннего должностования в финансово-правовых

---

Российской Федерации (муниципального образования) в виде обязательств по государственным (муниципальным) ценным бумагам субъекта Российской Федерации (муниципального образования) и кредитам, полученным субъектом Российской Федерации (муниципальным образованием) от кредитных организаций, иностранных банков и международных финансовых организаций, на 2022 год» // Собрание законодательства РФ. 2022. № 20. Ст. 3287.

<sup>7</sup> Федеральный закон от 13.07.2024 № 177-ФЗ «О внесении изменений в Бюджетный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ 2024. № 29 (Часть III). Ст. 4106; постановление Правительства РФ от 01.02.2025 № 79 «Об утверждении Правил списания задолженности субъектов Российской Федерации перед Российской Федерацией по отдельным бюджетным кредитам и направления субъектами Российской Федерации средств, высвобождаемых в результате списания задолженности субъектов Российской Федерации по указанным бюджетным кредитам» // Собрание законодательства РФ. 2025. № 6, Ст. 435.

<sup>8</sup> Малько А.В. Стимулы и ограничения в праве. Саратов. филиал ИГП РАН. 2-е изд., перераб. и доп. М.: Юрист, 2005. 248 с.

<sup>5</sup> Оперативный доклад Счетной палаты Российской Федерации о ходе исполнения консолидированных бюджетов субъектов Российской Федерации: январь — декабрь 2025 года. URL: <https://ach.gov.ru/upload/iblock/a17/zr1us2ahf2g6b9b6z3k4ij6kdwm0dmr/Operdoklad-IV-2025-KBS-20260306.pdf>

<sup>6</sup> Абз. 6 п. 1 ст. 93.3. Бюджетного кодекса Российской Федерации; постановление Правительства РФ от 05.05.2022 № 815 «Об утверждении Правил предоставления, использования и возврата субъектами Российской Федерации бюджетных кредитов, полученных из федерального бюджета для погашения долговых обязательств субъекта

исследованиях, относящихся к советскому периоду, преобладала точка зрения, согласно которой обязательство — это категория гражданского права, которая не применима к регулированию сферы публичных финансов.

Вместе с тем дореволюционные исследователи, разрабатывающие теорию обязательств, не исключали из системы обязательственных правоотношений обязательства, вытекающие из закона<sup>9</sup>, в т.ч. финансовые обязательства. В частности, К.Д. Кавелин в работе «Права и обязанности по имуществам и обязательствам в применении к русскому законодательству: опыт систематического обозрения» к обязательствам относил подати, налоги, сборы, пошлины, а также деньги, ценные бумаги<sup>10</sup>. А выделенные в литературе ключевые признаки обязательств, отличающие их от иных правоотношений, вполне применимы к финансовым обязательствам. К числу таких признаков относится особый характер действий, заключающийся в том, что юридическую обязанность, охватываемую обязательством, могут составлять лишь действия, представляющие материальную ценность. Кроме того, в отличие от вещных правоотношений, обязательство содержит отношение между кредитором и должником, в результате чего кредитор может получить предмет только посредством действий, совершаемых должником<sup>11</sup>.

Подход, ориентированный на признание финансового обязательства в качестве ключевой категории финансового права, не получил должного развития в XX веке, что во многом было обусловлено политикой военного коммунизма, направленной на свертывание товарно-денежных отношений, в результате чего исследования по теории финансовых обязательств, надолго выпали из фокуса финансово-правовой науки.

Работы, посвященные внедрению обязательственного метода в регулирование публичных финансов, начинают появляться в 80-е гг. XX века<sup>12</sup>. Позднее в юридической литературе разрабатывается понятие налогового обязательства, его структура. В составе налогового права выделяется налоговое обязательственное право<sup>13</sup>. Появляются исследования, касающиеся изучения существа финансовых обязательств, их видов [3—5].

Вместе с тем до сих пор не завершена работа по систематизации фискальных обязательств, число которых

продолжает расти, создавая дополнительную фискальную нагрузку для предпринимателей [6]. Недостаточно внимания уделяется изучению расходных финансовых обязательств [7, 8], обеспечивающих финансирование государственных расходов, а также кредитных обязательств, составляющих существо правового механизма денежной эмиссии.

Отрицание существования финансовых обязательств расходного типа приводит к тому, что финансирование государственных расходов представляет собой ничто иное, как распорядительный акт уполномоченного субъекта по доведению лимитов бюджетных обязательств до получателей бюджетных средств, в результате чего право требования исполнителей по государственным контрактам на увеличение финансирования в случае изменения цены контракта практически невозможно реализовать<sup>14</sup>, а связанные с этим споры рассматриваются на основании положений гражданского законодательства<sup>15</sup>.

Непринятие обязательственной природы правоотношений, возникающих по поводу денежной эмиссии, является причиной того, что выпуск денежных знаков в обращение превращается в односторонний акт государства по наделению платежеспособностью участников гражданского оборота. А положение ст. 75 Конституции РФ, на основании которого за Банком России закреплена функция по защите и обеспечению устойчивости рубля, не обеспечено действенным механизмом защиты права требования субъектов-держателей денежных знаков к их эмитенту в случае невыполнения последним конституционных предписаний.

Сложившийся подход противоречит природе денег, являющихся обязательствами особого рода, специфика которых заключается в том, что, во-первых, роль должника в них играют публично-правовые образования, выпустившие эти денежные знаки, а во-вторых, они теряют долю своей цены при большом их избытке<sup>16</sup>. Именно такой подход отражен в работе К.Д. Кавелина «Права и обязанности по имуществам и обязательствам в применении к русскому законодательству». Несколько по-иному природа денег описана Н.И. Ладыженским, который, с одной стороны, рассматривал деньги как выражение права владения стоимостью товаров, тем самым связывая их с реализацией вещного права, однако, с другой стороны, приписывал им характер долгового обязательства со стороны

<sup>9</sup> Голевинский В.И. О происхождении и делении обязательств // Соч. В. Голевинского. Варшава : тип. О. Бергера, 1872. 302 с.

<sup>10</sup> Кавелин К.Д. Права и обязанности по имуществам и обязательствам в применении к русскому законодательству : опыт систематического обозрения. СПб. : тип. М.М. Стасюлевича, 1879. 410 с.

<sup>11</sup> Дернбург Г. Пандекты Г. Дернбурга. Обязательственное право / пер. под руков. и ред. проф. П. Соколовского; пересмотрено и согласовано с 7 изд. подлинника приват-доцентами А.Э. Вормсом и И.И. Вульффертом. М., 1911. 396 с.

<sup>12</sup> Запольский С.В. Правовые вопросы самофинансирования предприятий в условиях полного хозяйственного расчета (финансово-правовой аспект) : автореф. дис. ... д-ра юрид. наук : 12.00.02 / ВНИИ сов. гос. стр-ва и законодательства. М., 1989. 45 с.

<sup>13</sup> Винницкий Д.В. Российское налоговое право: проблемы теории и практики. СПб., 2003.

<sup>14</sup> Решение Арбитражного суда Орловской области от 05.08.2024, постановления Девятнадцатого арбитражного апелляционного суда от 07.05.2025 и Арбитражного суда Центрального округа от 25 ноября 2025 г. по делу № А48-2988/2024 // Справочно-правовая система.

<sup>15</sup> Постановление Третьего Арбитражного апелляционного суда от 22.11. № А69-333/2024; постановление Двадцатого арбитражного апелляционного суда от 06.09.2023 № 20АП-3207/2023 по делу № А09-4044/2021 // Справочно-правовая система.

<sup>16</sup> Кавелин К.Д. Права и обязанности по имуществам и обязательствам в применении к русскому законодательству : опыт систематического обозрения. СПб. : тип. М.М. Стасюлевича, 1879. 410 с.



держателя денежных знаков, обеспечивающих процесс обращения товаров<sup>17</sup>.

Наглядной иллюстрацией кредитной сущности денег является описанная в литературе денежная система островов Яп, в рамках которой роль денег выполняли огромные камни, являющиеся носителями информации о системе кредитных обязательств местных жителей [9]. Тезис о том, что деньги — это обязательства особого рода, подтверждается современной денежной теорией, согласно которой государство, будучи единственным эмитентом национальной валюты, наделяет ее покупательной способностью через систему обязательств [10].

И наконец, именно обязательственный характер отличает национальную валюту от криптовалюты, в отношении которой, в противоположность фиатным деньгам, отсутствует обязанное лицо перед каждым ее обладателем, что является основной причиной высокой волатильности децентрализованной цифровой валюты<sup>18</sup>.

Неразработанность юридической конструкции финансового обязательства, обеспечивающего процесс выпуска денежных знаков в обращение, затрудняет реализацию права требования держателей денег к их эмитенту по поводу осуществления последним возложенной на него функции по обеспечению устойчивости курса национальной валюты и поддержанию покупательной способности денежных знаков. Так, применяемые в 90-е гг. XX века инструменты восстановления покупательной способности сбережений, к числу которых относятся индексация<sup>19</sup>, компенсация<sup>20</sup> и долговой рубль<sup>21</sup>, стало предметом острых политических дискуссий и судебных разбирательств<sup>22</sup>. А сформированный

в отдельных судебных решениях подход, на основании которого в условиях резкого роста инфляции, изменения курса валют, удовлетворялись требования заемщиков к банкам о прекращении кредитных обязательств в связи с ненадлежащей реализацией Банком России функции по обеспечению устойчивости курса рубля<sup>23</sup>, пока не стал ориентиром в рассмотрении подобных категорий дел.

## Заключение

Современные исследования в области финансового права следует нацелить на совершенствование системы финансовых обязательств (табл. 1), составляющих существо финансового права, посредством переориентации технико-юридического аппарата кредитных, фискальных, расходных и долговых обязательств на цели развития финансово-кредитной системы государства, отвечающие современным экономическим вызовам.

Развитие теории финансовых обязательств должно идти по пути разработки как *общих положений* о финансовых обязательствах, включающих понятие финансового обязательства, исполнение финансовых обязательств, положения об ответственности за нарушение финансовых обязательств, о перемене лиц в обязательстве и т. д., так и *особенной части*, описывающей отдельные виды финансовых обязательств, обеспечивающих функционирование финансовой системы государства.

Учитывая обязательственную природу денег, а также закрепленные нормативными правовыми актами формы, порядок и условия осуществляемого Банком России рефинансирования, есть все основания утверждать, что эмиссионная деятельность государства в основе своей имеет кредитные обязательства, сторонами которых являются держатели денежных знаков, с одной стороны, и их эмитент, реализующий функцию по обеспечению устойчивости курса национальной валюты, — с другой.

Кредитные обязательства, составляющие основу эмиссионной деятельности государства, с учетом оснований возникновения и порядка их исполнения делятся на:

- 1) кредитные обязательства, обеспечивающие рефинансирование, т. е. кредитование Банком России кредитных организаций;
- 2) кредитные обязательства, сопровождающие эмиссию кредитных денег, проводимую поднадзорными Банку России кредитными организациями.

Для достижения баланса целей монетарной и бюджетно-налоговой политики кредитные обязательства, осуществляемые в процессе эмиссионной деятельности государства, должны содержать условия,

<sup>17</sup> Лодыженский, Николай Иванович. Деньги как выражение права владения. Петроград : 1918. 86 с.

<sup>18</sup> Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 2020. № 31 (часть I). Ст. 5018.

<sup>19</sup> В соответствии с Основами законодательства Союза ССР и Республик «Об индексации доходов населения» от 25 июня 1991 г. № 2266-1 индексация доходов населения — это механизм повышения денежных доходов граждан, позволяющий частично или полностью возместить им удорожание потребительских товаров и услуг.

<sup>20</sup> Согласно Указу Президента СССР от 22 марта 1991 года № УП-1708 «О компенсации населению потерь от обесцененных сбережений в связи с единовременным повышением розничных цен», а также постановлению Съезда народных депутатов РФ от 23 марта 1993 г. № 4677-1 «О компенсации и восстановлении сбережений граждан Российской Федерации» компенсация рассматривается в качестве механизма, направленного на обеспечение восстановления уровня покупательной способности денежных средств.

<sup>21</sup> Долговой рубль представляет собой единицу номинала целевого долгового обязательства, рассчитываемого исходя из изменения соотношения контрольной стоимости необходимого социального набора и базовой стоимости данного набора (Федеральный закон от 6 июля 1996 № 87-ФЗ «О порядке установления долговой стоимости единицы номинала целевого долгового обязательства Российской Федерации»).

<sup>22</sup> Апелляционное определение Московского городского суда от 08.11.2012 г. по делу № 11-26246/12; решение Верховного Суда Российской Федерации в решении от 01.12.2010 г. № ГКПИ410-1179; определение Конституционного Суда от 19.10.2010 г. № 1336 — О-О.

<sup>23</sup> Решение Моршанского районного суда № 2-1661/2015 2-1661/2015~М-1466/2015 М-1466/2015 от 19 ноября 2015 г. по делу № 2-1661/2015. URL: <https://sudact.ru/regular/doc/2BaZ0R5OB9Zu/> (дата обращения: 10.04.2020).



касающиеся адресности и целевого освоения кредитных денег. Этого можно достичь посредством применения ст. 37 Федерального закона «О Центральном Банке Российской Федерации (Банке России)», позволяющей Банку России применять несколько процентных ставок по различным видам операций в рамках осуществля-

емой им кредитной деятельности, а также в результате установления дифференцированных процентных ставок за кредиты, предоставляемые поднадзорными мегарегулятору банками, хозяйствующим субъектам в зависимости от целей их использования.

Таблица 1

**Система финансовых обязательств**

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>кредитные</b>  | <ul style="list-style-type: none"> <li>- кредитные обязательства, обеспечивающие рефинансирование, т. е. кредитование Банком России кредитных организаций<sup>1</sup></li> <li>- кредитные обязательства, обеспечивающие осуществление поднадзорными Банку России кредитными организациями эмиссию кредитных денег<sup>2</sup></li> <li>- бюджетный кредит<sup>3</sup></li> <li>- казначейские инфраструктурные кредиты<sup>4</sup></li> <li>- займы, предоставляемые за счет привлеченных средств ФНБ<sup>5</sup></li> </ul>                                                                                                                                                                                                                                                   |
| <b>фискальные</b> | <ul style="list-style-type: none"> <li>- фискальные обязательства, возникающие из закона (налоги, сборы, таможенные платежи)</li> <li>- фискальные деликтные обязательства (штрафы за нарушение законодательства)</li> <li>- фискальные обязательства, имеющие компенсационный характер (взносы операторов связи сети общего пользования<sup>6</sup>, отчисления организациями, эксплуатирующими особо радиационно опасные и ядерно опасные объекты, на формирование резервов, предназначенных для обеспечения безопасности указанных производств и объектов на всех стадиях их жизненного цикла и развития<sup>7</sup>; взносы в компенсационные фонды саморегулируемых организаций<sup>8</sup>, платежи за негативное воздействие на окружающую среду<sup>9</sup>)</li> </ul> |
| <b>расходные</b>  | <ul style="list-style-type: none"> <li>- расходные финансовые обязательства, исполнение которых обеспечивается на основании государственных (муниципальных) контрактов</li> <li>- расходные финансовые обязательства, исполнение которых обеспечивается на основании соглашений о предоставлении грантов (субсидий)</li> <li>- расходные финансовые обязательства, связанные с исполнением концессионных соглашений</li> <li>- расходные финансовые обязательства, связанные с осуществлением бюджетных инвестиций<sup>10</sup></li> </ul>                                                                                                                                                                                                                                      |
| <b>долговые</b>   | <ul style="list-style-type: none"> <li>- обязательства по кредитам, привлеченным от кредитных организаций, иностранных государств, международных финансовых организаций и (или) иных субъектов международного права, иностранных юридических лиц</li> <li>- обязательства по государственным ценным бумагам</li> <li>- обязательства по бюджетным кредитам</li> <li>- обязательства по государственным гарантиям<sup>11</sup></li> <li>- обязательства по гарантированным сбережениям граждан<sup>12</sup></li> </ul>                                                                                                                                                                                                                                                           |

<sup>1</sup> Ст. 40 Федерального закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» // Собрание законодательства РФ. 2002. № 28. Ст. 2790; Условия проведения операций по предоставлению и погашению кредитов Банка России, обеспеченных ценными бумагами или правами требования по кредитным договорам (приложение 1 к приказу Банка России от 24.12.2019 N ОД-2967); Указание Банка России от 18.09.2023 № 6531-У «О размерах процентных ставок по кредитам Банка России» // Вестник Банка России. 2023. № 62; Указание Банка России от 15.09.2021 № 5930-У «О форме и условиях рефинансирования кредитных организаций под обеспечение» // Вестник Банка России. 2021. № 75; Указание Банка России от 23.04.2014 № 3239-У «О предоставлении Банком России кредитов без обеспечения кредитным организациям» // Вестник Банка России. 2014. № 62.

<sup>2</sup> Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 3 14-ФЗ // Собрание законодательства РФ. 1996. № 5. Ст. 410; Федеральный закон от 21.12.2013 № 353-ФЗ «О потребительском кредите (займе)» // Собрание законодательства РФ. 2013. № 51. Ст. 6673 и др.

<sup>3</sup> Ст. 93.2 Бюджетного кодекса Российской Федерации от 31.07.1998 № 145-ФЗ // Собрание законодательства РФ. 1998. № 31. Ст. 3823.

<sup>4</sup> Ст. 93.9 БК РФ; Постановление Правительства РФ от 25.01.2025 № 48 «Об утверждении Правил предоставления Федеральным казначейством бюджетам субъектов Российской Федерации бюджетных кредитов на финансовое обеспечение реализации инфраструктурных проектов за счет временно свободных средств единого счета федерального бюджета, а также их использования и возврата» // Собрание законодательства РФ. 2025. № 7. Ст. 604.

<sup>5</sup> Постановление Правительства РФ от 02.02.2022 № 87 «О предоставлении публично-правовой компанией „Фонд развития территорий“ за счет привлеченных средств Фонда национального благосостояния займов юридическим лицам, в том числе путем приобретения облигаций юридических лиц при их первичном размещении, в целях реализации проектов по строительству, реконструкции, модернизации объектов инфраструктуры, и о внесении изменения в Положение о Правительственной комиссии по региональному развитию в Российской Федерации» // Собрание законодательства РФ. 2022. № 7. Ст. 957.

<sup>6</sup> Ст. 60 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» // Собрание законодательства РФ. 2003. № 28. Ст. 2895.

<sup>7</sup> Постановление Правительства РФ от 21.09. 2005. № 576 «Об утверждении правил отчисления организациями, эксплуатирующими особо радиационно опасные и ядерно опасные производства и объекты (кроме атомных станций), средств для формирования резервов, предназначенных для обеспечения безопасности указанных производств и объектов на всех стадиях их жизненного цикла и развития» // Собрание законодательства РФ. 2005. № 39. Ст. 3956.

<sup>8</sup> Ст. 13 Федерального закона от 01.12.2007 № 315-ФЗ «О саморегулируемых организациях» // Собрание законодательства РФ. 2007. № 49. Ст. 6076.

<sup>9</sup> Ст. 16 Федерального закона от 10.01.2002 № 7-ФЗ «Об охране окружающей среды» // Собрание законодательства РФ. 2002. № 2. Ст. 133.

<sup>10</sup> Бюджетный кодекс Российской Федерации от 31.07.1998 № 145-ФЗ // Собрание законодательства РФ. 1998. № 31. Ст. 3823.

<sup>11</sup> Ст. 98 Бюджетного кодекса Российской Федерации от 31.07.1998 № 145-ФЗ // Собрание законодательства РФ. 1998. № 31. Ст. 3823.

<sup>12</sup> Федеральный закон от 10.05.1995 73-ФЗ «О восстановлении и защите сбережений граждан Российской Федерации» // Собрание законодательства РФ. 1995. № 20. Ст. 1765.

Требуется совершенствования сформированная в бюджетном законодательстве совокупность финансовых обязательств, обеспечивающих сбалансированность бюджетов бюджетной системы государства. Поскольку рост коммерческого долга регионов, возникающий в связи с увеличением размера дефицитов бюджетов, во многом зависит от ограничивающей доходную базу региональных бюджетов и закреплённого на федеральном уровне порядка распределения налоговых доходов между бюджетами бюджетной системы, во избежание роста доли коммерческих кредитов в структуре долга публично-правовых образований целесообразно рассмотреть вопрос о создании и применении централизованного механизма осуществления займов и их распределения для покрытия дефицитов региональных бюджетов.

Переориентация технико-юридического аппарата финансовых обязательств на достижение национальных целей развития государства потребует проведения работы, направленной на устранение закреплённых в законодательстве обязательств, которых на самом деле вообще не может существовать в правовом поле по причине совпадения финансового кредитора и финансового должника. Речь, в частности, идет о долговых обязательствах по кредитам, предоставляемым государству банками с государственным участием, а также об обязательствах, возникающих в связи с размещением государственных ценных бумаг, приобретаемых кредитными организациями за счет полученных от Банка России кредитов.

## Литература

1. Запольский С.В. Правовой генезис финансовой системы России // Государство и право. 2025. № 3. С. 132—139.
2. Пепеляев С.Г. Налоги по согласованию // Налоговед. 2026. № 7. С. 4—8.
3. Запольский С.В., Васянина Е.Л. Обязательства — ключевая категория теории финансового права // Государство и право. 2022. № 8. С. 111—120.
4. Запольский С.В., Васянина Е.Л. Обязательства — способ осуществления финансовой политики государства // Государство и право. 2020. № 5. С. 55—63.
5. Васянина Е.Л. Обязательства в финансовом праве : монография. М. : РУСАЙНС, 2020. 130 с.
6. Копина А.А. Налоговая реконструкция // Финансовое право. 2022. № 4. С. 23—28.
7. Забралова О.С. Расходные обязательства в системе финансовых обязательств: проблемы теории и практики // Финансовое право. 2022. № 3. С. 12—15.
8. Чуряев А.В. Понуждение к исполнению расходного обязательства // Вестник экономического правосудия Российской Федерации. 2025. № 7. С. 97—119.
9. Васянина Е.Л., Шапсугова М.Д. Публично-правовые и частноправовые начала в механизме регулирования денежной эмиссии // Банковское право. 2021. № 5. С. 28—37.
10. Грищенко В.О., Ткачев В.Н., Остапенко В.М., Тунев В.Д. Современная денежная теория (ММТ): новая парадигма или набор рекомендаций для макроэкономической политики // Экономическая политика. 2021. Т. 16. № 3. С. 8—43.

SECTION:  
CONSTITUTIONAL LAW

# THE SYSTEM OF FINANCIAL OBLIGATIONS AS AN ALGORITHM FOR THE DEVELOPMENT OF FINANCIAL AND LEGAL INSTITUTIONS

Vasyanina E.L.<sup>24</sup>

**Keywords:** financial law, taxes, budget, expenditures, credit, public debt, obligations, finance.

<sup>24</sup> Elena L. Vasyanina, Dr.Sc. (Law), Leading Researcher at the Sector of Administrative Law and Process of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.  
E-mail: [elenavasyanina@yandex.ru](mailto:elenavasyanina@yandex.ru)

**Abstract**

**Objective:** to define the system of financial obligations that constitutes the essence of financial law, as well as to formulate a number of substantiated and mutually agreed-upon proposals aimed at reorienting the technical and legal apparatus of credit, fiscal, expenditure, and debt obligations, ensuring the development of the state's financial and credit system, taking into account modern economic challenges.

**Research method:** general scientific methods of analysis and synthesis, comparative legal methods, and formal legal methods.

**Result:** It is concluded that the development of the theory of financial obligations should proceed along the path of developing both general provisions on financial obligations, including issues of fulfilling financial obligations, provisions on liability for breach of financial obligations, changes in parties to the obligation, etc., and a specific section covering individual types of financial obligations that ensure the functioning of the state's financial system. It is substantiated that the state's issuing activities are based on credit obligations, the parties to which are banknote holders, on the one hand, and their issuer, which implements the function of ensuring the stability of the national currency exchange rate, on the other. This approach, facilitating the development of a two-way relationship between the financial creditor and the financial debtor, makes it possible to define the parameters for the implementation of the right of claim of banknote holders against their issuer in the event of the latter's improper implementation of the function of ensuring the stability of the ruble exchange rate. The set of financial obligations established in budget legislation, ensuring budget balance, requires further development. Given the centralized procedure for distributing tax revenues between budgets at different levels of the budget system, in order to avoid an increase in the commercial debt of the constituent entities of the Russian Federation, it is advisable to consider the issue of creating and applying a centralized mechanism for implementing loans and distributing them among the regions.

**Scientific novelty:** consists in defining the system of financial obligations that constitute the essence of financial law and serve as a guideline for the development of financial legislation, as well as in developing substantiated proposals aimed at reorienting the technical and legal apparatus of financial obligations to achieve the national development goals of the country.

**References**

1. Zapol'skii S.V. Pravovoi genezis finansovoi sistemy Rossii // Gosudarstvo i pravo. 2025. No. 3. S. 132—139.
2. Pepeliaev S.G. Nalogi po soglasovaniyu // Nalogoved. 2026. No. 7. S. 4—8.
3. Zapol'skii S.V., Vasianina E.L. Obiazatel'stva — kliuchevaia kategoriia teorii finansovogo prava // Gosudarstvo i pravo. 2022. No. 8. S. 111—120.
4. Zapol'skii S.V., Vasianina E.L. Obiazatel'stva — sposob osushchestvleniia finansovoi politiki gosudarstva // Gosudarstvo i pravo. 2020. No. 5. S. 55—63.
5. Vasianina E.L. Obiazatel'stva v finansovom prave : monografiia. M. : RUSAINS, 2020. 130 s.
6. Kopina A.A. Nalogovaia rekonstruktsiia // Finansovoe pravo. 2022. No. 4. S. 23—28.
7. Zabalova O.S. Raskhodnye obiazatel'stva v sisteme finansovykh obiazatel'stv: problemy teorii i praktiki // Finansovoe pravo. 2022. No. 3. S. 12—15.
8. Churiaev A.V. Ponuzhdenie k ispolneniiu raskhodnogo obiazatel'stva // Vestnik ekonomicheskogo pravosudiia Rossiiskoi Federatsii. 2025. No. 7. S. 97—119.
9. Vasianina E.L., Shapsugova M.D. Publichno-pravovye i chastnopravovye nachala v mekhanizme regulirovaniia denezhnoi emissii // Bankovskoe pravo. 2021. No. 5. S. 28—37.
10. Grishchenko V.O., Tkachev V.N., Ostapenko V.M., Tunev V.D. Sovremennaia denezhnaia teoriia (MMT): novaia paradigma ili nabor rekomendatsii dlia makroekonomicheskoi politiki // Ekonomicheskaiia politika. 2021. T. 16. No. 3. S. 8—43.



# О ПРАВОВЫХ ОСНОВАХ ДЕЯТЕЛЬНОСТИ АФФИЛИРОВАННЫХ АКЦИОНЕРНЫХ ОБЩЕСТВ В СОСТАВЕ ГОСУДАРСТВЕННЫХ КОРПОРАЦИЙ И КОМПАНИЙ

Запольский С.В.<sup>1</sup>

**Ключевые слова:** акционерное общество, государственное участие, корпоративное управление, публичный интерес, частное право, публичное право, холдинг, концерн, аффилированность, государственный оборонный заказ, системообразующая организация, стратегическое общество.

## Аннотация

**Цель работы** состоит в выявлении особенностей правового положения аффилированных акционерных обществ, входящих в состав государственных корпораций, холдингов и иных интегрированных хозяйственных структур. Особое внимание уделяется соотношению корпоративной самостоятельности таких обществ с публичными задачами государства в стратегических отраслях, оборонно-промышленном комплексе и системе поддержки системообразующих организаций.

**Методы исследования:** формально-юридический, системный и историко-правовой. Посредством формально-юридического метода проанализированы положения законодательства, регулирующие корпоративное управление, государственное участие, деятельность стратегических обществ и выполнение государственного оборонного заказа. Системный метод применен для изучения взаимосвязи корпоративных, административных, договорных и финансовых механизмов государственного воздействия. Историко-правовой и сравнительно-правовой методы использованы для выявления преемственности между советскими формами отраслевого управления и современными моделями корпоративной интеграции.

**Результаты исследования:** установлено, что аффилированные акционерные общества в составе государственных корпораций и компаний сохраняют статус самостоятельных коммерческих юридических лиц, однако их деятельность может быть существенно обусловлена публичными целями и решениями, принимаемыми на уровне головной организации либо государства как акционера. Обосновано, что современное государственное управление экономикой реализуется преимущественно посредством корпоративного участия, формирования органов управления, государственного заказа, бюджетного финансирования и специальных режимов стратегических обществ, а не только через прямое административное подчинение.

Разграничены понятия акционерного общества с государственным участием и государственной корпорации как особой некоммерческой организации. Показано, что публичный интерес может возникать как вследствие государственной собственности, так и в связи с системообразующим значением частной организации. Установлено, что частноправовая форма становится организационным способом концентрации публичной собственности и выстраивания единой хозяйственной политики.

Сделан вывод о необходимости обеспечения баланса между управляемостью корпоративной группы, самостоятельностью ее участников, интересами акционеров и выполнением публично значимых задач.

DOI: 10.24412/1994-1404-2026-3-00-12

## Введение

В организации крупных хозяйственных систем, где юридически самостоятельные акционерные общества включены в единую производственную, финансовую и управленческую кооперацию наблюдается двойственность правового положения субъ-

ектов хозяйствования, существенно влияющая на их деятельность и имеющая принципиальное значение. Общество сохраняет статус коммерческой корпорации, действует через общее собрание акционеров, совет директоров и исполнительные органы, обладает

<sup>1</sup> **Запольский Сергей Васильевич**, доктор юридических наук, профессор, заслуженный юрист Российской Федерации, главный научный сотрудник Института государства и права Российской академии наук, г. Москва, Россия.  
E-mail: [zpmoscow@mail.ru](mailto:zpmoscow@mail.ru)



собственным имуществом и несет самостоятельную ответственность. Вместе с тем цели его существования, пределы допустимого хозяйственного риска, структура основных производственных связей и даже кадровые решения нередко определяются задачами, сформулированными вне самого общества. Тем самым частнопредпринимательская оболочка не устраняет публичного содержания деятельности, а становится одной из юридических форм его осуществления.

Подобная конструкция не возникла внезапно вместе с приватизацией и распространением акционерной формы. Советская и постсоветская история управления хозяйственными организациями показывает устойчивый поиск такой модели, которая позволяла бы соединить самостоятельность производителя с управляемостью крупных производственных комплексов. В послевоенный период менялась ведомственная принадлежность предприятий, они включались в союзные, союзно-республиканские и республиканские министерства, в 1958—1965 гг. в территориальные советы народного хозяйства, позднее — в производственные и научно-производственные объединения, хозрасчетные главки и иные отраслевые образования. При всем разнообразии реформ их инструментарий сводился преимущественно к трем направлениям: изменению объема прав предприятия, перестройке подчиненности и попыткам перевести управление экономикой на хозрасчетные основания.

Изменения конца XX века радикально изменили юридический язык хозяйственного управления. Децентрализация общественной собственности, приватизация и признание частной инициативы возвели акционерное общество в число основных организационно-правовых форм крупного производства. Но сама потребность в объединении предприятий, взаимной кооперации и выстраивании единой производственной стратегии никуда не исчезла. Напротив, в условиях сложных технологических цепочек она стала еще более заметной. Поэтому многие функции, ранее осуществлявшиеся отраслевыми органами управления, были воспроизведены уже в корпоративных формах — через владение пакетами акций, образование холдингов, концернов, интегрированных структур, формирование общих органов координации и закрепление обязательных для участников внутригрупповых решений.

В этом смысле опыт советского отраслевого управления представляет интерес не как модель, подлежащая восстановлению, а как материал для понимания природы современной корпоративной интеграции. Министерства промышленного профиля фактически объединяли множество производственных единиц в единую систему, а главные управления выполняли функции центров отраслевой координации. Попытка придать таким системам экономическую самостоятельность получила наиболее последовательное выра-

жение в реформе, провозглашенной Постановлением ЦК КПСС и Совета Министров СССР № 695 1979 года<sup>2</sup>, предусматривавшей перевод производственных министерств на хозрасчетные основы. Реформа не была реализована в полном объеме, однако закрепила саму идею крупного хозяйственного комплекса, в котором производственный капитал, инвестиционные и инновационные ресурсы концентрируются ради достижения общего результата. Н.И. Михайлов позднее справедливо связывал развитие корпоративных комплексов с жестким структурированием и интеграцией ресурсов в пределах определенного рыночного сектора<sup>3</sup>.

### **Правовое положение акционерных обществ в государственных корпоративных группах**

Современное акционерное общество принципиально отличается от административно подчиненного предприятия. Его корпоративная правосубъектность опирается на частнопредпринимательские категории собственности, участия, риска, дивиденда, сделки и ответственности. Акционерная форма позволяет аккумулировать капитал, отделять функцию собственности от текущего управления, привлекать профессиональных менеджеров, включать работников и контрагентов в систему имущественной заинтересованности. Именно эти свойства объясняют устойчивость акционерной формы в государственном секторе: государство получает возможность воздействовать на хозяйственную организацию не только посредством властного предписания, но и в качестве акционера, реализующего корпоративные права по правилам гражданского законодательства.

Такое сочетание хорошо видно на уровне органов управления. Для акционерных обществ с государственным участием типична трехзвенная система: общее собрание акционеров, совет директоров и единоличный исполнительный орган. Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах»<sup>4</sup> относит к совету директоров общее руководство деятельностью общества, оставляя за общим собранием вопросы его исключительной компетенции; статьи 64 и 65 Закона очерчивают содержание этого уровня управления, а статья 66 препятствует совмещению должности единоличного исполнительного органа с председательством в совете директоров. Формально перед нами классическая частнопредпринимательская конструкция разграничения корпоративных полномочий. Однако при государственном контроле персональный состав

<sup>2</sup> Постановление Центрального комитета КПСС и Совета Министров СССР от 12 июля 1979 года № 695 «Об улучшении планирования и усилении воздействия хозяйственного механизма на повышение эффективности производства и качества работы» // Бюллетень текущего законодательства СССР, июль 1979 г., № 7.

<sup>3</sup> Михайлов Н.И. Правовое моделирование корпоративных комплексов (интегрированных структур): монография. М.: ИГП РАН, 2016. 160 с. ISBN 978-5-8339-0168-7.

<sup>4</sup> Собрание законодательства Российской Федерации. 01.01.1996. № 1. Ст. 1.

совета, характер директив голосования и стратегические ориентиры общества способны придать этой конструкции отчетливо публичное измерение<sup>5</sup>.

Отсюда возникает один из центральных вопросов организации государственных корпоративных групп: где проходит граница между корпоративным контролем и административным руководством? Если управляющая компания владеет контрольным пакетом акций дочернего или зависимого общества, формирует его совет директоров и определяет ключевые хозяйственные решения, юридическая связь строится прежде всего на гражданско-правовом титуле участия. Но когда сама управляющая компания создана государством для реализации отраслевой политики, а содержание ее решений обусловлено актами Президента Российской Федерации, Правительства Российской Федерации, государственным заказом или режимом стратегического предприятия, частноправовой механизм фактически становится проводником публичной воли<sup>6</sup>. Такая ситуация не отменяет корпоративной самостоятельности, однако делает ее носителем и функционально ограниченной.

Особенно ясно эта закономерность проявляется в концернах и холдингах. Участники концерна сохраняют статус самостоятельных юридических лиц, но согласуют производственную, инвестиционную и финансовую политику, подчиняются общим технологическим и рыночным решениям, а в ряде случаев — единому центру корпоративного контроля. Экономическая польза подобной интеграции очевидна: перераспределение ресурсов внутри группы позволяет поддерживать предприятия в сложные периоды, внутригрупповые поставки обеспечивают устойчивость кооперации, результаты научно-исследовательских и опытно-конструкторских работ могут использоваться всей системой, а конфликты между участниками нередко разрешаются внутри группы без дорогостоящего судебного спора. Обратной стороной становятся рост управленческого аппарата, затяжные согласования и риск снижения конкуренции. Поэтому юридическая организация концерна неизбежно требует баланса: система должна быть управляемой, но не должна уничтожать хозяйственную инициативу входящих в нее обществ.

С этой точки зрения зависимость общества внутри корпоративной группы не может быть сведена только к конструкции основного и дочернего общества. Холдинговая связь шире: она может складываться из участия в капитале, договорных обязательств, единства управленческого состава, технологической зависимости, общего государственного задания и иных факторов. В результате происходит своеобразное «расщепление» компетенции. Формально решение принимается органом конкретного общества, но материально оно может

быть подготовлено или предопределено на уровне головной компании либо публичного субъекта, контролирующего всю систему [1]. Чем значительнее решение для судьбы общества — изменение производственного профиля, инвестиционная программа, участие в государственном оборонном заказе, распоряжение крупным активом, — тем заметнее внешнее влияние. Локальные же вопросы внутренней организации сохраняют существенно больший объем корпоративной автономии.

Именно поэтому необходимо различать акционерные общества, имеющие в фирменном наименовании слово «корпорация», и государственные корпорации как особый вид некоммерческой организации. В соответствии с Федеральным законом от 12.01.1996 г. № 7-ФЗ «О некоммерческих организациях»<sup>7</sup> государственная корпорация учреждается Российской Федерацией на основе имущественного взноса для осуществления социальных, управленческих или иных общественно полезных функций и создается специальным федеральным законом. Переданное ей имущество принадлежит самой государственной корпорации; по общему правилу она не отвечает по обязательствам Российской Федерации, а Российская Федерация — по ее обязательствам. Акционерное же общество, даже если оно именуется «корпорацией» и все его акции находятся в федеральной собственности, остается коммерческой корпоративной организацией и действует прежде всего в режиме Федерального Закона от 26.12.1995 № 208-ФЗ «Об акционерных обществах».

Формальное различие, однако, не устраняет функционального сходства. Крупная государственная головная компания, объединяющая акционерные общества одной отрасли, нередко осуществляет координацию, которая по экономическому содержанию напоминает отдельные функции прежнего отраслевого министерства. Здесь и обнаруживается особенность российской модели: публичная власть не обязательно управляет предприятием непосредственно. Она способна построить многоуровневую корпоративную цепь, где государство владеет головной компанией, головная компания контролирует пакеты акций входящих обществ, а уже их органы управления принимают юридически самостоятельные решения<sup>8</sup>. Власть как бы переводится с языка административного распоряжения на язык корпоративного участия, не теряя при этом стратегической направленности.

### **Взаимодействие публично-правовых и частноправовых механизмов в деятельности государственных и системообразующих корпораций в стратегических отраслях**

Наиболее плотное переплетение двух правовых начал наблюдается в оборонно-промышленном ком-

<sup>5</sup> Шиткина И.С. Основные направления развития корпоративно-законодательства и тенденции правоприменительной практики // Предпринимательское право. Приложение «Право и Бизнес». 2018. № 2.

<sup>6</sup> Дурдыева Д.А., Дзукаева А.Л. Проблемы и особенности управления акционерными обществами как фактор обеспечения конкурентоспособности корпораций // Вестник экспертного совета. 2017. № 2 (9).

<sup>7</sup> Собрание законодательства Российской Федерации. 15.01.1996. № 3. Ст. 145.

<sup>8</sup> Винницкий А.В. Государственная собственность в административном праве. М.: Статут, 2010. 429 с.

плексе. Статья 71 Конституции Российской Федерации<sup>9</sup> относит вопросы обороны, безопасности и оборонного производства к ведению Российской Федерации. Уже поэтому хозяйственная деятельность организаций ОПК не может строиться исключительно как свободное осуществление частной инициативы. Начиная с приватизационных процессов 1990-х годов законодатель последовательно выделял оборонные и иные стратегические предприятия в особую категорию. Государственному комитету Российской Федерации по управлению государственным имуществом предписывалось учитывать специальные режимы приватизации, а Постановлением Правительства Российской Федерации от 17.07.1998 № 784<sup>10</sup> закреплялся перечень акционерных обществ, производивших продукцию стратегического значения для национальной безопасности, федеральные пакеты акций которых не подлежали досрочной продаже.

Эта линия была продолжена Указом Президента Российской Федерации от 04.08.2004 № 1009 «Об утверждении Перечня стратегических предприятий и стратегических акционерных обществ»<sup>11</sup>. Включение соответствующих активов в прогнозный план приватизации связывалось с предварительным решением Президента Российской Федерации об исключении предприятия из числа стратегических либо об уменьшении участия Российской Федерации в управлении стратегическим акционерным обществом. Для федеральных государственных унитарных предприятий, включенных в перечень, предусматривалось преобразование в акционерные общества, 100% акций которых находятся в федеральной собственности. Тем самым акционерная форма была использована не для ухода государства из экономики, а, напротив, для соединения рыночной формы хозяйствования с сохранением публичного контроля над стратегическим производством.

Конституционно-правовое обоснование такой модели состоит в том, что свобода экономической деятельности не существует изолированно от публичных интересов. В практике Конституционного Суда Российской Федерации подчеркивалось, что защита экономического суверенитета, обороны страны и безопасности государства позволяет федеральному законодателю устанавливать специальные условия осуществления и ограничения экономических прав. По той же логике Федеральный закон от 29.04.2008 № 57-ФЗ «О поряд-

ке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства»<sup>12</sup> установил особый порядок иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства. Закон ограничивает возможность бесконтрольного приобретения такого влияния, которое позволило бы иностранному инвестору определять деятельность стратегического общества, в том числе через формирование органов управления.

При поверхностном взгляде подобные ограничения могут показаться внешними по отношению к корпоративному праву. На деле они меняют само содержание корпоративной автономии. Владение акциями стратегического общества, возможность голосовать ими, определять состав органов управления и совершать сделки с соответствующими пакетами перестают быть исключительно частным делом собственника. Публичный интерес входит внутрь корпоративной конструкции и задает условия осуществления субъективного права [2]. Это не превращает акционерное общество в орган государственной власти, но свидетельствует о том, что режим корпоративного имущества и управления способен быть одновременно частноправовым по форме и публично обусловленным по целям и пределам [3].

Еще более наглядно это видно в отношениях государственного оборонного заказа. Значительная часть деятельности акционерных обществ ОПК, для которых выполнение ГОЗ составляет основной производственный профиль, регулируется Федеральным законом от 29.12.2012 № 275-ФЗ «О государственном оборонном заказе»<sup>13</sup> [4]. Закон формирует специальную кооперацию: в нее входят головной исполнитель, заключивший государственный контракт с государственным заказчиком, исполнители, заключившие контракты с головным исполнителем, а также последующие исполнители. Головной исполнитель определяет состав кооперации, обосновывает с ее участниками цену продукции, согласует сроки и условия финансирования и поставок. В установленных законом случаях отказ или уклонение от заключения контракта не допускается. Частноправовой договор здесь сохраняется, но свобода его заключения и содержания существенно модифицирована публичной задачей обеспечения обороны.

Было бы, однако, неточно описывать эту систему как простое административное подчинение предприятия государственному заказчику. Внутри холдинга решения по-прежнему принимаются органами юридических лиц; в советах директоров представлены руководители вышестоящих обществ, представители государственных структур и специалисты иных органи-

<sup>9</sup> Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (с изм. и доп.) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 04.07.2020.

<sup>10</sup> Постановление Правительства Российской Федерации от 17.07.1998 № 784 «О перечне акционерных обществ, производящих продукцию (товары, услуги), имеющую стратегическое значение для обеспечения национальной безопасности государства, закреплённые в федеральной собственности акции которых не подлежат досрочной продаже» // Собрание законодательства Российской Федерации. 27.07.1998, № 30, ст. 3778.

<sup>11</sup> Собрание законодательства Российской Федерации. 09.08.2004, № 32, ст. 3313.

<sup>12</sup> Собрание законодательства Российской Федерации. 05.05.2008. № 18. Ст. 1940.

<sup>13</sup> Собрание законодательства Российской Федерации. 31.12.2012. № 53 (ч. 1). Ст. 7600.

заций с государственным участием. Сама зависимость распределена между несколькими юридическими механизмами: правом собственности на акции, корпоративными процедурами, специальными требованиями закона о государственном оборонном заказе, бюджетным финансированием и отраслевой координацией. В результате возникает не классическая вертикаль «орган власти — подчиненное предприятие», а сложная система взаимосвязанных полномочий, в которой публичное управление осуществляется через корпоративные и договорные формы.

Показательно и содержание постановления Правительства Российской Федерации от 03.11.2014 № 1151 «Об утверждении Положения о коллегии Военно-промышленной комиссии Российской Федерации»<sup>14</sup>, которым утверждено Положение о коллегии Военно-промышленной комиссии Российской Федерации. К числу рассматриваемых ею вопросов отнесена кадровая политика в отношении руководителей организаций ОПК, включая кандидатуры для избрания в исполнительные органы и представителей Российской Федерации в советы директоров и ревизионные комиссии акционерных обществ, включенных в соответствующие перечни. Такая компетенция показывает, что кадровое решение, которое в обычном обществе выглядело бы исключительно результатом корпоративного волеизъявления акционеров, в стратегическом секторе включается в механизм публичного управления.

Сходная логика действует за пределами оборонной промышленности применительно к системообразующим организациям. Постановлением Правительства Российской Федерации от 10.05.2020 № 651 «О мерах поддержки системообразующих организаций»<sup>15</sup> был предусмотрен специальный механизм поддержки системообразующих организаций. Критерии и порядок включения организаций в перечень системообразующих организаций российской экономики, одобренные Правительственной комиссией по повышению устойчивости развития российской экономики в условиях санкций 22.04.2022, предполагают учет аффилированности в рамках групповой, в том числе холдинговой, структуры. Среди обстоятельств, имеющих значение, названы градообразующая роль, участие в кооперации по государственному оборонному заказу, эксплуатация критической инфраструктуры, разработка критических технологий, обеспечение информационной безопасности и транспортной доступности удаленных территорий.

Системообразующий статус особенно интересен тем, что публичная значимость возникает не только из государственной собственности. Частное по составу капитала общество также может стать объектом специальных мер поддержки и повышенного внимания

государства, если его устойчивость имеет значение для отрасли, региона, инфраструктуры или занятости. В такой ситуации публично-правовое влияние основано не на титуле собственника, а на общеэкономической функции корпорации. Государство вправе связывать предоставляемую поддержку с определенными ожиданиями относительно сохранения производства, занятости и выполнения государственных программ [5]. Тем самым публичный интерес способен возникнуть не после национализации предприятия, а непосредственно из масштаба и характера его экономической деятельности.

Вместе с тем государственное участие в капитале усиливает эту связь. Приказ Росимущества от 29.12.2014 № 524<sup>16</sup>, утвердивший Методические рекомендации по разработке дивидендной политики в акционерных обществах с государственным участием, демонстрирует, что даже такое классическое корпоративное решение, как распределение прибыли, включается в контекст реализации имущественной политики государства. Для частного акционера дивиденд прежде всего является формой дохода от капитала. Для государства как акционера он одновременно становится бюджетным ресурсом и элементом управления государственными активами. Следовательно, одно и то же корпоративное право в зависимости от личности акционера и целей его участия способно выполнять как частную, так и публичную функцию.

Характерен пример создания Акционерного общества «Корпорация морского приборостроения» Указом Президента Российской Федерации от 01.04.2020 № 235<sup>17</sup>. Было установлено, что 100% его акций находятся в федеральной собственности; в уставный капитал вносились принадлежащие Российской Федерации акции других акционерных обществ, а также денежные средства в размере 200 млн рублей. Юридическая техника такого решения показательна: отраслевой центр создается не как новый орган исполнительной власти, а как коммерческая корпорация, капитал которой формируется путем объединения государственных корпоративных активов. Частно-правовая форма становится организационным способом концентрации публичной собственности и выстраивания единой хозяйственной политики [6].

Для анализа внутренних отношений таких групп полезна и категория взаимозависимости, закрепленная ст. 105.1 Налогового кодекса Российской Федерации<sup>18</sup>. Лица признаются взаимозависимыми, когда особенности отношений между ними способны влиять

<sup>14</sup> Собрание законодательства Российской Федерации. 17.11.2014. № 46. Ст. 6352.

<sup>15</sup> Собрание законодательства Российской Федерации. 18.05.2020. № 20. Ст. 3175.

<sup>16</sup> Приказ Росимущества от 29.12.2014 № 524 «Об утверждении Методических рекомендаций по разработке дивидендной политики в акционерных обществах с государственным участием» // Информационно-правовой портал «Гарант».

<sup>17</sup> Указ Президента Российской Федерации от 01.04.2020 № 235 «О создании акционерного общества „Корпорация морского приборостроения“» // Собрание законодательства Российской Федерации. 06.04.2020. № 14. Ст. 2079.

<sup>18</sup> Собрание законодательства Российской Федерации. 03.08.1998. № 31. Ст. 3824.



на условия или результаты совершаемых сделок либо на экономические результаты деятельности; учитывается участие в капитале, соглашения и иная возможность определять решения других лиц. Хотя эта конструкция предназначена прежде всего для целей налогообложения, она точно передает важную характеристику интегрированных корпоративных систем: юридическая самостоятельность участников не означает экономической и управленческой изолированности [7]. Именно возможность одного центра влиять на решения нескольких обществ создает хозяйственную систему как единое фактическое образование.

В российской экономике поэтому нельзя удовлетворительно описать государственные корпоративные группы только языком гражданского либо административного права [8]. Частное право объясняет принадлежность акций, компетенцию органов, сделки, ответственность, распределение прибыли и имущественную самостоятельность. Публичное право определяет стратегические цели, специальные режимы допуска к капиталу, государственный заказ, бюджетное финансирование, кадровые ограничения, контроль и иные требования, обусловленные обороной, безопасностью и устойчивостью экономики. Между этими массивами не существует жесткой границы: они соединяются в конкретном корпоративном решении, которое одновременно должно отвечать интересам общества как самостоятельного юридического лица и целям хозяйственной системы, частью которой оно является.

Сравнение с зарубежными концернами лишь подчеркивает универсальность самой хозяйственной логики интеграции. Нередко в качестве примера приводится Volkswagen, в структуре которого наряду с автомобильным производством представлены организации электронной, судостроительной, финансовой и иных отраслей. Для целей настоящей статьи важен не конкретный состав группы, а юридический смысл такого объединения: один корпоративный центр способен соединять разнородные по профилю общества, если между ними существует общий экономический интерес. В частном концерне этот интерес обычно формируется собственником капитала и рыночной стратегией. В государственном — к нему добавляется публичное целеполагание, и потому тот же механизм корпоративной зависимости начинает одновременно обслуживать промышленную политику, безопасность, научно-техническое развитие или исполнение государственного заказа.

Особое значение при этом имеет вопрос юридической ответственности за решения, принимаемые в интересах всей группы. Корпоративная практика знает ситуации, когда экономически рациональное для холдинга решение оказывается неблагоприятным для отдельного общества, его кредиторов либо миноритарных участников. В государственной системе противоречие способно быть еще сложнее: общество может понести расходы не ради увеличения собственной прибыли, а ради исполнения стратегической задачи,

поддержания кооперации или сохранения производства, необходимого для государства. Простая ссылка на контрольный пакет акций здесь недостаточна. Если публичная цель фактически предопределяет хозяйственное решение, право должно давать ответ, кто несет экономические последствия такого выбора и каким образом защищается самостоятельный имущественный интерес юридического лица.

Отсюда становится понятной и потребность в систематизации нормативного материала, регулирующего отношения государства с аффилированными хозяйственными обществами. Сегодня соответствующие правила рассеяны по гражданскому, корпоративному, финансовому, бюджетному, административному и специальному отраслевому законодательству. В результате один и тот же управленческий процесс описывается различными правовыми режимами, которые не всегда согласованы между собой. Для крупных государственных хозяйственных систем вопрос уже состоит не столько в увеличении количества обязательных предписаний, сколько в установлении последовательной модели: публичная власть формулирует стратегическое задание и специальные ограничения, собственник реализует корпоративные права, головная компания координирует участников, а само общество сохраняет установленную законом компетенцию и ответственность<sup>19</sup>. Такая системность позволила бы отказаться и от фикции полной независимости, и от не менее опасной фикции административной подчиненности.

Из этого следует и более общий вывод о природе корпоративной автономии в государственном секторе. Она не может пониматься как свобода от государства, поскольку само государство нередко является единственным либо контролирующим акционером и учреждает соответствующую систему для решения публично значимых задач. Но столь же ошибочно сводить управление к административному подчинению. Корпоративная форма сохраняет самостоятельную ценность именно потому, что ограничивает прямую властную команду процедурами, компетенцией органов, имущественной ответственностью и требованиями добросовестности. Государственный интерес должен быть переведен в юридически определенную корпоративную волю, а не заменять ее.

## **Заключение**

В этом и состоит практический смысл разграничения публичного и частного. Публичное начало задает цель, пределы и обязательные условия деятельности там, где затронуты оборона, безопасность, критическая инфраструктура, системная устойчивость или государственная собственность. Частноправовое начало обеспечивает хозяйственную инициативу, имуществен-

<sup>19</sup> Малько А.В. Правовые акты как средства российской правовой политики в условиях глобализации и регионализации : монография / А.В. Малько, Я.В. Гайворонская. М. : Юстиция, 2018. 120 с.

ную обособленность, ответственность за результат, договорную кооперацию и внутреннюю корпоративную процедуру. При нарушении равновесия система либо теряет управляемость и способность решать стратегические задачи, либо превращается в квазиминистерство, где акционерная форма становится внешней декорацией административного распоряжения.

Поэтому дальнейшее развитие законодательства о государственных и системообразующих корпоративных структурах целесообразно связывать не с возвратом к прямой ведомственной подчиненности, а с более точным закреплением правовых каналов влияния [9]. Нуждаются в ясном разграничении полномочия государства как носителя публичной власти и как акционера, компетенция головной компании и органов зависимых обществ, пределы обязательности внутригрупповых решений, ответственность за причинение ущерба обществу при исполнении внешне заданной стратегии. Чем прозрачнее будет этот механизм, тем меньше оснований смешивать корпоративное управление с ад-

министративной командой и тем надежнее частнопредпринимательская форма сможет обслуживать публичные задачи российской экономики.

Исторический опыт и современная практика в конечном счете подтверждают совместимость рыночной организации хозяйствования с активным государственным участием. Проблема состоит не в самом присутствии государства, а в юридическом качестве такого присутствия. Там, где стратегическая цель проводится посредством понятных корпоративных полномочий, специальных законов, договорных механизмов и ответственности принимающих решения лиц, государственное влияние способно усиливать устойчивость хозяйственной системы, не уничтожая автономию ее участников [10]. Именно такая модель — сочетание публичного целеполагания с частнопредпринимательской организацией исполнения — представляется наиболее адекватной для крупных корпоративных хозяйствующих субъектов, действующих в ключевых секторах российской экономики.

## Литература

1. Запольский С.В. Правовое администрирование экономики : монография. М. : Директ-Медиа, 2026. 236 с.
2. Щукина Т.В. Трансформация системы публичного управления в Российской Федерации: новые стратегии и направления интеграции : монография. Воронеж : Научная книга, 2019. 242 с.
3. Россинский Б.В. Государственные корпорации как субъекты публичного управления // Вестник Нижегородского университета им. Н.И. Лобачевского. 2024. № 2. С. 153—160. С. 158.
4. Свинных Е.А., Кудашкин А.В. Оборонно-промышленный комплекс: понятие, структура, правовые основы деятельности // Право в Вооруженных Силах — Военно-правовое обозрение. 2020. № 11 (280). С. 37—48.
5. Административно-правовые средства обеспечения устойчивого экономического развития Российской Федерации : монография / Под общ. ред. В.Н. Плигина. М. : Рускайнс, 2025. 304 с.
6. Запольский С.В. Государственная корпорация как институт публично-частного управления: российская модель // Правовая информатика. 2026. № 1. С. 187—195. DOI: 10.24412/1994-1404-2026-1-00-21.
7. Кикавец В.В., Цареградская Ю.К. Финансовый контроль публичных закупок в Российской Федерации : монография / Под ред. В.В. Кикавца. М. : Проспект, 2022. 208 с.
8. Санжаревский И.И. Политика государственно-частного партнерства и институализация корпоративных отношений в государственном управлении современной России // Известия Саратовского университета. Новая серия. Серия: Социология. Политология. 2026. Т. 26. № 1. С. 68—78.
9. Россинский Б.В. Проблемы государственного управления с позиций теории систем : монография / МГЮА им. О.Е. Кутафина. М. : Норма : ИНФРА-М, 2021. 264 с.
10. Административно-правовые отношения в отраслях экономики : монография / Под общ. ред. М.Н. Кобзарь-Фроловой; ИГП РАН. Воронеж : Научная книга, 2023. 386 с.

SECTION:  
CONSTITUTIONAL LAW

# ON THE LEGAL BASIS FOR THE ACTIVITIES OF AFFILIATED JOINT-STOCK COMPANIES AS PART OF STATE CORPORATIONS AND COMPANIES

Zapolsky S.V.<sup>20</sup>

<sup>20</sup> *Sergey V. Zapolsky, Dr.Sc. (Law), Professor, Principal Researcher at the Sector of Administrative Law and Administrative Procedure of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia.*  
E-mail: [zpmoscow@mail.ru](mailto:zpmoscow@mail.ru)

**Keywords:** joint-stock company, state participation, corporate governance, public interest, private law, public law, holding company, concern, affiliation, state defense order, systemically important organization, strategic company.

#### **Abstract**

**Purpose of work:** to identify the specific features of the legal status of affiliated joint-stock companies forming part of state corporations, holding companies, and other integrated business structures. Particular attention is paid to the relationship between the corporate autonomy of such companies and the public objectives pursued by the state in strategic industries, the defense-industrial sector, and the system for supporting systemically important organizations.

**Research methods:** formal-legal, systemic, historical-legal, and comparative-legal methods. The formal-legal method was used to analyze legislative provisions governing corporate governance, state participation, the activities of strategic companies, and the performance of state defense orders. The systemic method was applied to examine the interrelationship between corporate, administrative, contractual, and financial mechanisms of state influence. The historical-legal and comparative-legal methods were used to identify continuity between Soviet forms of sectoral administration and contemporary models of corporate integration.

**Results of the study:** It has been established that affiliated joint-stock companies within state corporations and companies retain the status of independent commercial legal entities; however, their activities may be substantially conditioned by public objectives and decisions made at the level of the parent organization or the state as a shareholder. It has been substantiated that modern state administration of the economy is carried out primarily through corporate participation, the formation of governing bodies, state orders, budget financing, and special regimes for strategic companies, rather than solely through direct administrative subordination.

The concepts of a joint-stock company with state participation and a state corporation as a special non-profit organization have been distinguished. It has been shown that the public interest may arise both as a result of state ownership and in connection with the systemic importance of a private organization. It has been established that the private-law form serves as an organizational means of concentrating public property and developing a unified economic policy.

A conclusion has been drawn regarding the need to ensure a balance between the manageability of the corporate group, the independence of its participants, the interests of shareholders, and the performance of tasks of public importance.

#### **References**

1. Zapol'skii S.V. Pravovoe administrirovanie ekonomiki : monografiia. M. : Direkt-Media, 2026. 236 s.
2. Shchukina T.V. Transformatsiia sistemy publichnogo upravleniia v Rossiiskoi Federatsii: novye strategii i napravleniia integratsii : monografiia. Voronezh : Nauchnaia kniga, 2019. 242 s.
3. Rossinskii B.V. Gosudarstvennye korporatsii kak sub"ekty publichnogo upravleniia // Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo. 2024. No. 2. S. 153–160. S. 158.
4. Svininykh E.A., Kudashkin A.V. Oboronno-promyshlennyi kompleks: poniatie, struktura, pravovye osnovy deiatel'nosti // Pravo v Vooruzhennykh Silakh — Voenno-pravovoe obozrenie. 2020. No. 11 (280). S. 37—48.
5. Administrativno-pravovye sredstva obespecheniia ustoychivogo ekonomicheskogo razvitiia Rossiiskoi Federatsii : monografiia / Pod obshch. red. V.N. Pligina. M. : Rusains, 2025. 304 s.
6. Zapol'skii S.V. Gosudarstvennaia korporatsiia kak institut publichno-chastnogo upravleniia: rossiiskaia model' // Pravovaia informatika. 2026. No. 1. S. 187—195. DOI: 10.24412/1994-1404-2026-1-00-21.
7. Kikavets V.V., Tsaregradskaia Iu.K. Finansovyi kontrol' publichnykh zakupok v Rossiiskoi Federatsii : monografiia / Pod red. V.V. Kikavtsa. M. : Prospekt, 2022. 208 s.
8. Sanzharevskii I.I. Politika gosudarstvenno-chastnogo partnerstva i institualizatsiia korporativnykh otnoshenii v gosudarstvennom upravlenii sovremennoi Rossii // Izvestiia Saratovskogo universiteta. Novaia seriia. Seriia: Sotsiologiya. Politologiya. 2026. T. 26. No. 1. S. 68—78.
9. Rossinskii B.V. Problemy gosudarstvennogo upravleniia s pozitsii teorii sistem : monografiia / MGlUa im. O.E. Kutafina. M. : Norma : INFRA-M, 2021. 264 s.
10. Administrativno-pravovye otnosheniia v otraslakh ekonomiki : monografiia / Pod obshch. red. M.N. Kobzar'-Frolovoi; IGP RAN. Voronezh : Nauchnaia kniga, 2023. 386 s.



# КИБЕРНЕТИЧЕСКИЙ ПОДХОД К ПОНИМАНИЮ ГОСУДАРСТВА (СПЕЦИАЛЬНАЯ ТЕОРИЯ СИНЕРГЕТИКИ)

Зырянов А.В.<sup>1</sup>

**Ключевые слова:** теория государства, государственное управление, кибернетика, системогенез, гомеостаз, информалогия, математическое моделирование, программирование.

## Аннотация

**Цель работы** — исследовать влияние кибернетического подхода на понимание структуры и процессов функционирования государства, его эволюции, а также определить возможности его применения для повышения эффективности управления и развития государственных институтов — способствовать научно-методологическому обеспечению стратегического планирования в Российской Федерации.

**Методы.** Использование междисциплинарных методов (из области социальной философии, политологии, государственного управления, социологии, теории систем, синергетики, информатики, математики и др.), способных учитывать динамику и обратные связи внутри системы и межсистемные взаимодействия, призвано объективизировать представление о рассматриваемой проблеме. Заявленный подход позволяет моделировать государственные процессы как самоорганизационно-адаптивные информационные системы, выявлять их устойчивость, уязвимость и потенциал для развития.

**Результаты.** В результате исследования был решен ряд теоретико-практических задач, а именно: раскрыто понятие гомеостазиса государства; исследована проблема государственного системогенеза; проведен информалогический анализ государственного управления; представлены алгоритмы математического моделирования и программирования государственного и межгосударственного развития. Изложенные алгоритмы информационно-математического моделирования, как основы компьютерных симуляций для прогнозирования развития страны, здесь, были представлены на концептуальном, статическом и динамическом уровнях.

DOI: 10.24412/1994-1404-2026-3-120-130

## Введение

В работе «Синергетическая концепция государствопонимания»<sup>2</sup> кибернетика (от др.-греч. κυβερνήτικη — «искусство управления») указывается и анализируется в качестве предтечи синергетической парадигмы рациональности, она закладывает концептуальные основы самоорганизационных процессов общественного развития, однако делает это в контексте «специальной» теории, посвященной исследованию упорядоченных, гомеостатических, предзаданных, временных системных объектов, тогда, как синергетика раскрывает «общую» модель социо-политической реальности дополняя её стохастическими, хаотическими, нелинейными, бифуркационными, коэволюционными, незамкнутыми, необратимыми процессами и явлениями.

Снимая противоречия обозначенных концептуальных положений, усматривая естественность развития становящегося в ставшем<sup>3</sup>, для лучшего понимания настоящего и предвидения будущего, постараемся исследовать государство, по выражению Г. Кельзена, в его «широком смысле, как некую форму всего общества»<sup>4</sup>, включающую кибернетические процессы системной самоорганизации и управления, где государство представлено в виде сложной информационно-коммуникативной системы, функционирующей на основе обмена данными, обратных связей и автоматизированных процессов.

<sup>2</sup> Зырянов А.В. Синергетическая концепция государствопонимания : монография. М. : Юрлитинформ, 2019. 318 с.

<sup>1</sup> **Зырянов Алексей Викторович**, доктор юридических наук, доцент, профессор кафедры общетеоретических правовых дисциплин, Российский государственный университет правосудия, Уральский филиал, Россия, г. Челябинск, Россия. ORCID: 0000-0002-6364-1812.

E-mail: zav-nauka@mail.ru

<sup>3</sup> Грачев М.Н. Кибернетический подход и система философских взглядов Норберта Винера : автореф. дис. ... канд. филос. наук. М. : Российская академия управления, 1994. 24 с.

<sup>4</sup> Кельзен Г. Чистое учение о праве. СПб. : Алеф-Пресс, 2015. 540 с.



### **Гомеостазис государства**

Общая теория систем [1, 2], тектология [3, 4], кибернетика [5, 6] и синергетика [7, 8] формируют мировоззренческую установку и понятийно-категориальный аппарат, позволяющий, при исследовании общества и государства, оперировать универсальными закономерностями становления и развития сложных уровней материи, воспринимать социальные объекты в качестве компонентов «энергоинформационного поля Земли и макрокосмоса»<sup>5</sup>.

Так, государствообразная форма организации общества является негэнтропийным явлением — процессом, эволюционным признаком, позволяющем человечеству обеспечивать тенденцию к росту организованности путем отдачи информации (прямых (управляющих) сигналов) в окружающую среду, продуцируя сложные структуры и устойчивые политико-правовые режимы (от лат. *regimen* — правление).

Информация — ключевое понятие теории управления (кибернетики) — результат взаимодействия динамической системы со средой, приводящий к изменению системы сообразно отражаемого воздействия (обратных сигналов). Указанная адаптационная изменчивость позволяет системе существовать относительно равновесно — гомеостатично, в рамках параметров жизнеспособности.

Границы общественно-государственного гомеостаза определяются «квантовой запутанностью» группы лиц, где поступающая информация является актуальной для всего сообщества если актуальна хотя бы для одного её члена. Информационная связность определяет качество представления об объективной реальности. Здесь, человек понимается, действительно, в качестве системного элемента — функции, но не как атомизированного субъекта. (Внесистемная же автономизация субъективной воли, консолидируясь с себе подобными, создаёт альтернативный, деструктивный относительно первичной системы, информационный контур).

Соответствующая групповая самоопределённость (возможно и межгрупповая, трансгрупповая) детерминирует функцию согласованности организационных решений, что порождает внутреннюю иерархическую подсистему, фиксирующую информацию об «опыте»<sup>6</sup> и регулирующую поведение в окружающей среде, т. е. систему публичного властвования, государственного управления.

Собственно, государство можно представить в виде сетевой информационной модели системы выживания и развития общества, оно материализуется в человеке, как в «носителе программной информации» [9]. Государственные институты выступают в роли транслято-

ров программных команд (в т. ч. «вирусных» и «анти-вирусных»).

Так, под гомеостазисом государства понимается способность сохранять динамическое равновесие посредством преодоления положительных обратных связей, обеспечивая его системную устойчивость. «Устойчивость — проявление внутренней, сообразной целям и задачам, структуры; способность системы выполнять свойственные ей функции»<sup>7</sup>. Системная устойчивость государства обретает социальную ценность, обеспечивая поступательное общественное развитие. Именно устойчивость является критерием естественного отбора режимных состояний государств(а), его форм.

Временное постоянство структуры объекта — его системная память, обуславливается практикой адаптационного поведения. «Процессы застывают, кристаллизуются в структурах»<sup>8</sup>. Структурная («потенциальная») информация характеризует качество достигнутой организованности государственной системы и выступает проводником «кинетической» информации<sup>9</sup> — условием общественного развития.

Вместе с тем, каждый индивид одновременно является, как частицей материи общественных отношений, так и волновым источником информационного поля (источником импульса, энтропии и флуктуации). Так, в процессе развития государственности присутствует феномен спонтанной самоорганизации, который связан с базовым принципом системогенеза, где качество микросостояний определяет вероятность качества макросостояния (влияние положительных обратных связей). Однако число случайных вариаций развития ограничено спектром возможных информационных связей (коммуникаций) элементов системы и среды.

### **Системогенез государства**

Рассматривая государство с позиций информационно-кибернетического моделирования процесса развития самоуправляющейся иерархо-сетевой системы [10], мы имеем дело с исследованием социального феномена, сущностно теснейшим образом связанного с его системным генезисом.

Государствогенез в данном случае представляется в виде универсального, во времени и пространстве, процесса, протекающего в форме взаимодействия нескольких разноуровневых информационно-коммуникативных контуров социально-политической системы, а именно: консолидации, дифференциации, иерархизации, систематизации, структуризации и формализации.

<sup>7</sup> Горелова Г.В. Когнитивный анализ и моделирование устойчивого развития социально-экономических систем. Ростов н/Д : Изд-во Рост. ун-та, 2005. 288 с.

<sup>8</sup> Лисин А.И. Идеальность. Часть 1. Реальность идеальности. М. : Информациология, 1999. 832 с.

<sup>9</sup> Сяский Д.Ю. Отдельные аспекты управления в социальных системах: кибернетический подход // Экономика и управление: проблемы, решения. 2017. № 1 (5). С. 79—86.

<sup>5</sup> Грачев Н.И. Функции государства как социально-политического организма // Вестник СГЮА. 2017. № 1 (114). С. 16—27.

<sup>6</sup> Винер Н. Кибернетика и общество. М. : Изд-во иностр. лит., 1958. 142 с.

Раскрываемые ниже уровни-контуры можно описать в виде соответствующих этапов государствогенеза, однако важно понимать факт их цикличности, перманентной и одновременной динамики, коэволюционного взаимовлияния и внутренней флуктуации.

1. Консолидация. Человек — существо способное символически отражать реальность — хранить и передавать информацию. На основании практики взаимодействия людей относительно актуальных потребностей (безопасность, пропитание, размножение, развлечение, познание, обмен и т. д.) определяется, изначально, ситуативно и бессознательно, коммуникационная сфера взаимодополнительного существования. Различие потребностей, их приоритета, обособляет коммуникационные мета-группы.

2. Дифференциация. Волевое отношение индивидов к сфере потребностей и интересов, осознанность взаимодействия, ролевое самоопределение порождает общество, как особое организационное качество социальной материи. Образуется общесемиотическая информационная целостность — понимание каждым членом общества себя в качестве части коллективного образования и его функционального компонента. Воля является фактором власти, а власть фактором — системы.

3. Иерархизация. На основе опыта и рефлексии сознания происходит самоопределение элемента, обладающего максимальными способностями по сбору, хранению, обработке ключевой, обеспечивающей жизнеспособность сообщества, информации и принятию эффективных решений (охрана или захват территорий или торговля, или охота, или земледелие...). Данный элемент становится точкой коммуникативного центростремительного притяжения — началом политической организованности («владеющий информацией — владеет миром»). Здесь подчёркивается информационная обусловленность властеотношений, где центральный элемент, обладая большей информацией, уравнивается пропорциональной массой менее инфоёмких элементов.

4. Систематизация. Публичная определенность, легитимация властного центра обеспечивает организационную устойчивость общества. Устанавливается собственный системный контур прямых (распорядительных) и обратных (исполнительных) информационных связей.

5. Структуризация. Сообразно целям и задачам общественного развития, сферам общественных отношений формируется внутренняя структура, состоящая из информационно взаимосвязанных специальных функционально-управленческих точек социального пространства, замещаемых, периодически, возможным образом, людьми. (Отдельная личность, замещающая иерархическую точку социо-политического пространства может усиливать или ослаблять её функционал («роль личности в истории»)). Структуризация соотно-

сится, в первую очередь, с базовыми функциями системы: обеспечение взаимодействия с внешней средой (совещательные, представительные, судебные органы публичной власти); обеспечение взаимодействия между внутренними элементами (исполнительные, административные органы публичной власти); функция катализатора — обеспечение взаимодействия между структурами первой и второй функций — функция ядра системы (главствующий орган публичной власти). Структурные образования политической организации постепенно институционализируются.

6. Формализация. В зависимости от внешних и внутренних условий (военное противостояние или нейтралитет, классовая борьба или компромисс, кризис или благоденствие) вырабатывается оптимальное качество (сложность, скорость, интенсивность) информационных сигналов, прямых или обратных связей, что определяет режимную форму существования системы: централизованную, децентрализованную, смешанную. Эффективная форма системы публичного властвования информационно воспроизводя самоподобие обретает качество гомеостаза, фиксируется, как образец политико-организационной культуры общества (данные образцы (абсолютизм, дуализм, парламентаризм, министриализм, партократия и т. д.), составляя историческое наследие, могут периодически актуализироваться, «вспоминаться», как способы эффективного управления).

Важно отметить, что развитие системы государственной организации общества происходит в рамках тенденций: достижения, сохранения и утраты устойчивости. Устойчивость соотносится с эффективностью государственного аппарата — структурно-функциональных компонентов, обеспечивающих сбор, обработку и трансляцию управленческой информации (сигнала) с максимальным радиусом распространения.

Утрата адекватной управленческой реакции связана с самозамыканием, функциональной деградацией органов власти, что продуцирует формирование внесистемных автономизирующихся структур, стремящихся к занятию центра политического притяжения. Как следствие, актуализируются процессы по формированию нового информационно-коммуникативного контура власти, системная трансформация государственности.

На межгосударственном уровне проявляются процессы межсистемного (метасистемного) взаимодействия: взаимодополнительности; взаимоисключительности. Сходные по структурному потенциалу системы формируют межсистемные взаимоусиливающие связи. Конкурирующие социально-политические системы воздействуют друг на друга, разрушая системные связи, привнося инвазивные элементы, включая компоненты общественных отношений в собственную системную сферу влияния.

## **Информалогия государственного управления**

По Н. Винеру, «информация» — это обозначение содержания, полученного от внешнего мира в процессе приспособления к нему.

Кибернетический подход к государственному управлению непосредственно связан с универсальной коммуникативной функцией открытых систем, с процессом сбора, обработки и передачи существенной социетальной информации, который является целью и средством деятельности государственно-административных структур, выступающих в качестве контура прямой и обратной связи общества.

Принципиально можно говорить о действительности системы государственного управления в случае её (всегда уникальной) заданности, т. е. самоопределённости в качестве совокупности всех элементов (подсистем) и информационных связей между ними.

Управление определяется взаимодействием трех компонентов: субъект, объект, среда. Субъект способен оказывать целенаправленное воздействие на объект управления (управляемую часть среды), который, в свою очередь, вместе со средой влияет на потребности субъекта. Оптимизация потребностей порождает очередную волевую реакцию, задавая, тем самым, алгоритм циклического воздействия, улучшающего управленческую функцию.

Алгоритм управления декомпозируется при осознанном удовлетворении потребностей, добавляя новую стадию — формулировку цели управления. Состояние среды и состояние объекта образуют исходную информацию для системы управления. Система управления создаёт команду управления — в какое состояние, должен быть приведён тот или иной управляемый вход объекта — результатом работы алгоритма<sup>10</sup>. Первый закон кибернетики по У.Р. Эшби гласит: «управление может быть обеспечено только в том случае, если разнообразие средств системы управления не меньше, чем разнообразие управляемой им ситуации»<sup>11</sup>.

Так, кибернетическим понятием о действии информационного выхода через канал обратной связи на входную величину, возможно, например, описать процесс совершенствования правотворчества, связанного с анализом уполномоченными субъектами эффективности реализации правовых норм, с формированием, принятием, изменением нормативных правовых актов.

В данном случае норма права выступает в качестве формы коммуникации<sup>12</sup>, средством информационного обмена между обществом и государством, а также внутри государственных структур. Таким образом, право

является условием согласованности воли, информационной функцией системы государственного управления, что можно математически выразить формулой:  $y = f(x)$ , где  $y$  — государственное регулирование (властная интенция);  $f$  — право (норма);  $x$  — общественные отношения, где  $f$  есть информационный символ некоторого преобразования, которому нужно подвергнуть величину  $x$ , чтобы получить  $y$  — это условие поддержания динамического системного равновесия (адаптации) за счет уменьшения влияния входной величины управленческого сигнала на выходную величину).

Фундаментальной проблемой теории и практики управленческой деятельности выступает стратегическое планирование государственного развития. Данную проблему можно свести к задачам по определению детерминант эволюции и закономерностей целеполагания управляемой системы.

Так, эндогенным фактором эволюции можно считать, развиваемый в современных исследованиях, механизм «иерархической поисковой оптимизации», где модификация системы для улучшения собственной эффективности обеспечивается структурой каналов циркулирующей информации от узкоспециализированных компонентов к компонентам высшего яруса и обратно, с постепенным решением релевантных задач адаптации к изменениям внешней и внутренней среды. Здесь, периодически, эволюционно могут возникать новые надстройки иерархического информационного контура — наивысшие ярусы, «вкладываемые» в себя все низшие.

Чем менее разнообразны сигналы, тем быстрее реакция — ответ на информацию. По мере повышения уровня иерархии действия становятся более медленными, но отличаются большим разнообразием<sup>13</sup>.

В контексте государственного управления, данные иерархические ярусы можно, например, выявить во времени (от совета дружины до парламента), в пространстве (от муниципалитета до федерации), в механизме публичной власти (от делопроизводителя до президента).

«Канализируемость эволюции связана с влиянием системной памяти каждого из уровней интеграции на активные процессы генерации приспособительного поведения на всех ярусах иерархии, вложенных в рассматриваемый»<sup>14</sup> (экономические, духовно-культурные, национальные, оборонительные, завоевательные и иные тенденции развития).

В свою очередь, закономерности целеполагания государственного развития (зачастую надсубъективного характера), в структурно-функциональном смысле, базируются на информационном факторе, определяющем модель реализации системы управления.

<sup>10</sup> Днепровская М.А. Кибернетический подход к описанию информационных систем // E-Scio. 2020. № 1. С. 3—12.

<sup>11</sup> Эшби У.Р. Введение в кибернетику. М.: Изд-во иностранной литературы, 1959. 432 с.

<sup>12</sup> Антонова Ю.П. Исследование коммуникативных процессов в системе государственного управления // Бюллетень науки и практики. 2019. № 10. С. 1—11.

<sup>13</sup> Сяский Д.Ю. Отдельные аспекты управления в социальных системах: кибернетический подход // Экономика и управление: проблемы, решения. 2017. № 1 (5). С. 79—86.

<sup>14</sup> Гринченко С.Н. Информатико-кибернетический подход в проблемах естествознания // Системы и средства информ. 2006. Спецвыпуск. С. 299—324.

Цель — планируемый результат; результат (от. лат. *resultatus* — отраженный) — конечный итог, воспринимаемый, в кибернетическом смысле, как выходной сигнал, требует высокого качества формализованного описания, в противном случае, он явится лишь намерением, лишаящим систему алгоритма адаптивного поведения. Данный аспект особенно актуален при выработке государственных национальных проектов, программ, доктрин, стратегий.

Вместе с тем, подразделяя деятельность системы государственного управления на процессы:

- 1) функционирования — поддержание гомеостаза,
- 2) развития — аккумуляирования информации, способствующей переходу к иному качеству функционирования (гомеостазу),

стоит отметить, особенно во втором случае, важность анализа наличной структурной информации для определения цели и постановке задач (система не может стать тем, чем она в принципе не может стать).

В условиях динамики условий окружающей действительности, в контексте поисковой оптимизации, предполагающей изменяющееся руководящее воздействие, процесс развития системы государственной организацией общества возможно описать, применяя математику дифференциальных уравнений, где, при обнаружении верной траектории движения в фазовом пространстве (периоде изменений), обнаруживается исключительная чувствительность к начальным данным. Здесь, проблема целеполагания развития связана с тем, что минимальная неточность в определении исходного состояния нарастает со временем делая невозможным долгосрочное прогнозирование.

Так, становится очевидной, в процессе стратегического планирования государственного развития, необходимость (максимально адекватной информации о исторической данности) оценки собственной, уникальной самоидентичности с соответствующим идейно-мотивационным вектором — аттрактором эволюции.

### **Математическое моделирование и программирование государственного и межгосударственного развития**

Актуализируя идею применения математического моделирования (как универсального способа мироприспособления) в исследовании системы государственной организации общества (СГОО), как явления социальной действительности, обладающего свойствами сложной, открытой, нелинейной системы, представляется важным решение вопроса, связанного с выработкой соответствующей программной модели самоорганизационного развития. Здесь, помимо описания алгоритма собственной динамической устойчивости отдельного государства, будет сделан акцент на исследовании межсистемного взаимовлияния нескольких стран, что, в частности, отвечает целям и задачам, «Основ государственной политики в сфере стратегического планирования в Российской Федерации», утвержден-

ных Указом Президента Российской Федерации № 633 от 08.11.2021 г.<sup>15</sup>

Так, необходимо определить специальные аналитические (информационные) показатели — факторы СГОО, где каждый показатель (параметр порядка) имеет свои условия динамики (параметры состояния):

1. Экономические факторы: инфляция, уровень безработицы, ВВП, уровень коррупции, государственные расходы, производительность труда, процентная ставка.
2. Политические факторы: стабильность правительства, поддержка власти населением, эффективность достижения показателей, гражданская инициатива.
3. Социальные факторы: демография, уровень образования, здоровье населения, уровень социального неравенства, уровень благосостояния.
4. Технологические факторы: инновационные производства, доступ к технологиям, развитие науки, технологическая независимость.
5. Внешние факторы: мировая экономика, санкции, войны, природные катастрофы.

Указанные факторы, имея количественно-статистические выражения, могут взаимозависимо изменяться во времени, и каждая (всегда специфическая) СГОО может по-разному реагировать на такие изменения. В программном коде можно учесть динамику через изменения параметров, влияющих на системную устойчивость.

Идея программного кода: возможность обновлять факторы во времени с помощью модели, где качество устойчивости каждой из сосуществующих систем (здесь — двух) пересчитывается на каждом временном шаге в зависимости от изменения динамических факторов. Таким образом:

1. Устойчивость систем (*stability\_system\_1*, *stability\_system\_2*) зависит от различных динамических факторов (экономика, политика, социальная сфера, технологии...).
2. Функция обновления факторов (*update\_factors*) моделирует случайные изменения в значениях факторов на каждом шаге времени. Здесь, можно использовать более сложные модели, например, зависимости факторов друг от друга или влияние внешних событий (санкции, природные катастрофы).
3. Симуляция (*simulate\_stability*) выполняет расчёт устойчивости систем на каждом временном шаге, учитывая изменения факторов. Взаимодействие систем можно выбирать в зависимости от сценария (взаимное ослабление, дополнение и т. д.).
4. Результат — это массив значений, показывающий, как менялась устойчивость коэволюционирующей системы с течением времени.

<sup>15</sup> Указ Президента Российской Федерации от 08.11.2021 № 633 «Об утверждении Основ государственной политики в сфере стратегического планирования в Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 01.08.2026).



Расширение программной модели:

- Можно добавлять внешние воздействия (например, глобальные кризисы, санкции, война) как неожиданные изменения факторов.
- Ввести время реакции систем на изменения факторов (например, не мгновенное, а с задержкой).
- Учитывать обратную связь между системами, если одна система напрямую влияет на другую.

Таким образом, код может моделировать, как собственную динамику, так и динамическое взаимодействие отдельных СГОО с учётом множества меняющихся факторов.

Обратная связь между системами особенно важна, когда одна система детерминирует другую. Включение обратной связи означает, что изменения в одной системе могут как усиливать, так и ослаблять устойчивость другой системы, и этот эффект учитывается на каждом временном шаге.

Включение обратной связи в код программы:

1. Прямая, обратная связь: изменения в устойчивости одной системы могут влиять на устойчивость другой. Например, если одна система становится менее устойчивой, это может привести к ухудшению устойчивости другой системы.

2. Коэффициенты обратной связи: введём коэффициенты, которые будут регулировать силу взаимного влияния. Например:  $f_{12}$  — влияние первой системы на вторую;  $f_{21}$  — влияние второй системы на первую.

3. Модификация устойчивости: мы будем корректировать устойчивость систем на каждом шаге с учётом этих коэффициентов.

Описание соответствующего программного кода:

1. Функции устойчивости (`stability_system_1`, `stability_system_2`) теперь включают обратную связь. Например, в формуле для первой системы учитывается влияние второй системы через параметр `feedback_S2` и коэффициент обратной связи  $f_{12}$ .

2. Коэффициенты обратной связи:  $f_{12}$  — управляет тем, насколько сильно вторая система влияет на первую;  $f_{21}$  — управляет тем, насколько сильно первая система влияет на вторую. Эти коэффициенты могут принимать значения от 0 до 1. Чем они выше, тем сильнее системы взаимно влияют друг на друга.

3. Обновление устойчивости: на каждом шаге пересчитывается устойчивость систем с учётом факторов и влияния обратной связи.

4. Результат — это динамика взаимодействия двух систем с учётом их взаимного влияния.

Пример: если одна система, скажем, система 1, становится менее устойчивой из-за изменений в факторах или воздействий, это ухудшает систему 2 через коэффициент обратной связи  $f_{21}$ . Обратная связь работает в обе стороны, и система 2 может повлиять на систему 1, например, усугубляя её нестабильность.

Положительная динамика показателей системы находит свое развитие в оказании доминирующего влияния на другие СГОО, в том числе, посредством их поглощения или слияния, в результате чего

может сформироваться системная организация иного уровня.

Система, доминируя, встраивая другие системы (СГОО) реструктурирует количество и качество своих показателей путем взаимодействия с показателями встраиваемой или поглощаемой системы, при этом отсутствие или малозначительность определенного показателя у поглощаемой системы способно, при недостаточности ресурсов, вызвать дефект или уничтожение аналогичного показателя поглощающей системы, что может привести ее к деградации, как следствие саму сделать объектом поглощения.

В условиях указанного процесса, поглощаемая система, сама может приобрести или изменить уровень своих показателей за счет показателей поглощающей системы, и, повысив уровень устойчивости, выйти из-под ее влияния претерпев качественную и количественную трансформацию. Все описанные процессы, как относительно одной, так и определенной совокупности СГОО, могут происходить одновременно [11].

Этот подход позволяет моделировать сложные динамические взаимодействия СГОО, когда они взаимозависимы и влияют друг на друга через обратные связи.

Основные компоненты:

1. Устойчивость систем  $S_1$  и  $S_2$  как функции от факторов и обратной связи.

2. Факторы  $F_{econ}$ ,  $F_{pol}$ ,  $F_{soc}$ ,  $F_{tech}$  — экономические, политические, социальные и технологические показатели, влияющие на устойчивость.

3. Обратная связь — влияние одной системы на другую через коэффициенты  $f_{12}$  (влияние системы 2 на систему 1) и  $f_{21}$  (влияние системы 1 на систему 2).

Общая формула устойчивости систем с обратной связью:

Для системы 1:

$S_1(t) = \alpha_1 F_{econ}(t) + \beta_1 F_{pol}(t) + \gamma_1 F_{soc}(t) + \delta_1 F_{tech}(t) - f_{12}(1 - S_2(t-1))$   
где:  $\alpha_1, \beta_1, \gamma_1, \delta_1$  — весовые коэффициенты факторов для системы 1;  $f_{12}$  — коэффициент обратной связи, который регулирует, насколько сильно изменение устойчивости системы 2 влияет на систему 1;  $(1 - S_2(t-1))$  — влияние нестабильности системы 2 на систему 1 с задержкой на один шаг во времени.

Для системы 2:

$S_2(t) = \alpha_2 F_{econ}(t) + \beta_2 F_{pol}(t) + \gamma_2 F_{soc}(t) + \delta_2 F_{tech}(t) - f_{21}(1 - S_1(t-1))$   
где:  $\alpha_2, \beta_2, \gamma_2, \delta_2$  — весовые коэффициенты факторов для системы 2;  $f_{21}$  — коэффициент обратной связи, который регулирует влияние системы 1 на систему 2;  $(1 - S_1(t-1))$  — влияние нестабильности системы 1 на систему 2 с задержкой.

Объяснение:

1. Устойчивость системы: Каждая система на шаге  $t$  определяется суммой влияний динамических факторов  $F_{econ}(t), F_{pol}(t), F_{soc}(t), F_{tech}(t)$ . Эти факторы могут меняться во времени.

2. Обратная связь: Устойчивость системы 1 зависит от устойчивости системы 2 на предыдущем шаге, и наоборот. Это взаимное влияние отражено в терминах  $f_{12}(1 - S_2(t-1))$  и  $f_{21}(1 - S_1(t-1))$ . При снижении устой-

чивости системы 2 – то есть при приближении  $S_2(t-1)$  ( $S_2(t-1)$  к нулю – система 1 испытывает более сильное ослабление вследствие отрицательной обратной связи.

3. Временная динамика: В формулах учитывается задержка обратной связи на один временной шаг —  $t-1$ . Это означает, что изменения в одной системе влияют на другую с задержкой, что часто наблюдается в реальных системах.

Формула общей устойчивости взаимодействующих системы:

Для вычисления общей устойчивости двух систем можно использовать, например, модель взаимного ослабления:  $S_{\text{общ}}(t) = S_1(t) \cdot S_2(t)$  или взаимодополнения:  $S_{\text{общ}}(t) = S_1(t) + S_2(t) - (1 - S_1(t) \cdot S_2(t))$ , где  $S_1(t)$  и  $S_2(t)$  — устойчивости первой и второй систем на текущем временном шаге.

Динамическая модель:

Чтобы полностью описать систему во времени, можно повторять эти вычисления на каждом шаге  $t$  и обновлять значения  $S_1(t)$  и  $S_2(t)$  с учётом изменений факторов и обратной связи. При этом значения факторов ограничены диапазоном:  $0 \leq F_{\text{econ}}, F_{\text{pol}}, F_{\text{soc}}, F_{\text{tech}} \leq 1$ .

Пример с фиктивными коэффициентами:

Для системы 1:

$$S_1(t) = 0.7F_{\text{econ}}(t) + 0.1F_{\text{pol}}(t) + 0.1F_{\text{soc}}(t) + 0.1F_{\text{tech}}(t) - 0.2 \cdot (1 - S_2(t-1))$$

Для системы 2:

$$S_2(t) = 0.6F_{\text{econ}}(t) + 0.15F_{\text{pol}}(t) + 0.15F_{\text{soc}}(t) + 0.1F_{\text{tech}}(t) - 0.3 \cdot (1 - S_1(t-1))$$

Такой подход позволяет выразить взаимодействие двух систем с учётом динамики факторов и взаимного влияния через обратную связь.

Здесь, значение  $S=0$  соответствует неконкурентоспособности. Можно добавить в модель условие, что при достижении или приближении к нулю система становится нестабильной и неконкурентоспособной. Например, это можно интерпретировать как точку, где система полностью теряет свою эффективность или способность к конкуренции и/или автономности.

Новая формулировка с ограничением на  $S=0$ :

Для системы 1:

$$S_1(t) = \max(0, \alpha_1 F_{\text{econ}}(t) + \beta_1 F_{\text{pol}}(t) + \gamma_1 F_{\text{soc}}(t) + \delta_1 F_{\text{tech}}(t) - f_{12} \cdot (1 - S_2(t-1)))$$

Для системы 2:

$$S_2(t) = \max(0, \alpha_2 F_{\text{econ}}(t) + \beta_2 F_{\text{pol}}(t) + \gamma_2 F_{\text{soc}}(t) + \delta_2 F_{\text{tech}}(t) - f_{21} \cdot (1 - S_1(t-1)))$$

Здесь, функция  $\max(0, \dots)$  гарантирует, что устойчивость не опустится ниже 0. Это фиксирует ситуацию, когда система неконкурентоспособна при достижении значения  $S=0$ .

Динамическая модель: устойчивость можно рассматривать как нефиксированную величину, которая эволюционирует в зависимости от множества внешних и внутренних факторов. Это позволяет моделировать поведение систем в реальном времени, учитывая, как их взаимозависимость, так и независимые изменения факторов.

Представим, что на определённом шаге времени экономический кризис снижает  $F_{\text{econ}}$ , что уменьшает

устойчивость системы 1. Это изменение оказывает обратную связь на систему 2, которая начинает терять устойчивость, тем самым создавая цикл, в котором системы постоянно взаимодействуют и меняют своё состояние.

Такой подход позволяет не просто оценить статическое состояние устойчивости СГОО, но и предсказать возможные сценарии её изменения и критические моменты, когда системы могут стать неконкурентоспособными.

Далее, для того чтобы внедрить в систему возможность учета отрицательных показателей, можно использовать подходы, которые основаны на математическом моделировании процессов в эргосистемах [12]. Опираясь на концепции ситуационного планирования, координации и обработки информации, мы можем адаптировать модель к условиям, в которых показатели могут принимать как положительные, так и отрицательные значения.

Возможности интеграции отрицательных показателей:

1. Математическое моделирование показателей:

Показатели (например, утраты территории, убыли населения, дефицита бюджета, потеря политических рейтингов) можно рассматривать как величины, изменяющиеся со временем, которые принимают как положительные, так и отрицательные значения. Это можно выразить через функцию, которая описывает изменение показателя, например:  $P(t) = P_0 + \sum_{i=1}^n \Delta P_i(t)$ , где  $P(t)$  – значение показателя в момент времени  $t$ ,  $P_0$  – начальное значение показателя,  $\Delta P_i(t)$  — изменение показателя в  $i$ -й период времени (оно может быть положительным или отрицательным).

1. Адаптация координационного планирования:

В координационном управлении эргосистемами, можно учитывать отрицательные изменения путем введения сигналов коррекции, которые будут реагировать на изменения в показателях. Например, если в модели планирования учесть отрицательные значения, это можно сделать через модифицированную целевую функцию:

$$F(t) = \alpha_1 P_1(t) + \alpha_2 P_2(t) + \dots + \alpha_n P_n(t)$$

где каждый показатель  $P_i(t)$  может быть как положительным, так и отрицательным; коэффициенты  $\alpha_i$  определяют вес каждого показателя в общей функции.

2. Учет неопределенности и ситуации с отрицательными значениями:

Ситуационное планирование в условиях неопределенности (как в иерархических эргосистемах — СГОО) позволяет учитывать ситуации, когда показатели имеют отрицательные значения. Для этого можно использовать механизм принятия решений, который оптимизирует управление в зависимости от текущего состояния показателя:  $\text{Решение} = \arg \max F(t, W)$ , где  $W$  — набор управленческих решений, а  $F(t, W)$  — функция, зависящая от текущего состояния показателей (включая отрицательные).

3. Примеры использования отрицательных значений:

В модели эргасистемы отрицательные значения могут указывать на ситуации дефицита ресурсов или снижения эффективности системы. Например, если система государственного управления получает сигнал о снижении населения, то это может скорректировать распределение ресурсов и изменить приоритеты.

Используя координирующие сигналы, центральный элемент системы может реагировать на отрицательные изменения показателей, например:  $S_i(t+1) = S_i(t) - \beta P_{\text{decrease}}(t)$ , где  $P_{\text{decrease}}(t) \geq 0$  — величина отрицательного изменения показателя, а  $\beta$  — коэффициент, определяющий степень влияния этого изменения на устойчивость системы.

Таким образом, формула для расчета показателя с учетом отрицательных значений может выглядеть следующим образом:

$$S_i(t+1) = \max(0, \alpha_1 F_{\text{econ}}(t) + \beta_1 F_{\text{pol}}(t) + \gamma_1 F_{\text{soc}}(t) + \delta_1 F_{\text{tech}}(t) - \eta \cdot |P_{\text{negative}}(t)| - f_{ij}(1 - S_j(t)))$$

где  $S_i(t+1)$  — устойчивость системы на следующем шаге времени;  $P_{\text{negative}}(t)$  — отрицательное изменение показателя, учитывающее убыль или дефицит;  $\eta$  — коэффициент его влияния на устойчивость системы;  $f_{ij}$  — коэффициент обратной связи между системами  $i$  и  $j$ .

Этот подход позволяет учитывать как положительные, так и отрицательные изменения в показателях, адаптировать управление к текущей ситуации и учитывать их влияние на общую устойчивость системы.

Изложенная математическая модель может быть описана соответствующим программным кодом<sup>16</sup>:

```
import numpy as np

# Устойчивость системы 1 с учетом отрицательных факторов
def stability_system_1(factors, feedback_s2, f12, negative_impact, eta1):
    economic, political, social, tech = factors

    base_stability = (
        0.7 * economic
        + 0.1 * political
        + 0.1 * social
        + 0.1 * tech
    )

    return max(
        0,
        base_stability
        - eta1 * abs(negative_impact)
        - f12 * (1 - feedback_s2)
    )
```

```
# Устойчивость системы 2 с учетом отрицательных факторов
def stability_system_2(factors, feedback_s1, f21, negative_impact, eta2):
    economic, political, social, tech = factors

    base_stability = (
        0.6 * economic
        + 0.15 * political
        + 0.15 * social
        + 0.1 * tech
    )

    return max(
        0,
        base_stability
        - eta2 * abs(negative_impact)
        - f21 * (1 - feedback_s1)
    )

# Обновление факторов с учетом отрицательных и положительных изменений
def update_factors(factors):
    economic, political, social, tech = factors

    return (
        np.clip(economic + np.random.uniform(-0.02, 0.02), -1, 1),
        np.clip(political + np.random.uniform(-0.01, 0.01), -1, 1),
        np.clip(social + np.random.uniform(-0.015, 0.015), -1, 1),
        np.clip(tech + np.random.uniform(-0.01, 0.02), -1, 1),
    )

# Моделирование динамики устойчивости систем
def simulate_dynamic_stability(
    steps,
    initial_factors,
    f12,
    f21,
    eta1,
    eta2,
    initial_negative_impact
):
    factors = initial_factors
    stability_over_time = []

    s1 = 1.0
    s2 = 1.0
    negative_impact = initial_negative_impact
```

<sup>16</sup> Используемый язык программирования — Python.

```

for step in range(steps):
    s1 = stability_system_1(
        factors, s2, f12, negative_impact, eta1
    )

    s2 = stability_system_2(
        factors, s1, f21, negative_impact, eta2
    )

    stability_over_time.append((s1, s2))

    factors = update_factors(factors)

    # Случайное изменение отрицательного
    показателя
    negative_impact = np.random.
    uniform(-0.05, 0.05)

    return stability_over_time

# Исходные параметры
initial_factors = (0.7, 0.8, 0.6, 0.7)

f12 = 0.2 # Влияние системы 2 на систему 1
f21 = 0.3 # Влияние системы 1 на систему 2

eta1 = 0.5 # Влияние отрицательных
показателей на систему 1
eta2 = 0.4 # Влияние отрицательных
показателей на систему 2

initial_negative_impact = -0.1

# Симуляция на 100 шагов
stability_result =
simulate_dynamic_stability(
    steps=100,
    initial_factors=initial_factors,
    f12=f12,
    f21=f21,
    eta1=eta1,
    eta2=eta2,
    initial_negative_impact=initial_
negative_impact
)

# Вывод результатов
for step, (s1, s2)
in enumerate(stability_result, start=1):
    print(
        f"Шаг {step}: "
        f"устойчивость системы 1 = {s1:.3f}, "
        f"устойчивость системы 2 = {s2:.3f}"
    )

```

Таким образом, представленный программный код способен учитывать широкий диапазон экономических и социальных условий, что делает его подходящим для реальных сценариев государственного развития и управления.

Изложенные алгоритмы информационно-математического моделирования, как основы компьютерных симуляций для прогнозирования развития страны, здесь, были представлены на концептуальном, статическом и динамическом уровнях. Практическое же их применение связано с соответствующим операционным уровнем, в рамках которого должен быть задействован огромный массив актуальной статистической информации (Big Data).

### Заключение

Подводя итог, стоит еще раз обозначить, что в результате настоящего исследования был решен ряд актуальных теоретических задач, а именно: описаны принципы кибернетического научного подхода; раскрыто понятие гомеостазиса государства; исследована проблема государственного системогенеза; проведен информалогический анализ государственного управления; представлены алгоритмы математического моделирования и программирования государственного и межгосударственного развития.

Можно сказать, что кибернетические методы и модели, являясь специальными теоретическими конструктами синергетической научной парадигмы, представляют собой мощный междисциплинарный инструмент для анализа и моделирования государственных процессов, позволяя выявлять внутренние механизмы функционирования системы, прогнозировать развитие событий и оптимизировать управление.



## Литература

1. Грибков А.А. Теория познания и общая теория систем // Общество: философия, история, культура. 2023. № 7. С. 21—27. DOI: 10.24158/fik.2023.7.2.
2. Кучин Н.С., Распереза О.А. Общая теория систем как эффективный методологический инструмент построения системной, прикладной теории права // Образование и право. 2022. № 3. С. 60—64.
3. Тарент И.Г., Грошева А.Р. «Забывтая» тектология А.А. Богданова и современные проблемы организации научного познания // Гуманитарный вестник ВА РВСН. 2021. № 1 (23). С. 13—21.
4. Борейко А.В. Тектология А. Богданова и мир-системный анализ в ТМО // Общественные науки и современность. 2024. № 2. С. 52—62.
5. Кузнецов Е.Д., Кесель С.А. Кибернетический подход к управлению национальной безопасностью: предиктивное моделирование сложных систем с помощью графовых сетей // Правовая информатика. 2025. № 4. С. 86—94.
6. Новиков А.В., Габараев А.Ш. Процесс планирования в сложных динамических системах. Кибернетический подход в правоохранительной деятельности // Экономика: вчера, сегодня, завтра. 2024. Т. 14. № 8А. С. 595—603.
7. Россинский Б.В. Синергетический подход как атрибут системы публичного управления // Административное право и процесс. 2026. № 5. С. 11—18.
8. Гарашко А.Ю. Синергетический подход как основа развития системной методологии юридической науки // Юридическая техника. 2023. № 17. С. 250—252.
9. Луковкин К.Е. Ассоциальный подход к пониманию общественных систем // Теория государства и права. 2024. № 2 (40). С. 65—71.
10. Гринченко С.Н. Общественно-экономические формации в контексте системного генезиса Человечества: кибернетический взгляд // Современные информационные технологии и ИТ-образование. 2021. № 17 (2). С. 355—368.
11. Зырянов А.В. Синергетическая концепция государствовопонимания : дис. ... докт. юрид. наук. М. : РУДН, 2023. 402 с.
12. Ловцов Д.А. Информационная теория эргасистем. М. : РГУП, 2021. 314 с.

**SECTION:**  
*CONSTITUTIONAL LAW*

# CYBERNETIC APPROACH TO UNDERSTANDING THE STATE (SPECIAL THEORY OF SYNERGETICS)

*Zyryanov A.V.<sup>17</sup>*

**Keywords:** *theory of the state, public administration, cybernetics, systemogenesis, homeostasis, informatology, mathematical modeling, programming.*

## **Abstract**

**Purpose of work:** *The aim of this study is to investigate the impact of the cybernetic approach on understanding the structure and functioning processes of the state, its evolution, as well as to determine the possibilities for its application in enhancing management efficiency and developing state institutions — thereby contributing to the scientific and methodological support of strategic planning in the Russian Federation.*

**Research method.** *The use of interdisciplinary methods (from social philosophy, political science, public administration, sociology, systems theory, synergetics, informatics, mathematics, etc.) capable of accounting for dynamics and feedback loops within the system and inter-system interactions is intended to objectify the perception of the problem under consideration. The proposed approach enables modeling state processes as information systems, revealing their stability, vulnerability, and potential for development.*

**The results of the study:** *As a result of the study, a number of theoretical and practical tasks were solved, specifically: the concept of the state's homeostasis is elucidated; the problem of state systemogenesis is investigated; an infological analysis*

---

<sup>17</sup> **Aleksey V. Zyryanov**, Dr.Sc. (Law), Professor of the Department of General Theoretical Legal Disciplines, Russian State University of Justice, Ural Branch, Chelyabinsk, Russia. ORCID: 0000-0002-6364-1812.  
E-mail: [zav-nauka@mail.ru](mailto:zav-nauka@mail.ru)

*of public administration is conducted; algorithms for mathematical modeling and programming of national and interstate development are presented. he presented algorithms of information-mathematical modeling — as the foundation for computer simulations aimed at forecasting national development — are described here at conceptual, static, and dynamic levels.*

## References

1. Gribkov A.A. Teoriia poznaniia i obshchaia teoriia sistem // Obshchestvo: filosofia, istoriia, kul'tura. 2023. No. 7. S. 21—27. DOI: 10.24158/fik.2023.7.2.
2. Kuchin N.S., Raspereza O.A. Obshchaia teoriia sistem kak effektivnyi metodologicheskii instrument postroeniia sistemnoi, prikladnoi teorii prava // Obrazovanie i pravo. 2022. No. 3. S. 60—64.
3. Tarent I.G., Grosheva A.R. "Zabytaia" tektologiiia A.A. Bogdanova i sovremennye problemy organizatsii nauchnogo poznaniia // Gumanitarnyi vestnik VA RVSU. 2021. No. 1 (23). S. 13—21.
4. Boreiko A.V. Tektologiiia A. Bogdanova i mir-sistemnyi analiz v TMO // Obshchestvennye nauki i sovremennost'. 2024. No. 2. S. 52—62.
5. Kuznetsov E.D., Kesel' S.A. Kiberneticheskii podkhod k upravleniiu natsional'noi bezopasnost'iu: prediktivnoe modelirovanie slozhnykh sistem s pomoshch'iu grafovyykh setei // Pravovaia informatika. 2025. No. 4. S. 86—94.
6. Novikov A.V., Gabaraev A.Sh. Protsess planirovaniia v slozhnykh dinamicheskikh sistemakh. Kiberneticheskii podkhod v pravookhranitel'noi deiatel'nosti // Ekonomika: vchera, segodnia, zavtra. 2024. T. 14. No. 8A. S. 595—603.
7. Rossinskii B.V. Sinergeticheskii podkhod kak atribut sistemy publichnogo upravleniia // Administrativnoe pravo i protsess. 2026. No. 5. S. 11—18.
8. Garashko A.Iu. Sinergeticheskii podkhod kak osnova razvitiia sistemnoi metodologii iuridicheskoi nauki // Iuridicheskaiia tekhnika. 2023. No. 17. S. 250—252.
9. Lukovkin K.E. Assotsial'nyi podkhod k ponimaniu obshchestvennykh sistem // Teoriia gosudarstva i prava. 2024. No. 2 (40). S. 65—71.
10. Grinchenko S.N. Obshchestvenno-ekonomicheskie formatsii v kontekste sistemnogo genezisa Chelovechestva: kiberneticheskii vzgliad // Sovremennye informatsionnye tekhnologii i IT-obrazovanie. 2021. No. 17 (2). S. 355—368.
11. Zyrianov A.V. Sinergeticheskaiia kontseptsiiia gosudarstvoponimaniia : dis. ... dokt. iurid. nauk. M. : RUDN, 2023. 402 s.
12. Lovtsov D.A. Informatsionnaia teoriia ergasistem. M. : RGUP, 2021. 314 s.



# АДМИНИСТРАТИВНО-ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ПРАВ ГРАЖДАН В ФИСКАЛЬНЫХ ПРАВООТНОШЕНИЯХ

Кобзарь-Фролова М.Н.<sup>1</sup>

**Ключевые слова:** права и свободы в фискальной сфере как высшая ценность государства, обеспечение защиты прав, защита законных интересов, гарантии прав и свобод, средства и механизмы правовой защиты, диспозиция, административная и судебная защита, обжалование.

## Аннотация

**Цель работы:** продемонстрировать административно-правовые механизмы защиты прав граждан в фискальных правоотношениях, на примере механизма защиты прав в административном порядке в сфере налогов и сборов.

**Методы:** историко-правовой, логический, аналитический, методы синтеза и обобщающего анализа.

**Результат исследования:** в статье проводится линия, позволяющая проанализировать процесс формирования административно-правовых механизмов защиты прав граждан в фискальных правоотношениях, приведены отдельные нормативные правовые акты, имеющие историографическое значение, но и повлиявшие на становление механизмов защиты в административном порядке в современной правовой системе. В статье показано: встав на путь демократических преобразований, Российская Федерация на высшем, конституционном уровне закрепила положение о том, что человек, его права и свободы являются высшей ценностью государства. Присоединившись к международным договорам о защите прав и основных свобод, Российская Федерация перенесла основные постулаты международных актов в отечественное законодательство, тем самым подтвердила приверженность государства общепринятым международным нормам. Именно это стало основанием для разработки в фискальной сфере эффективно действующих правовых механизмов защиты прав и свобод человека. Проведенное исследование позволило выявить пробел в действующем законодательстве: до настоящего времени отсутствует определение понятия «защита прав» в публично-правовых отношениях. Данный вопрос требует отдельного внимания научной общественности.

DOI: 10.24412/1994-1404-2026-3-00-14

## Введение

Современное российское законодательство сформировалось и развивается с акцентом на защиту прав, законных интересов граждан. Данное требование было закреплено в нормах-принципах ныне действующей Конституции Российской Федерации, с учетом итогов всенародного обсуждения<sup>2</sup>. С момента ее принятия — человек, его права и свободы являются для государства высшей ценностью (1, ст. 2), государство признает свободы и обеспечивает гарантии защиты прав граждан. Научный и практический интерес представляет вопрос о действии (реализации на

практике) правового механизма защиты прав граждан в фискальных правоотношениях.

## Постановка проблемы

Право на свободу и защиту свобод и законных интересов является величайшим достижением человечества, уместно сказать «завоеванным» относительно недавно, с победой над фашизмом во всем мире. Это право закреплено в договорах, имеющих всемирно-историческое значение. Большинство стран поддержали и присоединились к международным актам, закрепившим право отстаивать и защищать свои права и законные интересы. Так, Всеобщая декларация прав человека, принятая Генеральной Ассамблеей ООН 10 декабря 1948 г. провозгласила право всех людей на равную защиту и право на эффективное восстановление в правах

<sup>2</sup> Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный текст Конституции РФ с внесенными поправками от 14.03.2020 опубликован на официальном интернет-портале правовой информации, URL: <http://pravo.gov.ru>, 04.07.2020.

<sup>1</sup> Кобзарь-Фролова Маргарита Николаевна, доктор юридических наук, профессор, главный научный сотрудник сектора административного права и административного процесса Института государства и права РАН, г. Москва, Россия.  
E-mail: [margokfnn@yandex.ru](mailto:margokfnn@yandex.ru)

компетентными национальными судами в случаях нарушения их основных прав, предоставленных им конституцией или законом<sup>3</sup>. Развитие этих положений нашло отражение в 7, 8, 12 и других статьях Декларации. Идентичные нормы содержатся в Международном пакте о гражданских и политических правах (ст. 17)<sup>4</sup>.

Заслуживает внимания статья 13 Конвенции о защите прав человека и основных свобод, которая устанавливает своеобразный примат частного интереса: «Каждый человек, чьи права и свободы... нарушены, имеет право на эффективные средства правовой защиты перед государственным органом даже в том случае, если такое нарушение совершено лицами, действовавшими в официальном качестве»<sup>5</sup>. Наряду с правом на равную защиту закона (статья 20) в Конвенции специально выделены положения о равном режиме осуществления и защиты субъективных прав физических и юридических лиц (статья 26). Каждый человек, права и свободы которого нарушены, имеет право на эффективное восстановление в правах и свободах в соответствии с национальным законодательством (статья 19).

Для целей данной работы **фискальная сфера** — это та сфера правоотношений, которые возникают по поводу реализации государственной политики по привлечению в бюджет государства доходов (налогов, сборов, пошлин, штрафов и прочих платежей), по поводу контроля за полнотой их уплаты, обжалования действий (бездействий) должностных лиц уполномоченных органов и прочие. Данный вид правоотношений, хоть и имеет непосредственное отношение к движению денежных средств, но вопросы управления в данной сфере отношений — это исключительная прерогатива административного права.

К настоящему времени разработана и действует система инструментов, обеспечивающих защиту прав и законных интересов граждан во всех сферах общественной жизни, в том числе в фискальной сфере. Законодательство о налогах и сборах, бюджетное, таможенное законодательство, гарантирует участникам фискальных правоотношений административную и судебную защиту их прав и законных интересов. Порядок защиты прав и законных интересов участников фискальных правоотношений определяется соответствующими законодательством Кодексом (например, Налоговым кодексом Российской Федерации<sup>6</sup>, Бюджетным кодексом Российской Федерации<sup>7</sup>, Кодексом Российской Федера-

ции об административных правонарушениях<sup>8</sup>) и иными кодифицированными актами и федеральными законами. Право судебной защиты прав и свобод, вплоть до обращения в международные органы по защите прав и свобод человека гарантируется каждому российскому гражданину Конституцией Российской Федерации (статья 46). Гражданский кодекс Российской Федерации направлен на обеспечение защиты гражданских прав лица во всех сферах деятельности, в т.ч. фискальной. Защиту нарушенных гражданских прав осуществляет суд, арбитражный суд или третейский суд. В случаях, прямо предусмотренных законом, защита гражданских прав осуществляется в административном порядке<sup>9</sup>. Надо заметить, что в юридической законодательной практике все отчетливее проявляется тенденция к сближению гражданско-правовых и бюджетных (налоговых, административных) правоотношений.

### Теоретико-правовая разработанность темы

Юридическая наука всегда относилась с большим интересом к исследованию проблем защиты прав и законных интересов граждан и организаций. Механизмы защиты прав не раз становились темой для дискуссий и научных статей<sup>10</sup>. В 2019 году Уральский государственный университет выпустил даже учебное пособие на данную тему<sup>11</sup>. Однако нужно заметить, что законодательного определения понятия «защита прав» в публично-правовых отношениях в российском праве до настоящего времени нет. Да и теоретики права до настоящего времени не предложили для целей применения отраслевыми публично-правовыми юридическими науками дефиниции «защита прав», не выделены критерии данного института для целей правоприменения. Нужно признать, что это существенный пробел как для науки, так и правоприменительной практики, который юридическая наука должна восполнить, только после чего правильным будет ставить вопрос о механизмах защиты. Тип решения такой проблемы в данном случае можно обозначить как концептуально-понятийный.

Попытка дать общее понятие защиты прав (в целом, без привязки к конкретной области правоотношений) была предпринята А.В. Малько, В.В. Субочевым, А.М. Шериевым, которые под защитой прав и свобод

<sup>3</sup> Российская газета, 1995, 04 марта. № 67.

<sup>4</sup> Международный пакт о гражданских и политических правах, вместе с Резолюцией 2200А (XXI) Генеральной Ассамблеи Организации Объединенных Наций (ООН) от 16 декабря 1966 г. Вступили в силу для СССР 23 марта 1976 года // Бюллетень Верховного Суда РФ. 1994. № 12.

<sup>5</sup> Примечание: подписана членами Совета Европы в 1950 году // Собрание Законодательства РФ. 2001. № 2. Ст. 163.

<sup>6</sup> Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ // Собрание законодательства Российской Федерации. 1998. № 31. Ст. 3824.

<sup>7</sup> Бюджетный кодекс Российской Федерации от 31 июля 1998 г. № 145-ФЗ // Собрание законодательства Российской Федерации. 1998. № 31. Ст. 3823.

<sup>8</sup> Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. 2002. № 1 (ч. I). Ст. 1.

<sup>9</sup> Ст. 11 Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. Ст. 3301.

<sup>10</sup> См. также: Сакун О.В. К вопросу о понятии «защита гражданских прав и законных интересов» // Вопросы гражданского права и процесса. № 1. 2011. С. 68—75; Смирнов А.П. К вопросу о понятии «охрана прав» и «защита прав» // Вестник Томского государственного университета, 2010, № 331, с. 123—130.

<sup>11</sup> Резер Т.М. Механизмы реализации и защиты прав человека и гражданина : учеб. пособие / Т.М. Резер, Е.В. Кузнецова, М.А. Лихачев / [под общ. ред. Т. М. Резер]; М-во науки и высш. образования Рос. Федерации, Урал. федер. ун-т. Екатеринбург : Изд-во Урал. ун-та, 2019. 110 с.



предлагают понимать правовой режим, носящий обеспечительный характер, способствующий реализации прав, свобод и законных интересов в случаях, когда имеется реальная угроза их нарушения, а также деятельности, связанной с восстановлением нарушенных прав, свобод и законных интересов либо добровольным удовлетворением требований обязанностями субъектами<sup>12</sup>. Уместно заметить, что данный режим связан с деятельностью правоохранительных (компетентных) органов и правосудием.

Анализ юридической научной литературы позволил выделить пять подходов к определению категории «защита права»:

- 1) как система юридических норм (в объективном смысле)<sup>13</sup>;
- 2) как система юридических мер<sup>14</sup>;
- 3) как деятельность специально уполномоченных органов публичной власти<sup>15</sup>;
- 4) как элемент субъективного права<sup>16</sup>;
- 5) как самостоятельное субъективное право (правомочие)<sup>17</sup>.

Нужно заметить, что в фискальных правоотношениях отсутствует единый подход к определению понятия «защита». Зачастую оно раскрывается через:

- принудительный способ осуществления права, применяемый в целях восстановления нарушенного права<sup>18</sup>;
- совокупность мер, направленных на восстановление или признание субъективных прав<sup>19</sup>;

- система государственно-правовых гарантий, а также деятельность уполномоченных органов, обеспечивающих защиту участников фискальных правоотношений<sup>20</sup>.

Многие авторы традиционно связывают вопросы защиты с нарушением субъективного права, законного интереса. Ученые-административисты нередко включают в понятие «защита» такие элементы, как «пресечение»<sup>21</sup>, «предупреждение», «восстановление» права<sup>22</sup>. Зачастую в научной литературе термин «защита» подменяется или отождествляется понятием «охрана». В нашем понимании термин «защита» в понятии «правовая защита» означает двуединое явление, вбирающее в себя, и охрану прав, и защиту прав. Но с лингвистических позиций в рамках этимологии они имеют разные корни и не вполне идентичный смысл. Так, в толковом словаре В.И. Даля «защищать» означает оберегать, оборонять, отстаивать, заступаться, не давать в обиду<sup>23</sup>. В словаре С.И. Ожегова и Н.Ю. Шведовой защита означает охраняя, оградить от посягательств, от враждебных действий, от опасности<sup>24</sup>.

Таким образом, с этимологической точки зрения смысловые понятия «защита» и «охрана» не идентичны, они соотносятся как частное и общее. Защита неизменно связана с реальным или возможным нарушением права, законного интереса. Именно такой подход важен при разграничении тесно взаимосвязанных понятий «защита» и «охрана».

А.С. Зырянова верно отмечает, что защита прав и законных интересов — есть часть правовой охраны, заключающая в себе деятельность по реализации гарантий прекращения нарушения, признанию и восстановлению прав<sup>25</sup>. Согласимся и с позицией Н.С. Малеина, который подчеркивает, что «охрана прав» — более широкое понятие, включающее все юридические правила по поводу определенного блага, «защита» же — это понятие, обозначающее меры, которые предусмотрены в законе на те случаи, когда право уже нарушено<sup>26</sup>. Аналогичное суждение высказано С.Н. Кожевниковым<sup>27</sup>: охрана — это установление общего правового режима, а защита — меры, которые предпринимаются в случаях, когда права нарушены или оспорены. В связи с чем абсолютно верна и вышеупомянутая позиция

<sup>12</sup> Малько А.В., Субочев В.В., Шериев А.М. Права, свободы и законные интересы: проблемы юридического обеспечения. М.: Норма: Инфра-М, 2010. С. 80—81.

<sup>13</sup> Малеин Н.С. Гражданский закон и право личности. М., 1981. С. 193; Стоякин Г.Я. Защита абсолютного субъективного права // Гражданско-правовая охрана интересов личности в СССР / Под ред. О.А. Красавчикова. Свердловск, 1977. С. 54; Рожкова М.А. Средства и способы правовой защиты сторон коммерческого спора. М., 2000. С. 21. Смирнов А.П. Юридические средства защиты субъективных прав: дис. ... канд. юрид. наук [Ом. гос. ун-т им. Ф.М. Достоевского]. Омск, 2016.

<sup>14</sup> Юрченко О.О. Право на защиту и способы защиты охраняемого законом интереса в гражданском праве. Тверь, 2004. С. 35; Басин Ю.Д. Основы гражданского законодательства и защита субъективных прав. Саратов, 1971. С. 34.

<sup>15</sup> Вершинин А.П. Меры защиты субъективных прав по гражданскому законодательству // Проблемы совершенствования законодательства о защите субъективных гражданских прав / Под ред. В.В. Бутнева. Ярославль, 1988. С. 53; Крашенинников Е.А. Право на защиту // Методологические вопросы теории правоотношений. Ярославль, 1986. С. 9.

<sup>16</sup> Клигман А.В. Защита субъективных гражданских прав: некоторые проблемы // Защита субъективных гражданских прав / Под ред. В.А. Рясенцева. М., 1989. С. 4; Александров Н.Г. Законность и правоотношения в советском обществе. М., 1955. С. 109; Грибанов В.П. Осуществление гражданских прав. М., 2000. С. 37; Брагинский М.И., Витрянский В.В. Договорное право. Общие положения. М., 2001. С. 425.

<sup>17</sup> Гражданское право: учебник. В 2 т. Т. 1 / Под ред. А.П. Сергеева, Ю.К. Толстого. М.: ПБОЮЛ Рожников, 2001. С. 292; Братусь С.Н. Юридическая ответственность и законность. М., 1976. С. 72—79.

<sup>18</sup> Балакирева М.И. Право на обжалование как элемент правового статуса налогоплательщика: дис. ... канд. юрид. наук, 2005, с. 15.

<sup>19</sup> Смирных С.Е. Проблемы гарантий, пределов осуществления и защиты субъективных прав налогоплательщиков: дис. ... канд. юрид. наук. М., 2006. С. 124.

<sup>20</sup> Дудина Н.В. Правовые и организационные аспекты защиты прав налогоплательщиков в Российской Федерации: дис. ... канд. юрид. наук. М., 2005. С. 116

<sup>21</sup> См. Долгополов О.И. Рассмотрение жалоб в налоговой сфере. М.: Налоговый вестник, 2009. С. 11.

<sup>22</sup> Смирных С.Е. Указ. соч. С. 124.

<sup>23</sup> Даль В.И. Толковый словарь живого великорусского языка: В 4 т. СПб., 1863—1866.

<sup>24</sup> Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка (он-лайн версия) // URL: <http://www.classes.ru/all-russian/russian-dictionary-Ozhegov-term-9872.htm>

<sup>25</sup> Там же.

<sup>26</sup> Малеин Н.С. Охрана прав личности советским законодательством. М., 1985. С. 18, 19.

<sup>27</sup> Кожевников С.Н. Меры защиты в советском праве: автореф. дис. ... канд. юрид. наук. Свердловск, 1968. С. 4, 5.

Н.И. Матузова, который считает, что охрана и защита субъективного права или охраняемого законом интереса — не одно и то же: охраняются они постоянно, а защищаются только тогда, когда нарушаются. Защита есть момент охраны, одна из ее форм. Эти понятия, как продолжает автор, — не совпадают<sup>28</sup>. Очевидно верно, отметил С.С. Алексеев, — охранительные правоотношения, как указывает, начинают складываться с момента правонарушения, и при их помощи осуществляются меры юридической ответственности и защиты субъективных прав<sup>29</sup>.

Указанные нормы имеют направленный, властный характер и находятся на стыке материального и процессуального права.

### Краткий историко-правовой анализ генезиса института защиты прав и законных интересов налогоплательщика

Германский философ Х.Г. Гадамер отмечал: в гуманитарных науках необходимо познавать сходства, регулярности и закономерности, которые делают явления и процессы предсказуемыми<sup>30</sup>. В свою очередь, русский юрист С.А. Муромцев подошел с практической точки зрения: историко-правовой анализ позволяет юристу исключить из области действующего права то, что уже отжило.... Это имеет значение, как для теории, так и для практики<sup>31</sup>.

Организационно-правовое становление института разрешения публичных споров в Российской империи было связано с формированием системы государственной власти. В 1711 году еще Петром I при Правительствующем Сенате был учрежден специализированный Верховный орган управления и суда, уполномоченный на разрешение споров, связанных с уплатой налогов, сборов и прочих платежей<sup>32</sup>. Вместе с тем анализ законодательства царской России, действовавший до 1860-х гг., показывает, что в России не был выработан механизм, предусматривающий судебное обжалование действий органов, взимающих налоги и иные платежи, как не существовало и специальной системы административной юстиции.

Крестьянская реформа 1861 г., судебная реформа Александра II в 1864 г., создали прогрессивные условия по введению земского и городского самоуправления, закрепили право на обжалование решений органов

управления, включая фискальные органы, в Сенат. Впервые был обозначен принцип состязательности сторон при разрешении споров (который, однако, не подлежал обязательному соблюдению). В это же время для контроля за законностью деятельности всех органов управления были сформированы губернское по земским и городским делам присутствие. Органы представляли собой особые учреждения, которые рассматривали различного рода жалобы на акты административных органов и действия (бездействие) их должностных лиц<sup>33</sup>. Деятельность присутствия по земским и городским делам и промысловому налогу регламентировалась в особом порядке, основная их функция — судебно-административная<sup>34</sup>. Смешанное губернское присутствие было утверждено в качестве первой инстанции. На заседаниях рассматривались споры, как по налогам, так и иные, например, несения повинностей и другие<sup>35</sup>. Вместе с тем в деятельности присутствия, по признанию профессора государственного права С.А. Корфа, наблюдалось нежелание «признать субъективные публичные права русских граждан, вследствие чего в русском праве всегда довлел начальственный надзор над прочими функциями власти надзора»<sup>36</sup>.

С введением в 1898 году промыслового налога была создана судебно-административная инстанция для рассмотрения жалоб на постановления казенных палат и общих присутствий по делам о государственном промысловом налоге<sup>37</sup>.

Развитие демократических взглядов в большинстве европейских государств не могло не отразиться на законодательстве имперской России. С 1904 г. начинается период активного реформирования органов административной юстиции. Именным Высочайшим Указом от 12 декабря 1904 г. «О предначертаниях к усовершенствованию государственного порядка» Сенат обязан был принимать действительные меры к охране силы закона и обеспечить должное правосудие лицам потерпевшим от незаконных действий администрации<sup>38</sup>. «Для упрочения правильного в Отечестве Нашем хода государственной жизни...» указом повелевалось: «в целях охранения равенства перед судом лиц всех состояний, ввести должное единство в устройстве судебной в Империи части и обеспечить

<sup>28</sup> Матузов Н.И. Правовая система и личность. Саратов. 1987. С. 130—131.

<sup>29</sup> Там же. Т. 2. М., 1982. С. 108, 125;

<sup>30</sup> Гадамер Г.-Г. Истина и метод : Основы филос. герменевтики : Пер. с нем. / Х.-Г. Гадамер; Общ. ред. и вступ. ст. [с. 5—36] Б.Н. Бессонова. М. : Прогресс, 1988. 699 (С. 44).

<sup>31</sup> Муромцев С.А. Избранные труды по римскому и гражданскому праву. М., 2004. С. 527.

<sup>32</sup> Об учреждении Правительствующего Сената и бытии при оном Розрядному столу вместо Розрядного приказа, и по два комиссара из губерний // ПСЗ. Т. IV. № 2321.

<sup>33</sup> Там же. См. также: Положение о губернских и уездных земских учреждениях высочайше утвержденное 12 июня 1890 г. // С.-Пб : типогр. Мин-ва внутренних дел, 1890.

<sup>34</sup> Зеленцов А.Б. Административная юстиция. М. : Изд-во УДН, 1997. С. 63.

<sup>35</sup> Мегрелидзе М.Р. Становление института разрешения административно-правовых споров. М. : ИД «Юриспруденция», 2008. С. 68.

<sup>36</sup> Корф С.А. Административная юстиция. СПб., 1910. С. 211.

<sup>37</sup> О поручении Правительствующему Сенату попечения о правосудии, об устройстве государственных доходов, торговли и других отраслей государственного хозяйства // ПСЗ. Т. IV. № 2330. URL: [https://ru.ruwiki.ru/wiki/Государственный\\_промысловый\\_налог](https://ru.ruwiki.ru/wiki/Государственный_промысловый_налог)

<sup>38</sup> Лазаревский Н.М. Соображения комитета министров о преобразовании административной юстиции // Право. 1905. № 6. С. 385.

судебным установлениям всех степеней необходимую самостоятельность»<sup>39</sup>.

В 1907 г. в рамках административной реформы, задуманной П.А. Столыпиным рассматривался вопрос о создании административных судов. По мнению Ю.Н. Старилова, в это время по многим причинам «попытки создания нормально работающей системы административной юстиции (административных судов) были безуспешны»<sup>40</sup>.

В 1914 году была проведена реформа порядка производства и решения дел в департаментах Сената<sup>41</sup>, которая отразилась на вопросах процессуального разрешения дел в административных департаментах Сената. Не вызывает сомнения, что реформа была направлена на обновление и оптимизацию вопросов, связанных защитой и обеспечением прав и законных интересов граждан. Одним из достижений данной реформы было установление состязательности сторон при даче объяснений по делу, как выражение принципа равноправия при представлении доказательств. В результате реформы I-й Департамент Сената превратился в Высший административный суд Российской империи<sup>42</sup>.

Последним актом, принятым до социалистической революции 1917 года, было Положение о судах по административным делам (30 мая 1917 г.)<sup>43</sup>, согласно которого судебная власть по административным делам принадлежит административным судьям; окружным судам и Правительствующему сенату. Как известно из истории, Советской властью были отвергнуты все законы и иные нормативные акты, принятые в имперской России. Выстраивать отношения юстиции пришлось заново. В целях упорядочения отношений между рабочими, крестьянами и представителями органов советской власти издается Постановление «О точном соблюдении законов». Оно было принято по инициативе В.И. Ленина в ноябре 1918 года на VI Всероссийском Чрезвычайном съезде Советов<sup>44</sup>. В п. 3 Постановления говорится: «вменить в обязанность всем должностным лицам и советским учреждениям по требованию любого гражданина Республики, желающего обжаловать их действия, волокиту или чинимые ему в его законных притязаниях затруднения, составление соответствующего краткого протокола»<sup>45</sup>.

Уместно заметить, что после свершения революции до перехода к НЭПу было провозглашено безналоговое общество, произошла отмена всех ранее действующих налогов и создана новая форма обложения (сбо-

ра), выполняющая чисто революционные задачи, налоговый аппарат был распущен, органы по рассмотрению жалоб были закрыты<sup>46</sup>. Вплоть до 1937 г. законность в сфере управления обеспечивалась установлением государственного, ведомственного и общественного контроля<sup>47</sup>.

В 1922 г. утверждается Положение о взимании налогов<sup>48</sup>, раздел V которого предусматривал возможность подачи жалобы на неправильные действия/распоряжения должностных лиц при взимании платежей. А в 1937 г. был сделан переход к судебному надзору за законностью в вопросах государственного управления<sup>49</sup>. Каких-либо нормативных актов, регламентирующих защиту прав и законных интересов в фискальной сфере в военное время принято не было. Вплоть до 1961 года из-за отсутствия процессуально установленной формы обжалования актов в данной сфере, обжалование регламентировалось и осуществлялось в порядке гражданского судопроизводства<sup>50</sup>.

Право на обжалование действий должностных лиц органов государственной власти, в том числе в сфере финансов и налогов было предоставлено гражданам Указом Президиума Верховного Совета СССР от 12 апреля 1968 г.<sup>51</sup>. Нужно заметить, что указанным правовым актом впервые за долгие годы советской власти были закреплены виды обращений граждан (заявления, предложения, жалобы) и порядок их рассмотрения. Данное правило нашло отражение в консервативной Конституции СССР 1977 г. (ст. 58), в которой впервые на высшем, конституционном уровне было закреплено право граждан на обжалование в суд действий должностных лиц, однако данная норма целое десятилетие оставалась «мертвой» для большинства граждан<sup>52</sup>. Уже в постперестроечное время принимается Закон РФ № 4866-1 «Об обжаловании в суд действий

<sup>46</sup> Могилевский О.А. Налоги за 10 лет. Казань : Изд-во Татнаркомфина, 1927. С. 7.

<sup>47</sup> Чечот Д.М. Административная юстиция. Теорет. пробл. Л. : Изд-во Ленингр. ун-та, 1973. С. 63.

<sup>48</sup> Декрет совета народных комиссаров. Положение о взимании налогов и сборов от 6 мая 1922 г. URL: <https://docs.historyrussia.org/ru/nodes/351194>

<sup>49</sup> Постановление ЦИК и СНК СССР от 11 апреля 1937 г. «Об отмене административного порядка и установлении судебного порядка изъятия имущества в покрытие недоимок по государственным и местным налогам, обязательному окладному страхованию, обязательным натуральным поставкам и штрафам с колхозов, кустарно-промысловых артелей и отдельных граждан» // URL: <https://docs.historyrussia.org/ru/nodes/245813>

<sup>50</sup> Закон СССР от 8 декабря 1961 г. «Об утверждении Основ гражданского судопроизводства Союза ССР и союзных республик» // СЗ СССР. 1990. Т. 10. С. 133.

<sup>51</sup> Указ Президиума ВС СССР от 12 апреля 1968 г. № 2534-VII (в ред. от 02.02.1988) «О порядке рассмотрения предложений, заявлений и жалоб граждан» // Свод законов СССР. 1968. Т. 1. С. 373.

<sup>52</sup> Овечкин М.А. Специализированные суды в системе судов общей юрисдикции в Российской Федерации: конституционно-правовое исследование : автореф дис. ... канд. юрид. наук : 12.00.02 / СЮИ МВД РФ. Саратов, 2006. 26 с.

<sup>39</sup> URL: <https://constitution.garant.ru/history/act1600-1918/3080/>

<sup>40</sup> Старилов Ю.Н. Административная юстиция. Теория, история, перспективы. М. : НОРМА (Издательская группа «НОРМА-ИНФРА-М»), 2001. С. 6.

<sup>41</sup> Собрание узаконений и распоряжений Правительства. 1917. № 11. Ст. 68.

<sup>42</sup> Мергелидзе М.Р. Там же.

<sup>43</sup> Собрание узаконений и распоряжений Правительства. 1917. № 127. Ст. 692.

<sup>44</sup> URL: <https://istmat.org/node/31948>.

<sup>45</sup> URL: <https://istmat.org/node/31948>

и решений, нарушающих права и свободы граждан»<sup>53</sup>, который предусматривал право на обжалование в суд или государственный арбитраж любых актов органов государственной власти. В настоящее время действует глава 22 Кодекса административного судопроизводства РФ (КАС РФ)<sup>54</sup>.

### Современные административно-правовые механизмы защиты прав и законных интересов и их элементы

При выборе механизмов защиты прав в фискальных правоотношениях нельзя не учитывать, что их участники наделяются законом специальным статусом, например, налогоплательщики, плательщики сборов, пошлин иных платежей. Также необходимо учитывать особенности отраслевого правового регулирования видов правовых отношений. Р.О. Халфина, очевидно, верно отметила: в фискальных областях на первый план выступают особенные характеристики субъектов отношений и их права<sup>55</sup>. Субъекты налоговых правоотношений, являясь одновременно субъектами финансового (бюджетного) права и финансового (бюджетного) правоотношения, характеризуются комплексом юридических прав и обязанностей, свойственных одновременно гражданским отраслям и публично-правовым. Данный вид отношений, возникает, прежде всего, по поводу имущественных и личных неимущественных отношений и связан с движением денежных средств. Субъекты обязаны вести (налоговый) учет, составлять и сдавать на проверку отчетность, вести учет имущества, уплачивать законно установленные налоги и сборы в соответствующие бюджеты и внебюджетные целевые фонды и проч. Из этого следует, что специальный правовой статус участника фискальных отношений оказывает свое влияние на механизм защиты субъективных прав и законных интересов. Конституционное признание права на защиту налогоплательщика, получателя средств из государственных внебюджетных фондов и прочих, возлагает на государство обязанность создавать условия и вырабатывать действенные механизмы, способные гарантировать и обеспечить гражданам их законные права.

Подойдем к рассмотрению искомой темы с позиции административно-правовой защиты прав налогоплательщика. Статья 22 НК РФ закрепляет гарантии защиты прав и законных интересов налогоплательщиков в административном и судебном порядке. Часть 2 указанной статьи говорит о том, что права налогоплательщиков корреспондируются и обеспечиваются соответствующими обязанностями должностных лиц

налоговых органов и иных уполномоченных органов. Кодексом закреплено право любого лица обжаловать ненормативные акты налоговых органов действия или бездействие их должностных лиц, если, указанные акты, действия или бездействие нарушают его права (ст. 137 НК РФ). Данная модель обязательного последовательного обжалования введена законодателем относительно недавно — в 2013 году [1]. Участникам фискальных отношений, в т.ч. налогоплательщикам предоставляется право урегулировать спор в досудебном порядке [2, с. 39—45].

Производство об оспаривании нормативных правовых актов и актов, содержащих разъяснения законодательства по административным делам выделено отдельно, регулируется КАС РФ и осуществляется в судебном порядке<sup>56</sup>. Уместно заметить, что, например, в сфере государственных и муниципальных услуг законодатель избрал традиционный подход, позволив гражданину сделать самостоятельно выбор между административным (досудебным или внесудебным обжалованием) и судебным обжалованием [3, 4].

В административном порядке жалоба может быть подана в вышестоящий налоговый орган (п. 1, ст. 138)<sup>57</sup>, который рассматривает жалобу, в течение пяти дней и выносит одно из следующих решений: о приостановлении исполнения решения; о частичном приостановлении исполнения решения; об отказе в приостановлении исполнения решения полностью (например, о привлечении к ответственности). О принятом решении в течение трех дней со дня его принятия налоговый орган сообщает в письменной форме лицу, подавшему жалобу.

Жалобы на действия (бездействие) налогового органа могут подать не только предприниматели, но и лица, не относящиеся к ним, например, по вопросу о предоставлении налоговых вычетов и их сумме [5, с. 32—45], подлежащей к возмещению, о сумме сбора за предоставление услуги, на требование налогового органа об уплате задолженности, на решение о взыскании задолженности и проч. [6, с. 102—115].

Налоговый кодекс закрепляет административно-процессуальный порядок подачи жалобы и сроки подачи жалобы, порядок восстановления пропущенных сроков подачи жалобы и проч. (ст. 139), порядок и сроки подачи апелляционной жалобы [7, с. 33—36; 8, с. 115—124; 9, с. 11—19]. (ст. 139.1), процедуры рассмотрения жалобы и принятия решения по ней (ст. 140). Налогоплательщик и/или иное лицо **вправе:**

- 1) отказаться от жалобы,

<sup>53</sup> URL: <https://legalacts.ru/doc/zakon-rf-ot-27041993-n-4866-1-ob/> (в настоящее время закон утратил силу вступлением в силу Кодекса административного судопроизводства РФ).

<sup>54</sup> Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ // Собр. законодательства РФ, 2015, № 10, ст. 1391.

<sup>55</sup> Халфина Р.О. Общее учение о правоотношении. М., 1974. С. 138.

<sup>56</sup> Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ // Собр. законодательства РФ, 2015, № 10, ст. 1391.

<sup>57</sup> См. Письмо ФНС России от 24.10.2022 № 7-8-04/0005@ «О направлении Обзора правовых позиций, отраженных в судебных актах Конституционного Суда Российской Федерации и Верховного Суда Российской Федерации, принятых во втором квартале 2022 года по вопросам налогообложения» // СПС «КонсультантПлюс».



2) реализовать свое право на обжалование решения налогового органа путем подачи апелляционной жалобы,

3) реализовать свое право на обжалование путем подачи жалобы на вступившее в силу решение налогового органа,

4) отозвать поданную в вышестоящий налоговый орган апелляционную жалобу (жалобу) полностью или в части<sup>58</sup>.

Современный интернет-технологии позволяют участникам фискальных отношений подать жалобу посредством сети Интернет<sup>59</sup>.

Таким образом, в фискальной сфере законодатель использует не только императивные, но и диспозитивные механизмы, позволяя участникам делать выбор. Например: подать декларацию лично, либо иным законным способом (через представителя, почтовым отправлением, посредством сети Интернет по телекоммуникационным каналам или через личный кабинет налогоплательщика (п. 4 ст. 80 НК РФ); подать заявление на налоговый вычет или отказаться от данного права в текущем году, но использовать его в любом последующем периоде в течение трех лет (п. 1.1 ст. 172 НК РФ); выбрать метод учета доходов и расходов (ст. 271—273, 313 НК РФ) и проч., защищать свои права (в том числе истребовать излишне уплаченный налог — ст. 78 НК РФ, обжаловать акты налоговых органов — ст. 137 НК РФ) [10, с. 46—51] либо не предпринимать мер по их защите.

**Вместо заключения:** оказавшись на пути демократических преобразований, Российская Федерация избрала высшей ценностью — права и свободы человека. Это подтверждается тем, что Россия не просто присоединилась к международным договорам, закреп-

ившим принципы гарантированности и обеспечения и защищать прав и законных интересов граждан, но и перенесла основные постулаты международных актов в отечественное законодательство. Таким образом, в Российской Федерации были не только утверждены вопросы унификации отечественного и международного права, но и продемонстрирована приверженность государства общепринятым международным нормам.

Несомненно, на становление и законодательное закрепление административно-правовых механизмов защиты прав граждан в фискальных правоотношениях, оказал влияние тот исторический путь, который прошло российское законодательство в данной сфере.

В настоящее время в юридической законодательной практике все отчетливее проявляется тенденция к сближению гражданско-правовых механизмов защиты и публично-правовых (бюджетных налоговых, административных).

Анализ оспаривания актов должностных лиц, на примере налоговых правоотношений, показывает, что выработанный механизм защиты прав и свобод в фискальной сфере обладает некоторыми характерными свойствами, как например: упрощенный порядок, скорость рассмотрения вопроса (жалобы), отсутствие платы (не нужно уплачивать пошлину за рассмотрение дела), соблюдение налоговой тайны и проч. Кроме указанного нет необходимости привлекать защитников (адвокатов), все процедуры пошагово регламентированы одним актом — НК РФ.

В результате проведенного исследования поднята проблема: до настоящего времени отсутствует законодательное определение понятия «защита прав» в публично-правовых отношениях. Данный вопрос требует отдельного внимания научной общественности.

## Литература

1. Гиноман Е.Н. Административная жалоба // СПС «КонсультантПлюс».
2. Голубитченко М.А., Галанова И.С. Досудебное урегулирование налоговых споров: перспективы в эпоху цифровизации // Электронное приложение к «Российскому юридическому журналу». 2022. № 2. С. 39—45.
3. Зырянов С.М. Государственный контроль (надзор) : монография. М. : Контракт, 2023. 232 с.
4. Финансовое право (право публичных финансов): доктрина, законодательство, судебная практика, сравнительно-правовой анализ : монография / Д.В. Винницкий, Е.А. Захаров, М.И. Зимулькин и др.; под науч. ред. Д.В. Винницкого. Институт права БРИКС. М. : Юстицинформ, 2023. Т. I. 676 с.
5. Васильева Е.Г. Механизм взыскания неправомерно (ошибочно) предоставленного имущественного налогового вычета по НДФЛ: актуальные вопросы правоприменения // Имущественные отношения в Российской Федерации. 2023. № 10. С. 32—45.

<sup>58</sup> Иншина Р.С. Досудебное обжалование решений налогового органа, вынесенных по результатам рассмотрения материалов налоговых проверок // СПС «КонсультантПлюс». 2020.

<sup>59</sup> См. Приказ ФНС России от 24.10.2013 № ММВ-7-9/462@ «О вводе в эксплуатацию интерактивного сервиса «Решения по жалобам» на официальном сайте ФНС России» (вместе с «Порядком обработки и передачи данных для размещения в интернет-сервисе «Решения по жалобам») // Информация о публикации: СПС «КонсультантПлюс».

6. Лифанов Д.М. Некоторые проблемы обжалования актов органов публичной власти: теория и судебная практика // Российский юридический журнал. 2023. № 2. С. 102—115.
7. Тиханычев А.П. Налоговый оппортунизм и концепция законных интересов налогоплательщика: соотношение категорий и проблемы правоприменения // Финансовое право. 2024. № 3. С. 33—36.
8. Омелехина Н.В. Концепт интереса в финансовом праве и структуре финансовых правоотношений // Журнал российского права. 2022. № 7. С. 115—124.
9. Шишкин Р. Когда пропуск налоговиками сроков и иные их нарушения помогут налогоплательщику // Юридический справочник руководителя. 2025. № 8. С. 11—19.
10. Носенко А.В. Обжалование в механизме урегулирования административных споров при осуществлении государственного контроля (надзора) // Административное право и процесс. 2026. № 1. С. 47—51.

SECTION:  
CONSTITUTIONAL LAW

## ADMINISTRATIVE AND LEGAL MECHANISMS FOR PROTECTING THE RIGHTS OF CITIZENS IN FISCAL LEGAL RELATIONS

Kobzar-Frolova M.N.<sup>60</sup>

**Keywords:** rights and freedoms in the fiscal sphere as the highest value of the state, ensuring the protection of rights, protection of legitimate interests, guarantees of rights and freedoms, legal protection instruments and mechanisms, disposition, administrative and judicial protection, appeal.

### Abstract

**Purpose of the study:** to demonstrate the administrative-law mechanisms for protecting citizens' rights in fiscal legal relations, using the mechanism of administrative protection of rights in the field of taxes and levies as an example.

**Research methods:** historical-legal, logical, and analytical methods, as well as methods of synthesis and generalizing analysis.

**Results of the study:** The article traces the formation of administrative-law mechanisms for protecting citizens' rights in fiscal legal relations. It examines individual regulatory legal acts that are not only of historiographical significance but also influenced the development of administrative mechanisms for the protection of rights in the contemporary legal system. The article demonstrates that, having embarked on the path of democratic transformation, the Russian Federation established at the highest, constitutional level that human beings and their rights and freedoms constitute the highest value of the state. By acceding to international treaties on the protection of human rights and fundamental freedoms, the Russian Federation incorporated the fundamental principles of international instruments into its domestic legislation, thereby affirming the state's commitment to generally recognized international standards. This provided the basis for developing effective legal mechanisms for protecting human rights and freedoms in the fiscal sphere. The study revealed a gap in the current legislation: to date, there is no statutory definition of the concept of "protection of rights" in public-law relations. This issue requires further attention from the academic community.

### References

1. Ginodman E.N. Administrativnaia zhaloba // SPS "Konsul'tantPlius".
2. Golubitchenko M.A., Galanova I.S. Dosudebnoe uregulirovanie nalogovykh sporov: perspektivy v epokhu tsifrovizatsii // Elektronnoe prilozhenie k "Rossiiskomu iuridicheskemu zhurnalu". 2022. No. 2. S. 39—45.
3. Zyrianov S.M. Gosudarstvennyi kontrol' (nadzor) : monografiia. M. : Kontrakt, 2023. 232 s.

---

<sup>60</sup> **Margarita N. Kobzar-Frolova**, Dr.Sc. (Law), Professor, Principal Researcher at the Sector of Administrative Law and Administrative Process, Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia.  
E-mail: [margokfnn@yandex.ru](mailto:margokfnn@yandex.ru)

4. Finansovoe pravo (pravo publicnykh finansov): doktrina, zakonodatel'stvo, sudebnaia praktika, sravnitel'no-pravovoi analiz : monografiia / D.V. Vinnitskii, E.A. Zakharov, M.I. Zimul'kin i dr.; pod nauch. red. D.V. Vinnitskogo. Institut prava BRIKS. M. : Iustitsinform, 2023. T. I. 676 s.
5. Vasil'eva E.G. Mekhanizm vzyskaniia nepravomerno (oshibochno) predostavlenного imushchestvennogo nalogovogo vycheta po NDFL: aktual'nye voprosy pravoprimereniia // Imushchestvennye otnosheniia v Rossiiskoi Federatsii. 2023. No. 10. S. 32—45.
6. Lifanov D.M. Nekotorye problemy obzhalovaniia aktov organov publichnoi vlasti: teoriia i sudebnaia praktika // Rossiiskii iuridicheskii zhurnal. 2023. No. 2. S. 102—115.
7. Tikhanychev A.P. Nalogovyi opportunizm i kontseptsiiia zakonnykh interesov nalogoplatel'shchika: sootnoshenie kategorii i problemy pravoprimereniia // Finansovoe pravo. 2024. No. 3. S. 33—36.
8. Omelekhina N.V. Kontsept interesa v finansovom prave i strukture finansovykh pravootnoshenii // Zhurnal rossiiskogo prava. 2022. No. 7. S. 115—124.
9. Shishkin R. Kogda propusk nalogovikami srokov i inye ikh narusheniia pomogut nalogoplatel'shchiku // Iuridicheskii spravochnik rukovoditelia. 2025. No. 8. S. 11—19.
10. Nosenko A.V. Obzhalovanie v mekhanizme uregulirovaniia administrativnykh sporov pri osushchestvlenii gosudarstvennogo kontroliia (nadzora) // Administrativnoe pravo i protsess. 2026. No. 1. S. 47—51.



# ОБ ИНФОРМАЦИОННО-ПРАВОВОЙ ПРИРОДЕ ФИНАНСОВОГО КОНТРОЛЯ

Глазунова И.В.<sup>1</sup>, Запольский С.В.<sup>2</sup>

**Ключевые слова:** контроль, финансовый контроль, финансовые правоотношения, информационное право, обратная связь, мониторинг, правомерное поведение, юрисдикция, правоохранительная деятельность, представление, контрольная процедура.

## Аннотация

**Целью** статьи является обоснование подхода к финансовому контролю как особому виду информационно-правовых отношений, обеспечивающих обратную связь в механизме публичного управления финансами.

**Метод исследования.** Системный анализ, концептуальное моделирование, формализованное описание, сравнительно-правовой метод, метод документального исследования, догматический правовой анализ.

**Результаты.** Обосновывается необходимость разграничения собственно контроля и юрисдикционной деятельности: контрольный орган получает, сопоставляет и оценивает юридически значимую информацию, однако разрешение вопроса об ответственности и применение правоохранительных мер должны относиться к компетенции административного органа, следствия или суда.

Показано, что современный финансовый контроль постепенно смещается от эпизодического выявления уже совершенных нарушений к постоянному мониторингу правомерного поведения участников финансовых отношений по нормативно заданной траектории, что свидетельствует об изменении его места в системе государственного управления: от разновидности наказательной деятельности к самостоятельному механизму получения и юридической обработки информации.

Разграничен юридический переход от контрольного правоотношения к правоохранительному, который осуществляется посредством самостоятельного формализованного акта — представления, фиксирующего результаты контроля и создающего процессуальные основания для деятельности компетентного правоохранительного органа.

Признавая, что природа контрольно-финансового отношения является информационной, сделан вывод о необходимости самостоятельного юридического механизма перехода к правовосстановительным действиям, в роли которого может выступать формализованное представление.

DOI: 10.24412/1994-1404-2026-3-00-15

## Введение и постановка задачи

Финансовый контроль традиционно включается в число важнейших юридических средств обеспечения законности и финансовой дисциплины. Его значение обычно связывают с выявлением нарушений, предупреждением нецелевого расходования денежных средств, проверкой правильности налоговых и иных обязательных платежей, обеспечением сохранности публичных ресурсов. Такое представление справедливо лишь отчасти. Оно отражает наиболее заметный внешний результат контрольной деятельности,

но не раскрывает ее собственную правовую природу. Если контроль определяется через обнаружение нарушения и последующее властное реагирование на него, то в одном понятии неизбежно соединяются разные по назначению и юридической конструкции виды государственной деятельности: получение информации, ее оценка, управленческая коррекция, административное пресечение, расследование, разрешение спора и применение ответственности. При подобном подходе контроль перестает быть самостоятельной правовой

<sup>1</sup> Глазунова Инесса Владимировна, кандидат юридических наук, доцент, старший научный сотрудник сектора административного права и административного процесса Института государства и права РАН, г. Москва, Россия.

E-mail: [adminlaw@igpran.ru](mailto:adminlaw@igpran.ru)

<sup>2</sup> Запольский Сергей Васильевич, доктор юридических наук, профессор, главный научный сотрудник сектора административного права и административного процесса Института государства и права РАН, г. Москва, Россия.

E-mail: [zpmoscow@mail.ru](mailto:zpmoscow@mail.ru)



категорией и превращается в собирательное обозначение почти всякого властного воздействия на подконтрольного субъекта.

Именно поэтому исходным для определения финансового контроля должен быть не вопрос о санкции и не вопрос о том, какое неблагоприятное последствие может наступить для проверяемого, а вопрос об информационной связи между управляемой финансовой системой и субъектом, уполномоченным получать сведения о ее функционировании.

Как известно, контроль представляет собой правовую форму обратной связи. Закон задает определенную модель финансового поведения, участник финансового правоотношения совершает юридически значимые действия, а контрольный механизм сообщает публичному управлению сведения о том, соответствует ли фактическое движение денежных средств, принятие решений и исполнение обязанностей нормативно установленной программе. В таком качестве контроль не является приложением к юрисдикции, напротив, он предшествует ей, способен существовать без нее и имеет собственную систему субъектов, процедур, объектов и юридических результатов.

Необходимость такой обратной связи особенно очевидна в финансовой сфере. Финансовые отношения возникают преимущественно в связи с реализацией публичных интересов и предполагают участие государства либо иного субъекта, наделенного публичными полномочиями [1]. Их предметом является формирование публичных фондов денежных средств, распределение и использование финансовых ресурсов, налогообложение, бюджетное финансирование, кредитование, денежное обращение, валютные, таможенные, страховые и иные отношения, имеющие финансово-правовое значение. В отличие от классического гражданского обмена многие из этих связей не строятся на эквивалентном встречном предоставлении. Их имущественная природа сочетается с нормативно заданной обязанностью действовать в интересах, выходящих за рамки частной автономии участников.

Отсюда следует особая роль обязательства в финансовом праве. Оно индивидуализирует предусмотренную законом программу поведения, связывая уполномоченного и обязанного субъектов определенным порядком действий. Однако само наличие обязанности еще не гарантирует ее исполнения. Публичный финансовый механизм нуждается в постоянном поступлении достоверной информации о том, как эта программа реализуется фактически. Именно здесь и возникает потребность в контрольном правоотношении [2]. Оно не подменяет основное налоговое, бюджетное, кредитно-расчетное, валютное или иное финансовое правоотношение, а «наслаивается» на него как специальная информационная связь, посредством которой фактическое поведение сопоставляется с нормативной моделью.

### О правовой природе контроля

Распространенное понимание контроля как совокупности наблюдения, проверки и принятия правоохранительных мер требует существенного уточнения. Наблюдение, истребование документов, получение отчетности, сопоставление данных, фиксация расхождений и формирование вывода о соответствии либо несоответствии поведения установленным требованиям образуют собственно контрольную деятельность. Иная природа у действий, посредством которых устанавливается юридическая ответственность, разрешается спор о праве, назначается административное наказание, производится уголовное преследование или выносится судебный акт. Эти действия имеют юрисдикционный характер и должны быть выведены за пределы понятия контроля.

Подобное разграничение не означает, что контроль лишается правового результата. Напротив, его итог имеет собственное юридическое значение. Контролирующий субъект вправе зафиксировать установленный факт, определить его относимость к предмету контроля, сопоставить полученные сведения с нормой права и сформулировать вывод о наличии отклонения от заданной модели поведения. Но такой вывод по своей природе остается информационно-правовым: он свидетельствует о наличии данных, требующих дальнейшего реагирования, а не разрешает вопрос о виновности, противоправности поведения, ответственности. Контрольная квалификация является предварительной и функционально ограниченной целями самой проверки. Она не должна превращаться в скрытую юрисдикцию.

Исторический опыт организации государственного контроля подтверждает сложность соединения этих функций. Попытки наделить контрольные структуры одновременно полномочиями по собиранию информации и самостоятельному правоохранительному решению выявленных ими же нарушений всегда создавали внутренний конфликт ролей. Рабкрин<sup>3</sup>, Наркомат государственного контроля, партийно-государственный и Народный контроль, а в более поздний период налоговая полиция демонстрировали различные организационные модели, однако сама проблема оставалась неизменной: субъект, который формирует информационную картину и заинтересован в подтверждении результатов собственной контрольной работы, не должен одновременно выступать окончательным арбитром в вопросе о юридической ответственности. Особенно чувствительно это для финансовой сферы, где один и тот же массив документов может допускать разные правовые интерпретации, а цена квалификационной ошибки непосредственно затрагивает имущественную сферу граждан и организаций<sup>4</sup>.

<sup>3</sup> Рабоче-крестьянская инспекция.

<sup>4</sup> Овчарова Е.В. Финансовый контроль в Российской Федерации: учебное пособие. М.: Зерцало-М, 2013. 224 с. ISBN: 978-5-94373-241-6.

Разделение контроля и юрисдикции позволяет иначе определить место финансового контроля в системе государственного управления. Он оказывается не разновидностью наказательной деятельности и не «первой стадией» применения ответственности, а самостоятельным механизмом получения и юридической обработки информации. Его задача состоит в том, чтобы обеспечить публичную власть достоверным знанием о состоянии финансовых отношений, о соблюдении установленной траектории поведения, о возникающих отклонениях и рисках. Уже на основе этого знания и при наличии предусмотренных законом оснований может возникнуть иной эффект, а именно: правоотношение — административно-деликтное, уголовно-процессуальное, гражданско-процессуальное. Такой подход приобретает особое значение в условиях изменения самой технологии контроля. Классическая ревизионная модель была преимущественно ретроспективной. Проверяющий приходил к уже совершенной операции, восстанавливал ее документальную картину и искал нарушение, которое произошло ранее. Поэтому контроль естественным образом ассоциировался с обнаружением проступка или преступления. Современная финансовая деятельность устроена иначе. Значительная часть сведений возникает одновременно с совершением юридически значимых операций, передается в электронной форме, сопоставляется с иными массивами данных и может анализироваться без ожидания специальной выездной проверки. В результате контроль постепенно перемещается от эпизодического поиска правонарушения к мониторингу правомерного поведения [3].

Смысл такого мониторинга состоит не в тотальном наблюдении за участником финансовых отношений как таковым, а в проверке его «движения» по нормативно определенной траектории. Закон заранее устанавливает необходимые точки этой траектории: возникновение обязанности, срок и способ ее исполнения, порядок документирования, условия распоряжения средствами, требования к отчетности, допустимые пределы усмотрения. Контрольная система получает сведения о прохождении этих точек и фиксирует отклонения. Поэтому предметом контроля становится уже не только завершённое нарушение, но и состояние исполнения правовой программы на каждом существенном этапе [4].

В этом смысле традиционное деление финансового контроля на предварительный, текущий и последующий получает более точное объяснение. Речь идет не о трех самостоятельных разновидностях властного вмешательства, а о разных временных моментах обратной связи по отношению к контролируемой финансовой операции. Предварительный контроль сопоставляет проектируемое действие с нормативной моделью до его совершения, текущий сопровождает движение операции, последующий восстанавливает и оценивает уже реализованную последовательность действий. Во всех трех случаях сущность остается единой: сбор

и правовая обработка информации о соблюдении заданной законом траектории.

Такой подход позволяет отказаться и от количественного понимания контроля, в рамках которого его эффективность нередко связывается с числом проверок, выявленных нарушений, начисленных сумм или примененных санкций. Если контроль существует как необходимая информационная связь внутри финансового механизма, то его интенсивность не должна измеряться количеством репрессивных результатов. Более совершенным контролем является тот, при котором правомерное поведение становится наблюдаемым и верифицируемым без избыточного вмешательства, а юридически значимое отклонение обнаруживается в момент, когда оно еще может быть корректно оценено и, при необходимости, передано компетентному правоохранительному субъекту [5].

Отсюда вытекает и иное понимание правомерного поведения в системе контроля. В традиционной модели оно остается почти невидимым: если нарушение не выявлено, проверка как будто не производит юридически значимого результата. Между тем нормальное исполнение финансовых обязанностей, соблюдение запретов, надлежащее расходование публичных средств, своевременная отчетность и корректное документирование операций также являются результатами, которые контрольная система должна подтверждать. Контроль тем самым выполняет не только негативную функцию обнаружения отклонения, но и позитивную функцию подтверждения соответствия фактической деятельности правовой программе. Именно это сближает современный контроль с мониторингом и делает его элементом устойчивого управления, а не исключительно реакцией государства на уже состоявшееся правонарушение.

Информационная природа контроля предопределяет содержание компетенции контролирующих органов. Такая компетенция должна включать право получать сведения в установленном законом объеме, требовать необходимые документы и пояснения, использовать предусмотренные процедуры проверки, сопоставлять данные, фиксировать установленные обстоятельства и формулировать контрольный вывод. Одновременно она должна быть ограничена предметом ведения, территориальной, отраслевой или функциональной специализацией, требованиями относимости и достаточности запрашиваемой информации, режимами государственной, банковской и коммерческой тайны, а также процессуальными гарантиями контролируемого лица.

Праву контрольного органа на получение информации корреспондирует обязанность подконтрольного субъекта допустить предусмотренное законом контрольное воздействие и участвовать в нем в той мере, в какой это необходимо для формирования достоверной информационной картины. Такая обязанность не означает общего подчинения контролеру. Их юридическая связь возникает по строго определенному

предмету и существует только в пределах контрольной процедуры. Поэтому глубина доступа к документам, продолжительность мероприятия, способы получения сведений, право требовать пояснения, возможность использования информации из иных источников и порядок ее хранения должны иметь нормативное основание [6, 7]. Иначе информационная функция контроля легко превращается в неопределенную властную зависимость.

Важнейшей гарантией здесь является процедурная формализация. Чем шире технические возможности получения и сопоставления финансовой информации, тем меньше оснований оставлять порядок контрольного взаимодействия на усмотрение должностного лица. Процессуальная форма дисциплинирует обе стороны: она определяет, какие сведения вправе получить контролер, каким способом они могут быть истребованы, каким документом оформляются результаты, как контролируемый вправе представить возражения и каким образом исправляются фактические ошибки. Развитие налогового контроля особенно отчетливо показывает, что сложная финансовая деятельность закономерно порождает массив процедурных норм, судебных подходов и устойчивых правил взаимодействия участников [8].

Наиболее уязвимым остается момент, когда полученная в результате контроля информация начинает использоваться для правоохранительных целей. Именно здесь происходит качественное изменение юридической природы отношений. До этого момента перед нами существует информационная связь — контролер получает и оценивает сведения о поведении подконтрольного. После него возникает правоохранительное правоотношение, в котором иными становятся субъектный состав, процессуальные гарантии, права и обязанности сторон, предмет доказывания, стандарт оценки фактов и возможные юридические последствия.

Такой переход не должен происходить фактически, посредством телефонного сообщения, неформального сигнала, передачи документов «для сведения» либо простого помещения материалов в информационный массив, к которому имеет доступ правоохранительный орган. Необходим юридически распознаваемый момент преобразования одного правоотношения в другое. Для обозначения соответствующего акта представляется оправданным использовать категорию представления, понимая ее не в узком смысле какого-либо одного уже существующего вида акта прокурорского или административного реагирования, а как обобщенную конструкцию формализованного направления результатов контроля компетентному правоохранительному органу.

Представление в таком понимании должно выполнять пограничную функцию. Оно завершает контрольную процедуру в той части, в которой выявленные сведения выходят за пределы обычной информационной оценки, и одновременно создает юридически оформленный повод для самостоятельной деятельности

административного органа, следствия или суда. В нем должны быть индивидуализированы контролируемое лицо и соответствующая операция, обозначены источник и способ получения информации, указана нормативная модель, с которой сопоставлялось фактическое поведение, зафиксированы выявленные отклонения и приложены материалы, позволяющие проверить сделанный контрольный вывод. Само представление не устанавливает противоправность, виновность и не предрешает исход будущего дела. Его назначение состоит в легальной трансформации сведений из контрольного режима в правоохранительный.

Эта конструкция принципиально отличается от доносительной логики, при которой любая информация о предполагаемом нарушении воспринимается как достаточная для запуска принудительного механизма. Контрольный орган действует не как случайный информатор. Он получает сведения в силу специальной компетенции, в рамках установленной процедуры и с использованием властных возможностей, которых нет у обычного участника гражданского оборота. Поэтому и передача результатов его деятельности должна быть не менее формализованной, чем их получение. Считаем, что, если государство допускает принудительный доступ к информации ради контроля, оно обязано определить и юридическую форму, в которой такая информация может быть превращена в основание правоохранительного вмешательства.

Максимальная формализация отношений с правоохранительным субъектом имеет еще одно значение. Она не позволяет контрольному органу скрыто продолжать собственную деятельность уже внутри административного, следственного или судебного процесса. После направления представления компетентный орган должен самостоятельно решить вопрос о наличии предусмотренных законом оснований для производства, определить предмет доказывания, проверить относимость, допустимость и достоверность полученных материалов и обеспечить лицу соответствующие процессуальные гарантии.

Именно поэтому объединение в одном органе полномочий по контролю и окончательному применению юридической ответственности должно рассматриваться как исключение, требующее специального обоснования и дополнительных гарантий. Природа юрисдикционной деятельности предполагает возможность независимой проверки версии, сформированной контролером. Если же субъект, который собирал сведения, определял направление проверки и формулировал вывод об отклонении, затем сам разрешает вопрос о виновности и санкции, граница между информационным и правоохранительным отношением исчезает. Это повышает риск того, что предварительная контрольная гипотеза будет ошибочно воспринята как уже установленный юридический факт [1, с. 131].

Право на обжалование результатов проверки также должно оцениваться через информационную природу контроля. Возражение контролируемого или

обращение в вышестоящий орган и/или суд позволяет проверить не только законность действий должностного лица, но и качество сформированной контрольной информации. Обжалование, способное выявить ошибки в фактах, неправильное определение предмета проверки, выход за пределы компетенции, нарушение процедуры получения сведений и ошибочное сопоставление фактического поведения с правовой или технической нормой. Тем самым оно служит механизмом верификации контрольного результата до того, как этот результат либо связанные с ним материалы повлекут реальное правоохранительное воздействие.

### О соотношении контроля и надзора в финансовой сфере

В этой системе по-новому раскрывается и проблема соотношения контроля и надзора. Многолетняя дискуссия о границах этих понятий во многом была вызвана попыткой различить виды властного вмешательства по объему полномочий контролирующего субъекта [9]. Если же исходить из информационной функции, надзор может рассматриваться как одна из организационно-правовых форм получения обратной связи, при которой доступ к сведениям облегчается особым компетенционным или иерархическим положением наблюдающего органа. Сам по себе этот статус не превращает информационную деятельность в юрисдикционную. Прокурорский надзор, банковский и страховой надзор, таможенный контроль, финансово-бюджетное и казначейское наблюдение используют различные юридические режимы, однако принципиальным остается вопрос о том, где заканчивается получение и оценка информации и начинается применение самостоятельного правоохранительного механизма.

Ревизионный контроль, напротив, характеризуется специально организованной процедурой активного получения информации. Проверка или ревизия требует взаимодействия контролера и контролируемого, допуска к документам, исследования операций, фиксации результатов. Здесь особенно важно унифицировать не содержание отраслевых финансовых обязанностей, а процедурные гарантии самого информационного процесса [10]. Финансово-бюджетные проверки, мероприятия контрольно-счетных органов Российской Федерации и субъектов Федерации, а также ревизии, связанные с расследованием уголовных дел, различаются по основаниям и целям, но во всех случаях проблема законности получения и последующей передачи финансовой информации имеет общее значение.

Отдельное место занимает декларационный контроль. Его развитие свидетельствует о смещении правовой инициативы в получении информации от контролирующего органа к самому обязанному субъекту. Декларирование доходов, имущества и обязательств имущественного характера государственными служащими, сведений о наличии конфликта интересов, публичная финансовая отчетность, результаты аудита

крупных коммерческих структур, бухгалтерский учет финансово-хозяйственных операций — все эти инструменты строятся на предварительной обязанности сформировать и раскрыть юридически значимую информацию. Контроль в данном случае начинается не с требования проверяющего, а с существующей независимо от него обязанности сделать финансовое поведение наблюдаемым и проверяемым.

Такое развитие подтверждает общий вектор трансформации контроля. Чем сложнее финансовый механизм, тем менее эффективна модель, при которой государство реагирует только после появления внешнего признака нарушения. Информационная архитектура финансового права все в большей степени должна быть рассчитана на непрерывное подтверждение правомерного движения по установленной законом траектории. Это не означает презумпции виновности каждого участника. Напротив, постоянство и стандартизированность информационной связи способны уменьшить потребность в чрезвычайных, выборочных и инвазивных проверках, поскольку правомерность значительной части действий подтверждается в обычном режиме исполнения обязанностей [11].

При этом нельзя смешивать мониторинг правомерного поведения с тотальным цифровым наблюдением. Правовая траектория ограничивает не только контролируемого, но и контролера. Собираться и обрабатываться должны лишь те сведения, которые имеют юридически установленное значение для проверки конкретной финансовой обязанности, запрета или полномочия. Иначе техническая возможность получения данных начинает подменять юридическое основание контроля. Информационная теория финансового контроля имеет смысл только при условии, что обратная связь строится в пределах права, а не поверх него.

С этих позиций становится понятной необходимость системы сдержек и противовесов внутри общества контрольных органов. Их компетенция не должна полностью дублироваться, а взаимодействие целесообразно строить преимущественно на координационной, а не субординационной основе. Разные виды финансовых отношений требуют специализированного знания центр, который одновременно контролирует все финансовые потоки и обладает универсальной юрисдикцией, неизбежно ведет к чрезмерной концентрации информационной и принудительной власти. Напротив, разделение компетенций позволяет сопоставлять данные, не устраняя функциональную самостоятельность субъектов, которые отвечают за разные участки финансовой системы.

Сложившаяся доктрина финансового контроля не всегда дает инструменты для такого разграничения. Лимская декларация 1977 г. сыграла значительную роль в формировании представлений о государственном финансовом контроле, однако ее основные положения исторически ориентированы прежде всего на контроль публичных финансов. Сходная логика просматривается в Модельном законе о государственном



финансовом контроле, принятом Межпарламентской Ассамблеей государств — участников СНГ 4 декабря 2004 г. В нем выделяются президентский, парламентский, административный и независимый государственный финансовый контроль, что отражает институциональную сторону вопроса, но не устраняет смешения контрольной, распорядительной и в ряде случаев правоохранительной деятельности.

Ограниченность такой конструкции особенно заметна применительно к банковскому надзору, таможенному и валютному контролю, финансовому мониторингу, антикоррупционным механизмам. Они не исчерпываются наблюдением за формированием и использованием централизованных денежных фондов. Их общий признак заключается в другом: государство организует получение и оценку информации о соблюдении финансово-правовой программы поведения. Поэтому современная теория финансового контроля не может быть построена исключительно на фондовой теории финансов. Предмет контроля шире движения средств внутри централизованных фондов и охватывает те финансовые связи, в которых публичный интерес требует юридически организованной обратной связи.

Полагаем, что не следует необходимости унифицировать все виды финансового контроля в одном детальном законе. Налоговый, бюджетный, эмиссионный, кредитно-расчетный, таможенный, валютный, страховой и иные институты обладают собственной материально-правовой спецификой. Именно внутри этих институтов определяется, какое поведение является правомерным, какие документы и сведения имеют значение, какие сроки должны соблюдаться и какие операции допустимы. Поэтому отраслевой инструментарий контроля неизбежно остается различным. Унификации подлежит не сама финансовая операция, а основные принципы информационного взаимодействия и правового перехода от контроля к правоохранению.

В этом отношении показательно, что Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» не распространяет общий режим государственного контроля на значительный круг отношений в финансовой сфере. Такая особенность подтверждает невозможность механически подвести финансовый контроль под универсальную модель административной проверки. Вместе с тем отсутствие единого регулирования делает особенно заметными расхождения в правах и обязанностях участников финансово-контрольных отношений, процедурах получения информации, формах фиксации результатов и порядке их передачи для правоохранительного реагирования.

Идея сквозного акта об основах финансового контроля сохраняет практический смысл, если отказаться от попытки заменить им отраслевое регулирование. Его предметом могли бы стать общие начала контрольной правосубъектности, пределы доступа к финансовой информации, требования к относимости и достаточности истребуемых сведений, права

контролируемого лица, принципы хранения и использования данных, правила оформления контрольного результата, способы его обжалования и, что особенно важно, юридическая процедура передачи материалов в правоохранительную сферу. Такая регламентация позволила бы закрепить контроль как самостоятельное информационное правоотношение, а не как размытый комплекс любых властных действий в отношении финансового субъекта.

Возможное законодательное закрепление представления как универсальной пограничной конструкции заслуживает, на наш взгляд, в этой связи отдельного обсуждения. Речь не идет о введении единого документа без учета процессуальных различий. Смысл состоит в закреплении общего принципа: информация, полученная посредством публично-властного контроля, не должна превращаться в основание уголовно-процессуального или административно-юрисдикционного реагирования, иначе как через определенную законом форму передачи. Такая форма должна позволять установить происхождение сведений, пределы контрольной процедуры, ответственность должностного лица за содержание направляемого материала и момент, с которого начинается компетенция иного органа.

Подобная модель способна решить сразу несколько задач. Она отделяет информационную деятельность от юрисдикционной, делает прозрачной смену правового режима сведений, препятствует неформальному обмену материалами между ведомствами, обеспечивает возможность последующей проверки законности их получения и исключает автоматическое превращение контрольного вывода в доказанную противоправность. В конечном счете формализованное представление защищает не только контролируемого субъекта. Оно защищает и правоохранительный орган от принятия решения на основе информационного массива, происхождение и процессуальный статус которого неясны. При таком понимании меняется и само представление об эффективности финансового контроля. Она состоит не в максимальном числе обнаруженных нарушений и не в расширении властных полномочий контролеров. Эффективен тот контроль, который обеспечивает достоверную, своевременную и юридически корректную обратную связь, позволяет подтверждать правомерное поведение, обнаруживать значимые отклонения от нормативной траектории и передавать сведения о них компетентному субъекту в установленной форме<sup>5</sup>. Правоохранительный результат при этом остается возможным следствием контроля, но не его сущностью.

<sup>5</sup> Терехова Е.В. Негосударственный финансовый контроль : монография. М. : МГУ им. Ломоносова, 2006. 152 с. ISBN: 5-211-05254-4.

### Сущность контрольно-финансовых правоотношений

Контрольно-финансовое правоотношение может быть определено как урегулированная нормами права информационная связь между уполномоченным субъектом контроля и подконтрольным участником финансовой деятельности, возникающая в целях получения, проверки, сопоставления и юридической оценки сведений о соответствии фактического поведения нормативно установленной программе. Его завершение возможно подтверждением соответствия, фиксацией отклонения, выдачей предусмотренного законом организационного предписания в пределах контрольной компетенции либо оформлением представления материалов компетентному правоохранительному органу. Но решение о юридической ответственности, применение наказания и разрешение спора принадлежат уже иному правоотношению, другому органу и не должны включаться в понятие финансового контроля.

Такой подход позволяет согласовать несколько внешне противоречивых тенденций современной финансовой политики. Государство действительно нуждается в более полной и оперативной информации о движении финансовых ресурсов, однако это не означает необходимости увеличивать число традиционных проверок и расширять репрессивные полномочия контрольных органов<sup>6</sup>. Бизнес и граждане обеспокоены сокращением избыточного вмешательства, но это также не требует отказа от контроля как такового. Переход к мониторингу правомерного поведения, строгая специализация информационных полномочий и формализованное отделение правоохранительной стадии дают возможность одновременно повысить прозрачность финансовых процессов и уменьшить произвольность государственного вмешательства.

В конечном итоге центральной проблемой теории финансового контроля становится не поиск универсального ответа на вопрос о том, кто и кого вправе проверять, а определение правовой организации движения информации. Необходимо установить, каким образом сведения возникают и становятся доступными контролеру, по каким правилам они сопоставляются с нормативной моделью, как оформляется результат такого сопоставления, каким образом контролируемый может его оспорить и в какой юридической форме информация покидает контрольное правоотношение и становится основанием для самостоятельной правоохранительной деятельности. Именно в этой последовательности раскрывается природа контроля как обратной связи.

### Выводы

Разграничение контроля и юрисдикции в финансовой сфере имеет не терминологическое, а системное значение. Пока контроль понимается одновременно как наблюдение и наказание, невозможно последовательно определить пределы контрольной компетенции и процессуальные гарантии контролируемого. Если же контроль признать информационным отношением, становится очевидной необходимость самостоятельного юридического механизма перехода к правовосстановительным действиям. Таким механизмом и должно выступать формализованное представление, после которого информационный результат контроля получает новое процессуальное качество, а его проверка и правовая оценка осуществляются уже по правилам соответствующего правоохранительного производства.

Поэтому дальнейшее развитие финансового контроля следует связывать не с простым усилением контрольного аппарата, а с совершенствованием правовой формы обратной связи. Контроль должен сопровождать правомерное финансовое поведение, а не появляться только после его срыва; фиксировать отклонение, но не подменять собой юрисдикцию; обеспечивать государство информацией, но не превращать информационное преимущество в неограниченное властное усмотрение. В таком качестве контрольно-финансовые правоотношения способны занять самостоятельное место в системе права и стать юридической основой более точного, технологичного и одновременно гарантированного правом управления финансовыми процессами.

<sup>6</sup> Финансово-правовые аспекты и финансовая политика инновационного развития современной российской экономики : коллективная монография (Е.М. Ашмарина, Е.В. Терехова и др.). М. : Элит, 2011. 200 с. ISBN: 978-5-902405-61-0.

## Литература

1. Зырянов С.М. Государственный контроль (надзор) : монография. М. : ИЗИСП при Правительстве Российской Федерации; ООО «Юридическая фирма „Контракт“», 2023. 232 с.
2. Запольский С.В. Финансовое право России: контуры будущего : монография / С.В. Запольский, Е.Л. Васянина. М. : Директ-Медиа, 2025. 193 с.
3. Агамагомедова С.А. Теория контрольно-надзорного правоотношения: эволюция подходов и современное содержание // Журнал российского права. 2025. Т. 29. № 3. С. 105—116.
4. Андрианова Н.Г. Финансовый контроль в условиях перехода к цифровой экономике: основные проблемы и перспективы правового регулирования // Правовая информатика. 2025. № 4. С. 201—207.
5. Шохин С.О. Цифровизация в сфере государственного финансового контроля // Финансовое право. 2021. № 6. С. 7—10.
6. Система контроля в сфере государственного управления : монография / С.М. Зубарев. М. : Норма : ИНФРА-М, 2019. 150 с.
7. Кучеров И.И. Отдельные вопросы финансово-правового регулирования цифровой экономики. Цифровая валюта // Финансовое право. 2021. № 4. С. 3—7.
8. Налоговый контроль: Правовые проблемы и риски / Под ред. С.Г. Пепеляева; сост. С.А. Сосновский. М. : Статут, 2025. 400 с.
9. Публичная власть: система, компетенции : монография / М.Н. Кобзарь-Фролова, Е.Л. Васянина, Е.В. Виноградова и др. Воронеж : Научная книга, 2021. 237 с.
10. Омелехина Н.В. Цифровизация бюджетной сферы как предмет правового воздействия // Журнал российского права. 2020. № 8. С. 127—140.
11. Запольский С.В., Васянина Е.Л. Правовые вопросы цифровизации финансового контроля в России // Российский юридический журнал. 2022. № 4 (145) // СПС «КонсультантПлюс».

SECTION:  
CONSTITUTIONAL LAW

# ON THE INFORMATIONAL AND LEGAL NATURE OF FINANCIAL CONTROL

Glazunova I.V.<sup>7</sup>, Zapolsky S.V.<sup>8</sup>

**Keywords:** control, financial control, financial legal relations, information law, feedback, monitoring, lawful conduct, jurisdiction, law enforcement, submission, control procedure.

## Abstract

**The purpose** of this article is to substantiate an approach to financial control as a special type of information and legal relationship that provides feedback within the public financial management mechanism.

**Research method.** Systems analysis, conceptual modeling, formalized description, comparative legal method, documentary research method, and dogmatic legal analysis.

**Results.** The study substantiates the need to distinguish between control activities as such and jurisdictional activities: a supervisory body obtains, compares, and evaluates legally relevant information, whereas the determination of liability and the application of law-enforcement measures should fall within the competence of an administrative body, an investigative authority, or a court.

It is demonstrated that modern financial control is gradually shifting from the episodic detection of violations that have already been committed to the continuous monitoring of the lawful conduct of participants in financial relations in

<sup>7</sup> **Inessa V. Glazunova**, Ph.D. (Law), Associate Professor, Senior Researcher at the Sector of Administrative Law and Administrative Process of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia.

E-mail: [adminlaw@igpran.ru](mailto:adminlaw@igpran.ru)

<sup>8</sup> **Sergey V. Zapolsky**, Dr.Sc. (Law), Professor, Principal Researcher at the Sector of Administrative Law and Administrative Process of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia.

E-mail: [zpmoscow@mail.ru](mailto:zpmoscow@mail.ru)

*accordance with a normatively prescribed trajectory. This indicates a change in the role of financial control within the system of public administration: from a form of punitive activity to an independent mechanism for obtaining and legally processing information.*

*The legal transition from a control legal relationship to a law-enforcement relationship is delineated. This transition is effected through an independent formalized act — a submission — which records the results of the control and establishes the procedural grounds for the activities of the competent law-enforcement authority.*

*Recognizing the informational nature of control-and-financial relations, the study concludes that an independent legal mechanism is required for the transition to remedial measures. Such a mechanism may take the form of a formalized submission.*

### References

1. Zyrianov S.M. Gosudarstvennyi kontrol' (nadzor) : monografiia. M. : IZiSP pri Pravitel'stve Rossiiskoi Federatsii; OOO "Iuridicheskaia firma „Kontrakt“", 2023. 232 s.
2. Zapol'skii S.V. Finansovoe pravo Rossii: kontury budushchego : monografiia / S.V. Zapol'skii, E.L. Vasianina. M. : Direkt-Media, 2025. 193 s.
3. Agamagomedova S.A. Teoriia kontrol'no-nadzornogo pravootnosheniia: evoliutsiia podkhodov i sovremennoe soderzhanie // Zhurnal rossiiskogo prava. 2025. T. 29. No. 3. S. 105—116.
4. Andrianova N.G. Finansovyi kontrol' v usloviakh perekhoda k tsifrovoi ekonomike: osnovnye problemy i perspektivy pravovogo regulirovaniia // Pravovaia informatika. 2025. No. 4. S. 201—207.
5. Shokhin S.O. Tsifrovizatsiia v sfere gosudarstvennogo finansovogo kontroliia // Finansovoe pravo. 2021. No. 6. S. 7—10.
6. Sistema kontroliia v sfere gosudarstvennogo upravleniia : monografiia / S.M. Zubarev. M. : Norma : INFRA-M, 2019. 150 s.
7. Kucherov I.I. Otdel'nye voprosy finansovo-pravovogo regulirovaniia tsifrovoi ekonomiki. Tsifrovaia valiuta // Finansovoe pravo. 2021. No. 4. S. 3—7.
8. Nalogovyi kontrol': Pravovye problemy i riski / Pod red. S.G. Pepeliaeva; sost. S.A. Sosnovskii. M. : Statut, 2025. 400 s.
9. Publichnaia vlast': sistema, kompetentsii : monografiia / M.N. Kobzar'-Frolova, E.L. Vasianina, E.V. Vinogradova i dr. Voronezh : Nauchnaia kniga, 2021. 237 s.
10. Omelekhina N.V. Tsifrovizatsiia biudzhethnoi sfery kak predmet pravovogo vozdeistviia // Zhurnal rossiiskogo prava. 2020. No. 8. S. 127—140.
11. Zapol'skii S.V., Vasianina E.L. Pravovye voprosy tsifrovizatsii finansovogo kontroliia v Rossii // Rossiiskii iuridicheskii zhurnal. 2022. No. 4 (145) // SPS "Konsul'tantPlius".





# СОСТОЯНИЕ ЗАКОННОСТИ В СФЕРЕ БЕЗОПАСНОСТИ ДЕТЕЙ И РОЛЬ ПРОКУРАТУРЫ В ЕГО ОБЕСПЕЧЕНИИ

Ережипалиев Д.И.<sup>1</sup>

**Ключевые слова:** прокурорский надзор, законность, угрозы безопасности, несовершеннолетние, профилактика правонарушений, информационная безопасность, социальная защита, детский травматизм, правовое воспитание.

## Аннотация

**Цель работы** — на основе системного анализа состояния законности в сфере безопасности детей определить роль и направления совершенствования прокурорского надзора.

**Методологическую основу** составили общенаучные (анализ, синтез, системный подход) и частно-научные (формально-юридический, сравнительно-правовой, статистический) методы.

**Результаты исследования:** выявлены и систематизированы пять групп угроз безопасности детей (социально-экономические, физические, криминальные, информационные, ценностные); по каждой группе определены типичные нарушения законов и направления прокурорского реагирования. Обоснована роль прокурорского надзора как системообразующего инструмента выявления и устранения причин нарушений; выявлены пробелы в стратегическом планировании и предложены конкретные направления совершенствования законодательства и Стратегии комплексной безопасности детей. Обосновано, что пробелы в стратегическом планировании обусловлены недостаточной согласованностью мероприятий, показателей и механизмов межведомственного взаимодействия, а также отсутствием единых критериев оценки их результативности. Предложено совершенствовать законодательство и Стратегию комплексной безопасности детей посредством установления единых критериев оценки угроз, закрепления показателей раннего выявления девиантного, суицидального и деструктивного поведения, развития профилактики интернет-травли и распространения деструктивного контента. Также рекомендовано установить нормативы численности педагогов-психологов, единый стандарт постинтернатного сопровождения, систему учета суицидов и самоповреждений, а также четко разграничить полномочия субъектов профилактики.

DOI: 10.24412/1994-1404-2026-3-00-16

## Введение и постановка задачи

Российская Федерация признает детство важнейшим этапом развития человека и исходит из необходимости создания безопасных условий для реализации прав и законных интересов ребенка, подготовки детей к полноценной жизни в обществе, защиты их от факторов, негативно влияющих на физическое, интеллектуальное, психическое, духовное и нравственное развитие. В ч. 4 ст. 67<sup>1</sup> Конституции Российской Федерации закреплено, что дети являются важнейшим приоритетом государственной политики, для чего государство создает условия их всестороннего развития.

Правовую основу государственной политики в этой сфере составляют Конституция Российской Федерации, Федеральный закон от 24.07.1998 № 124-ФЗ «Об основ-

ных гарантиях прав ребенка в Российской Федерации»<sup>1</sup> (далее — Федеральный закон от 24.07.1998 № 124-ФЗ), Указ Президента Российской Федерации от 17.05.2023 № 358 «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года» (далее — Стратегия комплексной безопасности детей, Стратегия), а также отраслевое законодательство в сферах образования, здравоохранения, социальной защиты и профилактики безнадзорности и правонарушений несовершеннолетних.

Проведенный анализ нормативных правовых актов, регулирующих отношения в сфере обеспечения безопасности несовершеннолетних, позволяет клас-

<sup>1</sup> Собрание законодательства РФ. 1998. № 31. Ст. 3802.

<sup>1</sup> Ережипалиев Дамир Ильдарович, кандидат юридических наук, заведующий отделом научного обеспечения прокурорского надзора и укрепления законности в сфере защиты прав несовершеннолетних НИИ «Университет прокуратуры Российской Федерации», г. Москва, Россия.

E-mail: [damirastr@mail.ru](mailto:damirastr@mail.ru)

сифицировать их по сферам регулируемых отношений в соответствии с пятью блоками угроз, выделенными в Стратегии комплексной безопасности детей:

- законы, регламентирующие вопросы сбережения детей и укрепления благополучия семей (федеральные законы от 19.05.1995 № 81-ФЗ «О государственных пособиях гражданам, имеющим детей», от 22.11.1995 № 171-ФЗ «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции», от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»<sup>2</sup> и др.);
- законы о развитии безопасной инфраструктуры для детей (федеральные законы от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации» (далее — Закон о социальной защите инвалидов), от 04.12.2007 № 329-ФЗ «О физической культуре и спорте в Российской Федерации», от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»<sup>3</sup> и др.);
- законы о профилактике преступлений, совершаемых несовершеннолетними и в отношении них (федеральные законы от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних», от 06.04.2011 № 64-ФЗ «Об административном надзоре за лицами, освобожденными из мест лишения свободы», от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»<sup>4</sup> и др.);
- законы о формировании безопасной информационной среды (федеральные законы от 13.03.2006 № 38-ФЗ «О рекламе», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»<sup>5</sup> и др.);
- законы об укреплении института семьи и сохранении традиционных ценностей (Семейный кодекс Российской Федерации, от 30.12.2020 № 489-ФЗ «О молодежной политике в Российской

Федерации», от 14.07.2022 № 261-ФЗ «О российском движении детей и молодежи»<sup>6</sup> и др.).

Такая структура свидетельствует о том, что безопасность детей в законодательстве не сводится исключительно к охране от преступных посягательств, а представляет собой многоуровневую систему гарантий, охватывающих физическую, психическую, нравственную, социальную и информационную защищенность несовершеннолетних.

Однако наличие нормативных актов само по себе не гарантирует эффективности правового регулирования. Представляется важным исследование вопросов обеспечения безопасности детей именно через призму права как универсального регулятора общественных отношений, поскольку оно задает стандарты поведения, устанавливает гарантии и определяет механизмы защиты. К настоящему времени в рассматриваемой сфере сформирована правовая основа, представляющая собой совокупность взаимосвязанных, внутренне согласованных основополагающих нормативных правовых актов. Документы стратегического планирования в сфере обеспечения безопасности детей имеют большой регулятивный потенциал в качестве средства правовой политики, являясь политико-правовой доктриной, взаимосвязанной с принципами права и правовыми ценностями, формирующими правовое сознание, правовое воспитание и правовую культуру<sup>7</sup>.

Под безопасностью детей в настоящей статье понимается состояние защищенности интересов детей от внешних и внутренних угроз, при котором обеспечивается реализация их конституционных прав и свобод, достойные качество и уровень их жизни. Состояние защищенности представляет собой способность объекта безопасности сохранять свою качественную определенность и возможность выполнения своих функций и задач в условиях воздействия негативных факторов<sup>8</sup>. Как отмечает М.А. Задорина, безопасность детей в системе обеспечения национальной безопасности Российской Федерации должна быть обособлена в качестве отдельного стратегического национального приоритета и стоять на первом месте [1]. Комплексная безопасность детей является составной частью безопасности личности в целом [2], но в силу возрастных и психологических особенностей детей обуславливает необходимость специальных правовых и организационных механизмов ее обеспечения.

Реализация последовательной государственной политики в интересах детей за последние десять лет позволила наметить положительные тенденции. В 2025 г. младенческая смертность снизилась до историческо-

<sup>2</sup> Собрание законодательства РФ. 1995. № 21. Ст. 1929; Собрание законодательства РФ. 1995. № 48. Ст. 4553; Собрание законодательства РФ. 2011. № 48. Ст. 6724.

<sup>3</sup> Собрание законодательства РФ. 1994. № 35. Ст. 3648; Собрание законодательства РФ. 1995. № 48. Ст. 4563; Собрание законодательства РФ. 2007. № 50. Ст. 6242; Собрание законодательства РФ. 2012. № 53 (ч. 1). Ст. 7598.

<sup>4</sup> Собрание законодательства РФ. 1999. № 26. Ст. 3177; Собрание законодательства РФ. 2011. № 15. Ст. 2037; Собрание законодательства РФ. 2016. № 26 (ч. I). Ст. 3851.

<sup>5</sup> Собрание законодательства РФ. 2006. № 12. Ст. 1232; Собрание законодательства РФ. 2006. № 31 (ч. I). Ст. 3448; Собрание законодательства РФ. 2011. № 1. Ст. 48.

<sup>6</sup> Собрание законодательства РФ. 1996. № 1. Ст. 16; Собрание законодательства РФ. 2021. № 1 (ч. I). Ст. 28; Собрание законодательства РФ. 2022. № 29 (ч. II). Ст. 5325.

<sup>7</sup> Малько А.В., Гайворонская Я.В. Доктринальные акты как основной инструмент правовой политики // Право. Журнал Высшей школы экономики. 2018. № 1. С. 4—25.

<sup>8</sup> Прохожев А.А. Теория развития и безопасности человека и общества. М.: Ин-Октаво, 2006. 288 с.

го минимума в 3,6‰ (в 2023 г. — 4,2, в 2024 г. — 4,0)<sup>9</sup>. Смертность детей в возрасте до 17 лет с 2012 по 2025 г. снизилась на 61,5%<sup>10</sup>. Доля семей с детьми, получивших меры социальной поддержки на основании только заявления или проактивно, от общего числа семей с детьми, получивших меры социальной поддержки, составила 98,11%<sup>11</sup>. Более 150 тысяч семей обратились за помощью через семейные МФЦ, свыше 38 тысяч семей получили комплексное социальное сопровождение<sup>12</sup>. В сфере образования и оздоровления детей снижается число пострадавших при вспышках инфекционных заболеваний и пищевых отравлениях в летних лагерях (в 2023 — 619, в 2024 г. — 616, в 2025 г. — 477)<sup>13</sup>.

Однако вышеуказанные позитивные показатели не всегда отражают реальное состояние законности в сфере обеспечения безопасности детей. Анализ правоприменительной практики свидетельствует о том, что в современных условиях сохраняется комплекс угроз, систематизированных в Стратегии комплексной безопасности детей по пяти содержательным блокам: социально-экономические, физические, криминальные, информационные и ценностные. Каждый из этих блоков имеет специфические причины возникновения и требует адекватных правовых и организационных мер реагирования, причем особое место среди них занимают меры прокурорского реагирования.

Таким образом, несмотря на сформированную правовую основу и наличие позитивных статистических тенденций, состояние законности в сфере обеспечения безопасности детей требует системного научного анализа.

Цель настоящего исследования — на основе комплексного анализа состояния законности и правоприменительной практики определить роль прокурорского надзора за исполнением законов в сфере обеспечения безопасности детей и обосновать направления его совершенствования.

Достижение указанной цели предполагает решение следующих задач: выявить и систематизировать основные угрозы безопасности детей, а также типичные нарушения законности в каждой из выделенных сфер; проанализировать практику прокурорского надзора за исполнением законов в сфере обеспечения безопасности детей, определить его эффективность и пределы; установить факторы, препятствующие эффективному

осуществлению прокурорского надзора за исполнением законов в рассматриваемой сфере; выявить проблемы в стратегическом планировании и правовом регулировании, создающие условия для возникновения угроз безопасности детей; обосновать предложения по совершенствованию законодательства, Стратегии комплексной безопасности детей и организации прокурорского надзора.

Решение обозначенных задач позволит не только дать объективную оценку современного состояния законности в сфере безопасности детей, но и выработать конкретные меры, направленные на повышение эффективности прокурорского надзора и устранение системных причин нарушений прав несовершеннолетних.

### **Решение поставленной задачи**

Социально-экономические угрозы обусловлены изменениями макроэкономической обстановки, уровнем занятости и доходов населения, демографическими процессами, состоянием системы социальной поддержки семей с детьми. В последние годы состояние законности в данной сфере формировалось под влиянием инфляционных рисков<sup>14</sup>, роста потребительских цен<sup>15</sup>, тарифов на жилищно-коммунальные услуги<sup>16</sup> и проблемной задолженности по кредитам<sup>17</sup>. Именно поэтому на особом контроле у прокуроров остаются вопросы предоставления мер социальной поддержки семьям с детьми, в том числе прибывшим из воссоединенных и приграничных территорий, многодетным и малообеспеченным семьям.

Среди наиболее типичных нарушений законов в рассматриваемой сфере: отказы в назначении детских пособий из-за ненадлежащей оценки нуждаемости, неверного учета площади жилых помещений и ошибок в расчете среднедушевого дохода, в том числе из-за технических сбоев в системе межведомственного взаимодействия; непредоставление мер поддержки членам семей участников специальной военной операции; невыплата денежного довольствия членам семей с детьми безвестно отсутствующих военнослужащих.

В сфере охраны здоровья несовершеннолетних прокурорами выявляются: нецелевое расходование бюджетных средств; нехватка медицинских кадров; недостаточное оснащение медицинских организаций; нарушения порядка проведения диспансеризации детей; неинформирование медицинскими учреждениями правоохранительных органов о несовершеннолетних пациентах, в отношении которых имеются основания

<sup>9</sup> Государственная статистика ЕМИСС. URL: <https://www.fedstat.ru/indicator/61902> (дата обращения: 03.08.2026).

<sup>10</sup> Официальный сайт агентства ТАСС. URL: <https://tass.ru/obschestvo/24092303> (дата обращения: 03.08.2026).

<sup>11</sup> Доля семей с детьми, получивших меры социальной поддержки на детей на основании только заявления или проактивно. URL: <https://www.fedstat.ru/indicator/62812> (дата обращения: 03.08.2026).

<sup>12</sup> Официальный сайт «Десятилетие детства». URL: <https://10let.edu.gov.ru/novosty/pochti-150-tys-semej-poluchili-pomosch-v-semejnyh-mfts-v-2025-godu> (дата обращения: 04.08.2026).

<sup>13</sup> Число детей и подростков, пострадавших при вспышках и массовых инфекционных заболеваниях и пищевых отравлениях в летних оздоровительных учреждениях. URL: <https://www.fedstat.ru/indicator/37310> (дата обращения: 08.04.2026).

<sup>14</sup> Официальный сайт Банка России. URL: [https://cbr.ru/hd\\_base/inf/](https://cbr.ru/hd_base/inf/) (дата обращения: 04.08.2026).

<sup>15</sup> Официальный сайт Росстата. URL: <https://rosstat.gov.ru/statistics/price> (дата обращения: 04.08.2026).

<sup>16</sup> Жилищное хозяйство в России. 2025: Стат. сб. / Росстат. М., 2025. 53 с.

<sup>17</sup> Официальный сайт Банка России. URL: [https://cbr.ru/analytics/finstab ofs/2q\\_3q\\_2025/](https://cbr.ru/analytics/finstab ofs/2q_3q_2025/) (дата обращения: 04.08.2026).

полагать, что вред их здоровью причинен в результате противоправных действий.

Физические угрозы связаны с воздействием факторов, непосредственно создающих риск причинения вреда жизни и здоровью несовершеннолетних — дорожно-транспортные происшествия, пожары, падения, отравления, утопления и другие несчастные случаи.

За период с 2020 по 2024 гг. наблюдается устойчивый рост детского травматизма: общее число зарегистрированных случаев заболеваемости и смертности из-за внешних причин увеличилось на 18% (с 3,05 до 3,59 млн), показатель на 100 000 детей вырос на 20%<sup>18</sup>.

В 2025 г. в результате дорожно-транспортных происшествий погибло 792 ребенка в возрасте до 18 лет<sup>19</sup>. Такая динамика обусловлена несоответствием отдельных объектов детской инфраструктуры требованиям безопасности, недостаточным уровнем знаний детей и взрослых об основах безопасности жизнедеятельности, недостаточной эффективностью превентивного контроля со стороны уполномоченных органов. Наиболее распространенные нарушения законов в этой сфере: непринятие мер по профилактике детского травматизма; неудовлетворительное техническое состояние объектов детской инфраструктуры; несоблюдение требований пожарной безопасности, антитеррористической защищенности, санитарно-эпидемиологического законодательства; несоблюдение требований ст. 331, 351.1 Трудового кодекса Российской Федерации при приеме на работу в образовательные организации; отсутствие санитарно-эпидемиологических заключений о возможности использования пляжей для купания. Прокуроры устанавливают факты формального подхода к обеспечению антитеррористической защищенности объектов образования, отдыха и оздоровления, выявляют бесхозные спортивно-игровые площадки, пресекают деятельность несанкционированных лагерей.

Наряду с недостатками инфраструктурного и организационного характера, негативно сказывающимися на физической безопасности детей, не менее серьезную проблему представляет криминальное воздействие на несовершеннолетних. Речь идет не только о преступных посягательствах на жизнь и здоровье детей, но и о вовлечении их в противоправную деятельность, что напрямую влияет на формирование личности и долгосрочные социальные последствия. Криминальные угрозы — вовлечение несовершеннолетних в преступную деятельность и совершение преступлений в отношении детей — непосредственно посягают на жизнь, здоровье, права и законные интересы ребенка, а также создают устойчивые условия для его дальнейшей криминализации и социальной дезадаптации. Преступления, совершаемые в отношении детей

(насильственные, против половой неприкосновенности, жестокое обращение), причиняют значительный вред развитию личности ребенка.

В 2025 г. после нескольких лет снижения количество предварительно расследованных преступлений, совершенных несовершеннолетними или при их соучастии, возросло на 10,1% по сравнению с 2024 г. и составило 29 065 преступлений. Доля тяжких и особо тяжких преступлений в структуре подростковой преступности достигла 43,7% (в 2022 г. — 30,5%). Удельный вес несовершеннолетних, совершивших преступления в группе, остается стабильно высоким (в 2025 г. — 45,6%). Около трети преступлений (30,4%) совершены с использованием информационно-телекоммуникационных технологий. Отмечается рост числа преступлений, связанных с вовлечением несовершеннолетних в совершение преступления и антиобщественных действий (в 2025 г. — 1 338)<sup>20</sup>.

В 2025 г. наблюдался резкий, на 17,4%, рост выявленных прокурорами нарушений законов в сфере профилактики безнадзорности и правонарушений несовершеннолетних, что обусловлено целенаправленным усилением надзорной деятельности органов прокуратуры [3]. Прокурорами выявлялись многочисленные нарушения законов: отсутствие скоординированной деятельности по ранней профилактике, ненадлежащая индивидуально-профилактическая работа, неиспользование медиативных технологий, факты сокрытия школами случаев жестокого обращения и травли, что согласуется с выводами отдельных ученых о роли прокуратуры в противодействии насилию в образовательных организациях [4].

В условиях цифровизации общественных отношений особую актуальность приобретают информационные угрозы. Доступ несовершеннолетних к сети «Интернет» является повсеместным, при этом качество информации вызывает обоснованное беспокойство. В 2025 г. Роскомнадзор удалил или заблокировал 1,289 млн публикаций запрещенных материалов, что на 59% больше, чем годом ранее. Количество удаленных материалов со средствами обхода блокировок выросло на 1235%, с упоминанием ЛГБТ (международное общественное движение ЛГБТ признано в России экстремистским и запрещено) — на 269%, с детской порнографией — на 131%<sup>21</sup>. Сеть «Интернет» используется для вовлечения детей в диверсионную и террористическую деятельность, организацию бесконтактной торговли наркотиками, мошенничество. Информационная безопасность детей и подростков в настоящее время является ключевым предметом междисциплинарных исследований и практики, выделяются три основных направления: технологическое, социально-психоло-

<sup>18</sup> Здравоохранение в России. 2025: Стат. сб. / Росстат. М., 2025. 149 с.

<sup>19</sup> Показатели состояния безопасности дорожного движения за 2025 г. URL: <http://stat.gibdd.ru/> (дата обращения: 04.08.2026).

<sup>20</sup> Глава СК сообщил о росте преступности среди несовершеннолетних. URL: <https://www.gazeta.ru/social/news/2026/06/26/28768051.shtml> (дата обращения: 03.08.2026).

<sup>21</sup> Газета «Коммерсант». URL: <https://www.kommersant.ru/doc/8361576> (дата обращения: 03.08.2026).



гическое и общественно-политическое (нормативное) [5]. Особую озабоченность вызывает проблема детских суицидов, когда несовершеннолетние подвергаются психологической обработке в социальных сетях. Дети также вовлекаются в совершение мошеннических действий, используются в качестве дропперов для дистанционных хищений.

Описанные информационные угрозы не исчерпываются непосредственным вовлечением детей в противоправную деятельность. Не менее опасно их долгосрочное воздействие на систему ценностных ориентиров, которая находится в стадии активного формирования. Информационная среда, с которой несовершеннолетние взаимодействуют ежедневно, транслирует не только факты, но и модели поведения, жизненные приоритеты, представления о допустимом и недопустимом. В этих условиях ценностные угрозы, связанные с трансформацией системы духовно-нравственных ориентиров, определяющих процессы социализации подрастающего поколения, становятся логическим продолжением информационного вызова, но на более глубинном уровне — уровне мировоззренческих установок и социальных норм.

Ценностные угрозы связаны с трансформацией системы духовно-нравственных ориентиров, определяющих процессы социализации подрастающего поколения. В условиях глобализации и интенсивного развития цифровых коммуникаций существенно расширились каналы распространения культурных и идеологических установок. В числе негативных тенденций — снижение общественного авторитета института семьи, ослабление традиционных моделей семейного воспитания. Существенную роль в формировании установок несовершеннолетних играют популярные блогеры, транслируемые ими поведенческие практики не всегда соответствуют принципам законопослушности и социальной ответственности. В условиях обострения геополитической напряженности внешнее деструктивное воздействие может носить целенаправленный характер и использоваться как инструмент влияния на сознание несовершеннолетних.

Вместе с тем обращает на себя внимание, что в Стратегии комплексной безопасности детей отсутствуют положения, учитывающие ряд актуальных вызовов и угроз в сфере безопасности детей, возникших в современных условиях. Так, не отражена угроза безопасности детей, находящихся в зоне вооруженных конфликтов. Указанные вопросы актуализируются в условиях продолжающейся геополитической напряженности, беспрецедентного массированного санкционного давления на Россию, вооруженной агрессии и террористических актов, повлекших гибель, тяжелые ранения, физические и нравственные страдания детей на воссоединенных и приграничных территориях.

Кроме того, в Стратегии среди ключевых рисков не обозначены риски утраты ребенком родительского попечения и разлучения с родной семьей. С учетом выявляемых на практике проблем, связанных с ненадле-

жащей организацией работы с неблагополучными семьями, становится очевидным, что риски социального сиротства напрямую трансформируются в угрозы жизни, здоровью и развитию ребенка. Длительное нахождение детей в условиях семейного кризиса без системной помощи свидетельствует о недостаточности механизмов обеспечения их безопасности. Представляется, что в Стратегии должны быть отражены приоритетные меры, направленные на сохранение проживания ребенка в кровной семье, а при невозможности этого — на его семейное устройство в замещающие семьи. Однако разработанный в настоящее время перечень показателей оценки состояния безопасности детей не содержит даже такого базового индикатора, как численность детей, чьи родители лишены родительских прав, что затрудняет объективную оценку масштабов проблемы и эффективности принимаемых мер. Не учтен и другой значимый показатель — численность детей, находящихся в организациях для детей-сирот, при наличии кровных родителей, не лишенных родительских прав и сохраняющих статус законных представителей. Несмотря на признание специалистами данного явления как формы скрытого сиротства, указанная проблема фактически не получила должного отражения в стратегическом документе.

В Стратегии также не нашли отражения вопросы постинтернатного сопровождения детей-сирот и детей, оставшихся без попечения родителей, несмотря на то что данная категория лиц объективно относится к числу наиболее уязвимых с точки зрения различных видов рисков и угроз. Отсутствие эффективных механизмов социальной адаптации выпускников организаций для детей-сирот повышает риск формирования так называемого «вторичного сиротства», когда их собственные дети впоследствии оказываются в системе государственного попечения. Таким образом, недостаточное внимание к вопросам постинтернатного сопровождения фактически создает предпосылки для воспроизводства социального неблагополучия и возникновения новых угроз безопасности детей в долгосрочной перспективе.

### **Результаты исследования и выводы**

Проведенный анализ позволяет сделать вывод о том, что современное состояние законности в сфере безопасности детей в Российской Федерации характеризуется наличием комплекса взаимосвязанных угроз, каждая из которых имеет специфические причины возникновения [3]. В этих условиях прокурорский надзор за исполнением законов, осуществляемый на системной основе, является универсальным инструментом защиты публичных интересов. Наиболее действенными мерами реагирования являются те, что направлены не только на устранение конкретных нарушений, но и на вскрытие их причин. По результатам обобщения практики надзора за соблюдением прав несовершеннолетних в 2024—2025 гг. органами прокуратуры

вносились предложения о совершенствовании межведомственного взаимодействия, уточнении критериев оценки эффективности профилактической работы, о дополнительном нормативном регулировании порядка ограничения доступа несовершеннолетних к деструктивному контенту. Прокурорский надзор за исполнением законов в социальной сфере приобретает характер стратегического ресурса государства по защите прав граждан, особенно в части, касающейся уязвимых категорий населения [6]. Эффективность работы органов прокуратуры зависит от взаимодействия с иными правоохранительными органами, что подтверждается анализом практики [7].

К числу приоритетных направлений повышения эффективности прокурорского надзора за исполнением законов в рассматриваемой сфере можно отнести: усиление межведомственного взаимодействия органов прокуратуры с субъектами системы профилактики безнадзорности и правонарушений несовершеннолетних, в том числе на основе единых информационных платформ; развитие цифровых инструментов мониторинга состояния законности, включая автоматизированный анализ обращений граждан и данных ведомственной статистики; совершенствование методик оценки результативности надзора, переход от оценки исключительно количественных показателей к анализу реального восстановления прав несовершеннолетних; повышение требований к профессиональной подготовке прокурорских работников с учетом динамично меняющегося характера угроз.

Кроме того, выявленные пробелы в Стратегии комплексной безопасности детей обуславливают необходимость ее дополнения в части: закрепления мер по защите детей, находящихся в зоне вооруженных конфликтов; включения профилактики социального сиротства и сохранения ребенка в кровной семье в число приоритетных направлений; развития системы постинтернатного сопровождения выпускников организаций для детей-сирот; расширения перечня показателей оценки состояния безопасности детей за счёт включения численности детей, чьи родители лишены или ограничены в родительских правах, доли детей, находящихся в организациях для детей-сирот, а также доли выпускников, охваченных постинтернатным сопровождением.

К приоритетным направлениям совершенствования правового регулирования также следует отнести: установление нормативов штатной численности педагогов-психологов в образовательных организациях с учетом количества обучающихся и особенностей контингента; разработку и утверждение на федеральном уровне единого стандарта постинтернатного сопровождения, предусматривающего единые подходы к оказанию социальной, психологической и правовой помощи выпускникам; нормативное закрепление обязанности образовательных организаций и педагогических работников по обеспечению информационной безопасности несовершеннолетних обучающихся [8];

формирование комплексной системы профилактики травли, включая травлю в сети «Интернет», с закреплением соответствующих обязанностей образовательных организаций и иных субъектов профилактики; совершенствование механизмов раннего выявления девиантного, суицидального и деструктивного поведения несовершеннолетних, в том числе путем развития нормативной базы применения психодиагностических методик; разработку и нормативное закрепление системы учета суицидов несовершеннолетних, их попыток и самоповреждающего поведения, включая формирование единого реестра таких случаев [9]; совершенствование механизмов противодействия распространению среди несовершеннолетних деструктивного контента в сети «Интернет», в том числе связанного с пропагандой насилия, школьных нападения, саморазрушающего поведения; дальнейшее развитие правового регулирования в сфере культуры, в том числе путем уточнения полномочий федеральных органов государственной власти по разработке и реализации государственной культурной политики, осуществляемой в соответствии с традиционными российскими духовно-нравственными ценностями.

Таким образом, в Российской Федерации сформирована правовая основа и система организационных мер, направленных на обеспечение безопасности детей [10]. За последние годы достигнуты значимые позитивные результаты в сфере снижения младенческой и детской смертности, расширения охвата социальной поддержкой семей с детьми. Вместе с тем состояние законности характеризуется наличием комплекса взаимосвязанных угроз, систематизированных по пяти блокам. Прокурорский надзор за исполнением законов в этой сфере является универсальным механизмом, позволяющим не только выявлять и пресекать конкретные нарушения, но и вскрывать их причины, инициировать совершенствование законодательства и правоприменительной практики. Рост выявленных нарушений законов в рассматриваемой сфере в 2025 г. свидетельствует не столько об ухудшении ситуации, сколько о целенаправленном усилении надзорной деятельности. Перспективными направлениями совершенствования прокурорского надзора на данном участке являются развитие межведомственного взаимодействия, внедрение цифровых инструментов мониторинга, совершенствование методик оценки результативности, а также повышение профессиональной подготовки прокурорских работников с учетом динамично меняющегося характера угроз безопасности детей.

## Литература

1. Задорина М.А. Безопасность детей и ее место в системе обеспечения национальной безопасности // Национальная безопасность / nota bene. 2022. № 6. С. 152—163.
2. Колоткина О.А., Ягофарова И.Д. Комплексная безопасность детей — новый вид национальной безопасности в системе стратегического планирования // Актуальные проблемы государства и права. 2023. Т. 7. № 3. С. 450—457. DOI: 10.20310/2587-9340-2023-7-3-450-457.
3. Дымолазов В.С. Актуальные направления прокурорского надзора за соблюдением прав несовершеннолетних (на примере Новосибирской области) // Ex jure. 2025. № 2. С. 53—63.
4. Грачева О.А., Авдоница Т.М. Роль органов прокуратуры в противодействии насилию в образовательных организациях // Проблемы права. 2026. № 1. С. 538—542.
5. Сорокин П.А., Бочавер А.А. Информационная безопасность детей и подростков в мире: характеристика основных направлений исследований и научно-практических разработок // Психология и право. 2026. Т. 16. № 2. С. 118—131.
6. Ергашев Е.Р., Асоян К.А. О современных проблемах представления, применяемого при осуществлении надзорной функции прокуратуры // Российское право: образование, практика, наука. 2022. № 4. С. 23—31.
7. Юхнова В.А. Защита прав несовершеннолетних граждан Российской Федерации органами прокуратуры: проблемы реализации // Российское право: образование, практика, наука. 2025. Т. 8. № 2. С. 71—75.
8. Лебедев В.Н., Моренко К.В. Направления деятельности прокуратуры Российской Федерации в сфере обеспечения информационной безопасности государства // Правовая информатика. 2026. № 2. С. 280—289.
9. Струков В.Н. Проблемы расследования детоубийств и пути их решения // Мониторинг правоприменения. 2026. № 2 (59). С. 173—176.
10. Карчевская Н.И. К вопросу становления правовой защиты конституционных основ общественной безопасности. // Мониторинг правоприменения. 2026. № 1 (58). С. 26—32.

**SECTION:**  
CONSTITUTIONAL LAW

# THE STATE OF LEGALITY IN THE SPHERE OF CHILD SAFETY AND THE ROLE OF THE PROSECUTOR'S OFFICE IN ITS ENSURING

Erezhipaliev D.I.<sup>22</sup>

**Keywords:** child safety, prosecutorial supervision, legality, security threats, minors, crime prevention, information security, social protection, child injuries, legal education.

## Abstract

**The purpose of the work** is to determine the role and directions for improving prosecutorial supervision based on a systematic analysis of the state of legality in the sphere of child safety.

**Research methods:** basis comprises general scientific methods (analysis, synthesis, systems approach) and specific scientific methods (formal legal, comparative legal, statistical).

**Results of the study:** Five groups of threats to child safety are identified and systematized (socio-economic, physical, criminal, informational, value-based); for each group, typical violations of laws and directions of prosecutorial response are identified; the role of prosecutorial supervision as a system-forming tool for identifying and eliminating the causes of violations is substantiated; gaps in strategic planning are identified and specific directions for improving legislation and the Comprehensive Child Safety Strategy are proposed.

<sup>22</sup> **Damir I. Erezhipaliev**, Ph.D. (Law), Head of the Department for Scientific Support of Prosecutorial Supervision and Strengthening of Legality in the Sphere of Protection of the Rights of Minors of the Research Institute of the University of the Prosecutor's Office of the Russian Federation, Moscow, Russia.

E-mail: [damirastr@mail.ru](mailto:damirastr@mail.ru)

## References

1. Zadorina M.A. Bezopasnost' detei i ee mesto v sisteme obespecheniia natsional'noi bezopasnosti // Natsional'naia bezopasnost' / nota bene. 2022. No. 6. S. 152—163.
2. Kolotkina O.A., Iagofarova I.D. Kompleksnaia bezopasnost' detei — novyi vid natsional'noi bezopasnosti v sisteme strategicheskogo planirovaniia // Aktual'nye problemy gosudarstva i prava. 2023. T. 7. No. 3. S. 450—457. DOI: 10.20310/2587-9340-2023-7-3-450-457.
3. Dymolazov V.S. Aktual'nye napravleniia prokurorskogo nadzora za sobliudeniem prav nesovershennoletnikh (na primere Novosibirskoi oblasti) // Ex iure. 2025. No. 2. S. 53—63.
4. Gracheva O.A., Avdonina T.M. Rol' organov prokuratury v protivodeistvii nasiliia v obrazovatel'nykh organizatsiiakh // Problemy prava. 2026. No. 1. S. 538—542.
5. Sorokin P.A., Bocharov A.A. Informatsionnaia bezopasnost' detei i podrostkov v mire: kharakteristika osnovnykh napravlenii issledovaniia i nauchno-prakticheskikh razrabotok // Psikhologiya i pravo. 2026. T. 16. No. 2. S. 118—131.
6. Ergashev E.R., Asoian K.A. O sovremennykh problemakh predstavleniia, primeniaemogo pri osushchestvlenii nadzornoj funktsii prokuratury // Rossiiskoe pravo: obrazovanie, praktika, nauka. 2022. No. 4. S. 23—31.
7. Iukhnova V.A. Zashchita prav nesovershennoletnikh grazhdan Rossiiskoi Federatsii organami prokuratury: problemy realizatsii // Rossiiskoe pravo: obrazovanie, praktika, nauka. 2025. T. 8. No. 2. S. 71—75.
8. Lebedev V.N., Morenko K.V. Napravleniia deiatel'nosti prokuratury Rossiiskoi Federatsii v sfere obespecheniia informatsionnoi bezopasnosti gosudarstva // Pravovaia informatika. 2026. No. 2. S. 280—289.
9. Strukov V.N. Problemy rassledovaniia detoubiistv i puti ikh resheniia // Monitoring pravoprimeneniia. 2026. No. 2 (59). S. 173—176.
10. Karchevskaia N.I. K voprosu stanovleniia pravovoi zashchity konstitutsionnykh osnov obshchestvennoi bezopasnosti // Monitoring pravoprimeneniia. 2026. No. 1 (58). S. 26—32.





# ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ И РАЗВИТИЯ ТАКТИКИ НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ ПРОКУРАТУРЫ

Махьянова Р.М.<sup>1</sup>

**Ключевые слова:** прокурорские проверки, методики проверок, элементы тактики, тактическое мышление, ситуационный подход, принятие решений, профессиональная компетентность, организационно-распорядительные документы, цифровизация, искусственный интеллект, классификация предпосылок.

## Аннотация

**Цель работы:** на основе результатов, полученных в ходе ранее проведенного исследования, выявить и систематизировать предпосылки использования тактики в надзорной деятельности прокуратуры, определить основания их классификации и обозначить направления дальнейшего совершенствования прокурорского надзора.

**Методы исследования:** анализ, обобщение и систематизация научной и методической литературы, законодательства и организационно-распорядительных документов прокуратуры, а также классификация выявленных предпосылок использования тактики надзорной деятельности.

**Результаты исследования:** выявлены и систематизированы предпосылки разработки и реализации тактики на различных стадиях надзорной деятельности прокуратуры, содержащиеся в законодательных актах, организационно-распорядительных документах органов прокуратуры, научной и методической литературе по прокурорскому надзору. На основе комплексного анализа разноплановых научно-практических источников определены основания классификации выявленных предпосылок. В качестве их основы определены условия, способствующие проведению ситуационного анализа, поиску, разработке и реализации решений в ходе организации и проведения проверок вне уголовно-правовой сферы. Кроме того, обозначены основные направления дальнейшего развития надзорной деятельности прокуратуры и её тактического обеспечения, включая развитие теоретических положений, уточнение и разработку понятийного аппарата, цифровизацию и тактическое моделирование надзорной деятельности, составление методик на основе ситуационного подхода.

DOI: 10.24412/1994-1404-2026-3-00-17

## Введение

Развитие общества и государства предполагает использование современных подходов к осуществлению надзорной деятельности прокуратуры. Внедрение тактики в содержание надзорного процесса в качестве обеспечительной основы его результативности и эффективности потребует от прокуроров применения знаний из различных научных областей, цифровых технологий, систематического повышения уровня их профессиональной компетентности.

Надзорная функция прокуратуры напрямую сопряжена с охраной и защитой законных прав и интересов граждан, обеспечением верховенства закона, что в значительной степени повышает уровень требований, предъявляемых к ее реализации. Практическое использование тактики позволит усовершенствовать ее содержание и оптимизировать процесс преобразования надзорной деятельности прокуратуры.

В настоящее время в научной литературе отсутствуют единые доктринальные положения о сущности и содержании тактики надзорной деятельности прокуратуры, что создает трудности для ее практического применения и последующего развития. Решение указанной проблемы требует комплексного подхода, позволяющего установить обстоятельства, способствующие поиску, разработке и реализации решений при организации и проведении прокурорских проверок вне уголовно-правовой сферы.

Прежде чем перейти к освещению основной части, представляется целесообразным изложить некоторые выводы, полученные в процессе ранее проведенных научных изысканий в данной области в целях объективного понимания исследуемой темы.

Тактика используется в профессиональной и иной деятельности в качестве прикладного инструмента

<sup>1</sup> **Махьянова Римма Мубаракновна**, кандидат юридических наук, доцент, доцент Военного университета им. князя Александра Невского Министерства обороны Российской Федерации, г. Москва, Россия.  
E-mail: [r@9099177842.ru](mailto:r@9099177842.ru)

для выполнения поставленных целей и задач наиболее оптимальными способами. Ее основное предназначение заключается в осуществлении целенаправленного поиска в двух основных направлениях: во-первых, идей в целях разработки оригинальных методов, решений, а во-вторых, для выбора имеющихся средств применительно к динамическим обстоятельствам конкретной ситуации.

Применение тактики позволяет достигать промежуточных целей при условии наличия стратегических, или конечных целей. Результаты анализа использования тактики в различных сферах деятельности позволили выявить закономерности ее разработки и реализации [1], способствующие проведению дальнейших теоретических исследований в области тактики, определения ее места среди фундаментальных или прикладных наук. Тактика требует от субъекта ее разработки и реализации проявления развитых интеллектуальных способностей, в частности, тактического мышления [2], навыка и опыта осуществлять конкретную деятельность, научных знаний из различных областей, в том числе, которые используются применительно к предмету тактического сопровождения, а также фундаментальных наук, и применения научных и практических методов; проведения всестороннего ситуационного анализа (постоянного мониторинга (наблюдения) обстоятельств ситуации в динамике), прогнозирования и оценки условий, событий и влияющих на них факторов в целях выработки решения. Разработка и реализация тактики имеют свои особенности, связанные с уточнением, детализацией [3]<sup>2</sup>, постоянным изучением и сравнением всех обстоятельств, охваченных ситуацией для достижения тактического эффекта. Анализ различных источников об использовании тактики в профессиональной и иной деятельности дает основание полагать, что определения понятия «тактика» сформулированы таким образом, что не в полной мере отражают ее сущность и содержание [4]<sup>3</sup>.

В настоящее время в научно-практической литературе в основном преобладают труды, связанные с разработкой конкретных методик осуществления деятельности в конкретной сфере без раскрытия сущностного содержания тактики. В юриспруденции наиболее исследованными являются криминалистическая и следственная тактика, знания которых могут быть использованы в ходе тактического обеспечения профессиональной деятельности, в том числе надзорной, с учетом специфики организации и деятельности прокуратуры.

Разработаны элементы тактики, составляющие в своей совокупности единый механизм (систему [5]<sup>4</sup>), в котором объединены теоретические и практические основы тактики, раскрывающие ее содержание. Указанный механизм [4] работает по принципу алгоритмической конструкции — следование, ветвление и цикл [5] в зависимости от динамики надзорных ситуаций, складывающихся в пределах стадий надзорной деятельности. В целях оптимизации указанного процесса и снабжения элементов тактики актуальными сведениями, видится логичным ведение учета надзорных характеристик (объект — субъект — предмет надзора), отражающих результаты надзорной деятельности в динамике по принципу «было — стало».

Кроме того, ввиду большого массива информации, получаемой в ходе проверки, которая подлежит тщательной переработке и хранению, применение тактики способствует активному внедрению цифровых технологий в надзорную деятельность прокуратуры. Это позволит не только принимать обоснованные тактические решения с учетом автоматизированного анализа всех надзорных характеристик, но и выявлять проблемы прокурорско-надзорного процесса, связанные с его качеством и особенностями специфики предмета надзора и деятельности их объектов и субъектов, а также осуществлять рациональное планирование надзорных мероприятий, владеть объективными сведениями о состоянии законности.

Ведение электронного учета надзорных характеристик будет способствовать развитию междисциплинарных связей внутри органов прокуратуры, обеспечивать, при этом, эффективность иной прокурорской деятельности, например, правотворческой, обеспечения участия прокуроров в рассмотрении судами дел и др.

Системный, межпредметный подход к организации и осуществлению надзорной деятельности, его цифровизация позволяют во многом совершенствовать деятельность прокурора, предоставлять новые возможности для повышения эффективности прокурорского надзора и опыта профессиональной деятельности.

Ученые подчеркивают актуальность такого направления развития надзорной деятельности и отмечают, что «современные информационные технологии стали неотъемлемой частью служебной деятельности прокуроров. Прокуроры должны ориентироваться в электронном общественном пространстве. По-другому уже невозможно надзирать. Требуется научиться давать оценку нарушениям и реагировать на них по-новому» [6].

В некоторых трудах обоснованно отмечается, что «проведение цифровизации в органах и организациях отечественной прокуратуры не может быть оторвано от аналогичного процесса в других государственных органах [7]».

<sup>2</sup> Махьянова Р.М. Тактический аспект надзорной деятельности органов прокуратуры : монография. М. : Военный университет им. князя Александра Невского Минобороны России, 2022. 170 с. ISBN 978-5-6048563-8-3.

<sup>3</sup> Махьянова Р.М. Тактическое обеспечение надзорной деятельности органов прокуратуры : монография. М. : Военный университет им. князя Александра Невского Минобороны России, 2022. 202 с. ISBN 978-5-6048563-9-0.

<sup>4</sup> Толковый словарь государственного языка Российской Федерации (разработчик — ФГБОУ ВО «Санкт-Петербургский государственный университет»): утв. Распоряжением Правительства РФ от 30.04.2025 № 1102-р. С. 323.

Цифровая трансформация наблюдается в государственном управлении [8], в органах прокуратуры Российской Федерации намечены стратегические задачи по формированию «высокотехнологичного надзора» [9]<sup>5</sup>.

Важно подчеркнуть, что электронный обмен сведениями о состоянии законности, постоянный мониторинг надзорной практики и ее анализ предполагают обработку значительного объема соответствующих документов.

Ученые и практики отмечают, что стратегические цели цифровой трансформации прокуратуры заключаются в автоматизации аналитических процессов [10], тем самым перед прокурором откроются новые перспективы для самообучения, получения нового профессионального опыта.

Процесс разработки тактики, в основе которого лежит поиск, базирующийся не только на нормах прокурорского права, но и требующий научных знаний, возможно, тех, которые не были предметом изучения в высшем учебном заведении и на курсах повышения квалификации прокурорских работников. В этой связи требуется переосмысление вопросов о подготовке кадров для органов прокуратуры, введение новых дисциплин, связанных с цифровизацией надзорной деятельности прокуратуры, изучение которых будет способствовать повышению качества переподготовки прокурорских работников.

Данный вывод поддержан в трудах ученых [11].

Поскольку тактика требовательна к детальности любой информации и совершаемых действий в ходе ее разработки и реализации, то основным камнем преткновения в указанном процессе является недостаточность правового регулирования прокурорско-надзорного процесса, о чем также отмечено в научных работах<sup>6</sup>. Кроме того, отсутствие терминологического аппарата в базовом законодательстве о прокурорском надзоре не позволяет правильно трактовать некоторые термины, что негативно сказывается на качестве надзорной деятельности и ее развитии.

<sup>5</sup> Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2030 года, а также о внесении изменений в отдельные организационно-распорядительные документы Генерального прокурора Российской Федерации: Приказ Генпрокуратуры России от 11.09.2025 № 621 // Законность. № 11. 2025.

<sup>6</sup> Берензон А.Д., Мелкумов В.Г. Работа прокурора по общему надзору. М., 1974. С. 5; Николаева Л.А. Прокуратура и законность в советском государственном управлении. Л., 1978; Долежан В.В., Тарнавский Г.С. Прокурорский надзор за исполнением законов в сельском хозяйстве: методич. пос. М., 1986; Бойцова В.В. Роль общего надзора прокуратуры в укреплении правовой основы государственного управления: дис. ... канд. юрид. наук: 12.00.02 / Гос. Санкт-Петербург. ун-т. СПб., 1991. С. 160; Ломовский В.Д. Прокурорско-надзорный процесс: уч. пос.; М-во общ. и проф. образования РФ. Твер. гос. ун-т. Тверь: ТГУ, 1997. 111 с. Субанова Н.В. Теоретические и прикладные основы прокурорского надзора за исполнением законов о разрешительной систем: дис. ... докт. юрид. наук: 12.00.11, 12.00.14; [Место защиты: Акад. Генер. прокуратуры РФ]. М., 2014. С. 253; Ергашев Е.Р. Актуальные проблемы организации и деятельности прокуратуры Российской Федерации: монография. Екатеринбург. 2023. С. 83, 84.

Опыт надзорной практики позволяет выделить надзорную деятельность в систему, состоящую из последовательных стадий, тактическое обеспечение которых осуществляется путем встраивания в них элементов тактики, что предполагает: 1) более тщательное правовое регулирование прокурорско-надзорного процесса; 2) получение объективной и разносторонней информации, обусловленной предметом надзора, а также спецификой деятельности объекта (субъекта) надзора; 3) вовлечение тех научных и практических методов, применение которых в конкретной ситуации позволит получить результат и тактический эффект; 4) определение основных компонентов прокурорско-надзорного процесса в целях повышения его качества; 5) достижение предупредительного эффекта и результативности надзорной деятельности, выражающихся в выполнении конкретных целей и задач каждой ее стадии; 6) совершенствование профессионализма прокурорских работников; 7) обновление теории и практики прокурорского надзора; 8) обеспечение верховенства закона и укрепление российской государственности.

Тактика является не только одним из основных модернизационных инструментов надзорной деятельности, но и неотъемлемым элементом ее организации и осуществления на научной основе.

## **Основная часть**

С учетом обоснований внедрения тактики в надзорную деятельность прокуратуры, изложенных выше, настоящее исследование показало, что выявлению предпосылок для разработки и реализации тактики надзорной деятельности прокуратуры послужило содержание определения ее понятия, сформулированное автором.

Под *тактикой надзорной деятельности прокуратуры* понимаются поиск, разработка и реализация решений на основе оценки результатов анализа надзорных ситуаций, складывающихся на стадиях организации и проведения проверок, принятия мер прокурорского реагирования и контроля за выполнением требований прокурора.

Организационные и управленческие решения прокурора требуют проведения всестороннего ситуационного анализа, обусловливаемого предметом проверки и деятельностью поднадзорных объектов и субъектов.

Термином «надзорная ситуация» охватывается, в том числе, состояние законности, которое формируется за счет надзорных характеристик, полученных прокурорами по результатам проведенных проверок по направлениям надзора.

Исходя из содержания вышеприведенного понятия, необходимо подчеркнуть, что поиск решений о способах действий, методах, целесообразных средствах выявления, устранения и предупреждения нарушений закона, причин и условий им способствующих предполагает, в том числе, их выбор в зависимости от наличия таковых (в науке, практике, законодательстве),

исходя из анализа обстоятельств надзорной ситуации. Разработка новых методов и приемов осуществляется прокурорским работником путем использования его интеллектуальных возможностей, знаний и профессионального опыта.

В прошлом и нынешнем времени учеными сформулированы различные определения понятий тактики прокурорского надзора, но не одно из них не раскрывает ее сущностное содержание по причине отсутствия проведенных теоретических разработок. На наш взгляд, это является одной из проблем ее практической реализации и развития.

Ретроспективный анализ правовых норм об организации и деятельности органов прокуратуры позволяет выделить *историко-правовые предпосылки* применения тактики в ходе прокурорского надзора. В правовых документах содержатся нормы, создающие условия к поиску и выбору решений на основе анализа информационных сведений о состоянии законности, полученных в ходе наблюдения за деятельностью объектов и должностных лиц, поднадзорных прокурору.

Несмотря на то, что термин «тактика» отсутствует в советском и современном законодательстве, регламентирующем вопросы прокурорского надзора, условия для разработки и реализации тактики, целесообразность его практического использования прослеживаются по смыслу правовых норм, их практической реализации в ходе надзорной деятельности.

Одно из первых упоминаний о применении тактики в целях достижения эффективности прокурорского надзора и обеспечения надлежащего уровня состояния законности в войсках содержится в:

1) Инструкции «Военным прокурорам по осуществлению общего надзора за исполнением законов», утвержденной Прокурором СССР 29 июня 1938 года (далее — Инструкция<sup>7</sup>);

2) Наставлении военному прокурору морского и речного флота по надзору за соблюдением социалистической законности при применении уставов о дисциплине рабочих и служащих морского и речного флота Союза ССР<sup>8</sup> (далее — Наставление).

Так, в статье 15 раздела Инструкции «Методы общего надзора» военным прокурорам предписывалось проявлять инициативу в изыскании способов раскрытия и устранения нарушений закона.

Согласно положениям § 61 Наставления, оценка работы военного прокурора производилась исходя не только из количества и обоснованности его протестов на незаконные приказы и представлений об устранении отрицательных явлений, но и потому, насколько

военный прокурор был оперативен в принятии мер к восстановлению нарушенной законности, настойчив в осуществлении своих мероприятий.

Указанные требования организационно-распорядительных документов подчеркивают важность изучения и анализа обстановки на поднадзорных объектах в целях принятия решений и планирования надзорных мероприятий, требуют проявления профессиональной компетентности, действенности при достижении конечных результатов прокурорского надзора.

Положениями советского законодательства на прокуратуру, кроме надзора за деятельностью поднадзорных объектов, возлагалось непосредственное наблюдение за деятельностью следственных органов дознания в области раскрытия преступлений, за правильностью содержания заключенных под стражей, а также за деятельностью органов Государственного Политического Управления.

Кроме того, руководство и наблюдение возлагались на Прокурора Республики за деятельностью Помощников Прокурора Республики, а также Прокуроров, их Помощников на местах и дача им разъяснений и указаний по всем возникающим в их деятельности вопросам<sup>9</sup>. Прокурор должен был представлять каждые 3 месяца отчет о деятельности своей и своих Помощников Прокурору Республики и в Губернский Исполнительный Комитет.

Метод наблюдения применительно к объектам надзора реализуется, в том числе, для сбора информации о состоянии законности, их анализа в целях поиска и принятия организационных и управленческих решений — о немедленном вмешательстве прокурора и проведении проверки, планировании надзорной деятельности, оценке ее эффективности, определении проблемных вопросов и выработке основных направлений их решения. Кроме того, согласно нормам упомянутого законодательного акта, изучалась и анализировалась деятельность прокурорских работников, что способствовало оценке уровня их профессиональной компетентности.

К несомненным достоинствам советского законодательства о прокурорском надзоре можно отнести разнообразие мер реагирования, подлежащих выбору при определенных обстоятельствах надзорной ситуации.

Например, письменное предписание прокурора об устранении нарушений закона подлежало немедленному исполнению<sup>10</sup>, что в значительной степени повышало эффективность надзорной деятельности и сокращало путь к достижению предупредительного эффекта.

<sup>7</sup> Инструкция Военным прокурорам по осуществлению общего надзора за исполнением законов (Прокуратура Союза ССР. Главная военная прокуратура): утверждена прокурором СССР А. Вышинским 29 июня 1938 года.

<sup>8</sup> Наставление военному прокурору морского и речного флота по надзору за соблюдением социалистической законности при применении уставов о дисциплине рабочих и служащих морского и речного флота Союза ССР. М., 1944.

<sup>9</sup> Положение о прокурорском надзоре: постановление ВЦИК от 28.05.1922 // СУ РСФСР. 1922. № 36. Ст. 424; Известия ВЦИК. № 132. 16.06.1922. Документ утратил силу в связи с изданием Постановления ВЦИК, СНК РСФСР от 25.01.1928.

<sup>10</sup> О прокуратуре СССР: Закон СССР от 30.11.1979 № 1162-X (ред. от 07.01.1988) // Первоначальный текст документа опубликован в издании «Ведомости ВС СССР». 1979. № 49. Ст. 843. Ст. 24.1.



Акты реагирования должны обладать превентивным действием; а если он не достигается, то можно предположить следующее: несоответствие его характеру выявленных нарушений закона; не проведение комплексного сравнительного анализа надзорных характеристик объекта (субъекта) надзора, и, как следствие, отсутствие поиска решений, игнорирование разработки и реализации тактики на стадии устранения выявленных нарушений закона; ненадлежащее исполнение прокурором своих обязанностей, выразившееся в отсутствии принципиальной позиции в части удовлетворения требований, изложенных в документах реагирования.

Современное законодательство о прокурорском надзоре также содержит предпосылки к использованию тактики, в частности — полномочия прокурора, изучение состояния законности, всестороннее изучение ситуации, складывающейся при осуществлении надзорной деятельности в целях разработки и (или) выбора рационального правового средства, направленного на выявление, устранение, предупреждение нарушений законности, причин и условий их способствующих. Также предусмотрена ответственность за невыполнение требований прокурора, которая подлежит тактической корректировке во взаимосвязи с результатами анализа надзорной ситуации и сравнительного анализа надзорных характеристик объекта (субъекта) надзора.

На анализ обстановки, раскрывающей состояние законности в целях принятия решений об использовании прокурорами рациональных правовых средств, обращено внимание в ряде документов Генерального прокурора Российской Федерации и базовых законах об организации и деятельности органов прокуратуры.

Так, в действовавшем ранее приказе Генпрокуратуры России от 21.06.2013 № 252 «О совершенствовании прокурорского надзора за исполнением федерального законодательства органами государственной власти, местного самоуправления, иными органами и организациями» (п. 3.7)<sup>11</sup> прокурорам предписывалось при внесении актов реагирования обеспечить неукоснительное выполнение требований Приказа Генерального прокурора Российской Федерации от 07.12.2007 № 195 «Об организации прокурорского надзора за исполнением законов, соблюдением прав и свобод человека и гражданина», всесторонне и объективно оценивать ситуацию, возможные негативные последствия исполнения требований прокурора, руководствоваться принципом защиты законных прав человека и гражданина.

Анализ ситуации о состоянии законности важен не только для принятия решений в ходе тактического обеспечения надзорной деятельности, но и для плани-

рования, о чем указано в Регламенте Генеральной прокуратуры Российской Федерации<sup>12</sup>.

Вопросы изучения состояния законности на поднадзорных объектах регламентированы нормами советского законодательства<sup>13</sup>.

Согласно положениям действующего законодательства, «органы прокуратуры информируют федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы публичной власти федеральных территорий, органы местного самоуправления, а также население о состоянии законности»<sup>14</sup>.

Генеральный прокурор Российской Федерации ежегодно представляет палатам Федерального Собрания Российской Федерации и Президенту Российской Федерации доклад о состоянии законности и правопорядка в Российской Федерации и о проделанной работе по их укреплению<sup>15</sup>.

*Научные предпосылки* разработки и использования тактики при проведении прокурорских проверок, выявленные в научной литературе, носят более конкретный, а в некоторых случаях утвердительный характер.

Вопросы применения научной организации труда актуальны для советской<sup>16</sup> и современной прокуратуры<sup>17</sup>.

Сущность научной организации труда фактически сводится к экономии труда и времени и представляет собой процесс совершенствования организации труда путем ее обновления новыми направлениями, разработанными наукой и практикой в целях повышения продуктивности труда.

Вызывает интерес предложенный для применения в практической деятельности метод качественного учета сотрудников. Суть данного метода состоит в оценке качеств сотрудника руководителем на основании

<sup>12</sup> Об утверждении Регламента Генеральной прокуратуры Российской Федерации: приказ Генпрокуратуры России от 11.05.2016 № 276 // Первоначальный текст документа опубликован в издании «Законность». № 8. 2016.

<sup>13</sup> О прокуратуре СССР: закон СССР от 30.11.1979 № 1162-X, ст. 23 // Первоначальный текст документа опубликован в издании «Ведомости ВС СССР». 1979. № 49. Ст. 843.

<sup>14</sup> О прокуратуре Российской Федерации: федеральный закон от 17.01.1992 № 2202-1. Пункт 2. Статья 4 // Собр. законодательства Рос. Федерации. 20.11.1995. № 47. Ст. 4472; Российская газета. № 229. 25.11.1995.

<sup>15</sup> Там же. Пункт 7. Статья 12.

<sup>16</sup> Берензон А.Д. О структуре теории советского прокурорского надзора // Проблемы прокурорского надзора. Научная конференция, посвященная 50-летию советской прокуратуры: тезисы сообщений. 20—21 апреля 1972 г. М., 1972. С. 25; Добровольская Т.Н. Прокурорский надзор как одно из средств обеспечения социалистической законности // Проблемы прокурорского надзора. Научная конференция: тезисы сообщений. 20—21 апреля 1972 г. М., 1972. С. 30—33.

<sup>17</sup> О системе подготовки кадров, дополнительного профессионального образования работников органов и организаций прокуратуры Российской Федерации: приказ Генпрокуратуры России от 22.12.2021 № 774 // Первоначальный текст документа опубликован в изданиях: «Законность». № 2. 2022 (Приказ); «Законность». № 3. 2022 (Приложение). Абз. 4. П. 2.4.

<sup>11</sup> О совершенствовании прокурорского надзора за исполнением федерального законодательства органами государственной власти, местного самоуправления, иными органами и организациями: Приказ Генпрокуратуры России от 21.06.2013 № 252 / Документ опубликован не был и утратил силу в связи с изданием Приказа Генпрокуратуры России от 02.08.2022. № 421. П. 3.7.

сравнимых данных о нем (схемы служебной и психологической оценки сотрудника)<sup>18</sup>.

Некоторые ученые отмечали взаимосвязь поиска новых форм прокурорской деятельности с тактикой общего надзора, способствующей выбору наиболее эффективных средств выполнения поставленных перед прокуратурой задач в конкретный период времени<sup>19</sup>.

В научных трудах советского времени подчеркивалась необходимость разработки проблемных вопросов тактики прокурорского надзора<sup>20</sup>.

О необходимости разрешения научной проблемы путем проведения теоретической разработки тактики надзора отражено в трудах советских ученых. По их мнению, разработка тактики будет способствовать мобильному использованию прокурорских кадров и более действенному осуществлению надзора<sup>21</sup>.

Современными учеными и практиками актуализируется вопрос о проведении теоретических разработок тактики прокурорского надзора, в том числе<sup>22</sup>, в целях решения научной проблемы и повышения эффективности надзорной деятельности прокуратуры<sup>23</sup>.

Коллектив советских ученых обозначил более четкие границы такого исследования, отметив необходимость формирования понятийного аппарата тактики общенадзорной деятельности, ее понятия, задачи, принципы, предмет и др.<sup>24</sup>

В своем коллективном труде ученые обосновывают необходимость разработки тактических аспектов общего надзора, в том числе, понятийного аппарата тактики общенадзорной деятельности, включающего в себя понятия тактики, надзорной ситуации, предмета тактики, тактических приемов. В этих целях предлагается использовать знания из криминалистической науки, в первую очередь, по причине отсутствия научных исследований данного вопроса в теории и практике прокурорского надзора и недостаточного правового регулирования прокурорско-надзорного

процесса в законодательстве советского и современного периодов.

Обзор методической литературы о проведении проверок вне уголовно-правовой сферы свидетельствует о наличии предпосылок разработки тактики применительно к условиям ситуации в целях выбора прокурором эффективных правовых средств прокурорского надзора<sup>25</sup>.

Об использовании знаний из различных научных областей отмечается в трудах ученых в разделе, не относящемся к вопросам тактики и методики проверок<sup>26</sup>.

*Практические предпосылки* разработки и реализации тактики надзорной деятельности основаны на поисково-познавательной деятельности прокурора и обусловлены надзорными ситуациями, складывающимися на каждой стадии надзора в соответствии с поставленными целями и задачами.

Стадия надзора охватывается условиями и обстоятельствами конкретной ситуации и воздействующими на них внутренними и внешними факторами, что требует от прокурора проведения ее комплексного анализа и оценки.

Так, на стадии проведения проверки основной целью является сбор доказательств, позволяющих сделать обоснованный вывод о наличии (отсутствии) нарушений законности, что предполагает, в первую очередь, выработку способов действий или их выбор. Стадия принятия мер прокурорского реагирования характеризуется выбором эффективного правового средства, способного устранить нарушение и предупредить его повторение в будущем. На стадии контроля за выполнением требований прокурора предполагается применение различных способов действий и методов, направленных на полное удовлетворение требований, изложенных в документах реагирования, а также на выбор правового средства в случае их игнорирования или частичного выполнения.

Надзорная ситуация выполняет двоякую роль: является неотъемлемым компонентом надзорной деятельности и ведущим элементом тактики надзорной деятельности прокуратуры, определяющего ее формирование, содержание и реализацию.

Исходя из вышеизложенного, в целях наиболее качественного и эффективного выполнения требований законодательства о прокурорском надзоре необходимо введение в теорию и практику прокурорского надзора тактики, реализация которой позволит осуществлять поиск, как предусмотренных законом правовых средств в целях их выбора применительно к условиям ситуации, так и прибегать к разработке оригинальных

<sup>18</sup> Шпильрейн И. Метод качественного учета сотрудников // Времена. № 7. Апрель. 1924 г. Изд-во «Красная новь» Главполитпросвет. М., 1924. С. 86—90.

<sup>19</sup> Сафонов А.П. Резервы повышения эффективности прокурорского надзора // Проблемы прокурорского надзора. Научная конференция, посвященная 50-летию советской прокуратуры: тезисы сообщений. 20—21 апреля 1972. М., 1972. С. 98—102;

<sup>20</sup> Маркелов Т.Л. Тактика общего надзора прокуратуры и ее соотношение с методикой // Советская прокуратура на страже законности. Издательство Саратовского университета. 1973 г. С. 27-30.

<sup>21</sup> Там же.

<sup>22</sup> Винокуров Ю.Е. К вопросу о понятии «Научный продукт» (Версия) // Вестник научной школы «Повышение эффективности деятельности правоохранительных органов Российской Федерации»; отв. ред. А.Ю. Винокуров. Выпуск седьмой. М.: Московский гуманитарный университет, 2018. С. 3-8.

<sup>23</sup> Винокуров А.Ю., Винокуров Ю.Е. Теоретические основы эффективности прокурорского надзора за исполнением законов: монография / Московский гуманитарный ун-т, юридический фак-т. М.: издательство Московского гуманитар. ун-та, 2008. 100 с.

<sup>24</sup> Ястребов В.Б. Проблемы тактики общенадзорной деятельности прокуратуры / Ястребов В.Б. [и др.] // Вопросы борьбы с преступностью. Вып. 45. М.: Юрид. лит-ра, 1987. С. 75—84.

<sup>25</sup> Коршунова О.Н. Методика и тактика проведения прокурорской проверки: учеб. пос. / О.Н. Коршунова [и др.]; под ред. О.Н. Коршуновой. СПб.: Санкт-Петербургский юридический ин-т (фил.) Акад. Генеральной прокуратуры Российской Федерации, 2014. 239 с.

<sup>26</sup> Субанова Н.В. [доктор юрид. наук, доцент, проректор Университета прокуратуры Рос. Федерации]. Прокурорский надзор за исполнением законов вне уголовно-правовой сферы: проблемы теории и практики: монография. М.: Проспект, 2023. 400 с.

методов и действий, основанных на научных знаниях и профессиональном опыте.

Качество методических рекомендаций об осуществлении надзорной деятельности зависит от степени разработанности прокурорско-надзорного процесса, законодательного закрепления основных мероприятий и их тактического обеспечения. В настоящее время эти вопросы, как и в советское время, нуждаются в проведении дополнительных исследований. Очевидно, что методики, в первую очередь, должны учитывать ситуационный подход и тактический опыт прокуроров, накапливаемый ими в ходе прокурорско-надзорного процесса. Во-первых, представляется целесообразным составление единой методики, отражающей содержание прокурорско-надзорного процесса, основные мероприятия, обеспечивающие его качество, во-вторых, регламентирующие осуществление надзорной деятельности по направлениям надзора.

Следует заметить, что элементы тактики обладают двойным характером в связи с самостоятельностью тактики и их последующей адаптацией к осуществляемой деятельности с учетом правил, установленных в теории и практике. Некоторые из элементов имеют теоретические начала, в связи с чем раскрытие их содержания требует как научного, так и предметного обоснования применительно к надзорной деятельности прокуратуры с учетом принципов и предметов прокурорского надзора, исходя из сущности самой надзорной функции прокуратуры.

Так, подлежит детальному изучению надзорная ситуация, которая выступает в роли элемента, определяющего направление и содержание разрабатываемой и реализуемой тактики. В этой связи необходимо исходить из ситуационного подхода, который активно используется в иной профессиональной деятельности.

Тактическая гипотеза прокурора является одним из сложных, на наш взгляд, элементов, требующих научного и практического обоснования. Его реализация связана с прогнозированием и оценкой рисков при принятии тактических решений. Данный прогноз должен учитывать, соответственно, результаты оценки надзорной ситуации. Прокурору в целях обеспечения принятия рационального решения надлежит разрабатывать несколько гипотез для определения рабочей (основной) гипотезы, в соответствии с которой будут формироваться возможные тактические решения.

Тактическое решение прокурора имеет структуру, обусловленную особенностями профессиональной компетентности прокурорского работника. В ходе данного процесса не исключается возможность прокурора предусмотреть варианты решений в пользу единственно правильного, реализуемого в виде тактического приема.

Тактические приемы прокурора точнее всего выражаются в термине «средства тактического воздействия прокурора», который достаточно полно охватывает прокурорско-надзорный процесс. В их основу могут быть положены научные знания, практический опыт,

и, прежде всего средства прокурорского надзора, предусмотренные в законодательстве и подлежащие выбору применительно к обстоятельствам надзорной ситуации и, как мы отмечали ранее, выполняющие своего рода роль предпосылок (условий) для разработки и реализации тактики.

Принципы, функции и предмет тактики представляется объективным исследовать исходя из знаний фундаментальных наук, применительно к элементам тактики, с одной стороны, и руководствуясь этими понятиями, предусмотренными в действующем законодательстве о прокурорском надзоре, с другой.

В науке и практике прокурорского надзора вопросы оценки эффективности прокурорских работников и надзорной деятельности нуждаются в проведении научных исследований.

Некоторые ученые и практические работники отмечают, что критерии оценки эффективности работы прокуратуры — статистические показатели надзорной деятельности ... весьма несовершенны и не учитывают современных реалий [12].

Заслуживает внимания точка зрения ученых о необходимости соблюдения и уважения закона в целях обеспечения защиты прав и свобод человека и гражданина [13], что в значительной степени влияет на повышение уровня состояния законности и оценку деятельности прокуратуры и конкретного прокурорского работника.

В частности, вопрос эффективности надзорной деятельности напрямую зависит от личностных и профессиональных характеристик конкретного прокурорского работника. Видится, что оценка эффективности надзорной деятельности органов прокуратуры, от которой зависит формирование состояния законности на конкретных объектах надзора и в государстве в целом, должна начинаться с отдельной прокуратуры, отдельного прокурорского работника. Оценку эффективности надзорной деятельности можно определить так: **ПРОФЕССИОНАЛЬНАЯ КОМПЕТЕНТНОСТЬ ПРОКУРОРСКОГО РАБОТНИКА: КАЧЕСТВО — РЕЗУЛЬТАТ — ЭФФЕКТИВНОСТЬ**. По принципу обратной связи возможно оценить эффективность прокурорского работника. Кроме того, использование такого принципа позволит определить удельный вес вклада в законность прокуратуры и их сотрудников (каждого в отдельности) применительно к поднадзорным объектам (субъектам); возможна разбивка по предметам надзора или направлениям. Данное предложение требует детальной проработки с последующей реализацией в виде эксперимента на базе прокуратуры низового звена. По результатам которого, представляется наиболее объективным и определять основные критерии эффективности надзорной деятельности и прокурорских работников.

Таким образом, проведенная работа свидетельствует о том, что выявленные предпосылки послужили основанием для формирования проблемных направлений, подлежащих дальнейшему исследованию в целях преобразования надзорной деятельности

прокуратуры в соответствии с современными реалиями. К основным можно отнести — цифровизацию, ситуационный анализ, тактическое моделирование, внедрение искусственного интеллекта в надзорную деятельность прокуратуры.

### Заключение

Анализируя изложенное, впервые в науке посредством использования инновационного подхода на основе содержания определения понятия тактики надзорной деятельности прокуратуры выявлены предпосылки тактического обеспечения надзорной деятельности прокуратуры и основания их классификации в зависимости от источника происхождения. Результаты исследования дают основание полагать, что в источниках правового, научного и методического характера созданы условия для практического использования тактики, которые выражаются: в изучении и анализе состояния законности, складывающихся обстоятельств конкретной ситуации, в выборе эффективных правовых средств по выявлению, устранению и предупреждению нарушений законности, разработке оригинальных действий (приемов). Указанное обстоятельство дает однозначный утвердительный ответ о целесообразности применения и дальнейшего развития тактики в ходе организации и осуществлении надзорной деятельности прокуратуры.

Способствуют этому и государственные задачи, направленные на развитие информационного общества, трансформацию органов прокуратуры Российской Федерации.

Подводя итог сказанному, в целях развития тактики и ее эффективного использования представляется целесообразным в дальнейшем вести работу по следующим основным направлениям:

- проведение теоретических исследований надзорной деятельности прокуратуры для определения ее элементов и надлежащего законодательного регулирования;
- формирование понятийно-категориального аппарата тактики надзорной деятельности прокуратуры, определение ее принципов, функций и предмета;
- использование результатов теоретико-прикладных исследований основ тактики в теории и практике прокурорско-надзорного процесса;
- цифровизация надзорной деятельности в части сбора, накопления, обработки и хранения сведений о надзорных характеристиках поднадзорных объектов и субъектов в целях их постоянного обновления и практического использования (научное и методическое обеспечение органов прокуратуры);
- тактическое моделирование надзорной деятельности в соответствии с надзорными ситуациями, раскрывающими прокурорско-надзорный процесс на каждой стадии надзора, включая предметы надзора и поднадзорные объекты;
- составление методик надзорной деятельности на основе ситуационного подхода и результатов использованной тактики применительно к обстоятельствам надзорных ситуаций, отражающих деятельность прокуроров при проведении проверок и применение конкретных средств тактического воздействия (методы, способы, средства прокурорского надзора);
- разработка и реализация тактики надзорной деятельности посредством использования искусственного интеллекта (включает непосредственно сам механизм (элементы) и принцип его работы (алгоритм)).

### Литература

1. Махьянова Р.М. Тактика надзорной деятельности органов прокуратуры : уч. пос. М. : Военный университет им. князя Александра Невского Минобороны России, 2023. 108 с. ISBN: 978-5-6048563-6-9.
2. Махьянова Р.М. Тактическое мышление прокурора: понятие, содержание и влияние на состояние законности // Российский юридический журнал. 2024. № 5. С. 117—128. DOI: 10.34076/20713797\_2024\_5-117.
3. Махьянова Р.М. Основополагающие элементы тактики надзорной деятельности прокуратуры // Теория государства и права. № 1 (48). 2026. С. 219—231. DOI: 10.47905/MATGIP\_2026\_1\_48\_219.
4. Махьянова Р.М. Тактика надзорной деятельности прокуратуры: порядок разработки и реализации // Lex russica. № 78 (6). 2025. С. 67—77. DOI: 10.17803/1729-5920.2025.223.6.067-077.
5. Бессчасный С.А. Перспективы развития — цифровизация прокурорского надзора // Правовое регулирование прокурорской деятельности: история и новации (Сухаревские чтения) : сб. мат. VIII Всерос. науч.-практ. конф. (Москва, 7 окт. 2022 г.) / Под общ. ред. Р.В. Жубрина; [под науч. ред. А.Ю. Винокурова; сост. О.В. Боброва, Е.А. Непомнящая, Н.В. Трошина]; Ун-т прокуратуры Рос. Федерации. М., 2023. 428 с. С. 20—31.
6. Ергашев Е.Р. О некоторых аспектах стратегии и тактики цифровой трансформации российской прокуратуры // Правовое регулирование прокурорской деятельности: история и новации (Сухаревские чтения) : сб. мат. VIII Всерос. науч.-практ. конф. (Москва, 7 окт. 2022 г.) / Под общ. ред. Р.В. Жубрина; [под науч. ред. А.Ю. Винокурова; сост. О.В. Боброва, Е.А. Непомнящая, Н.В. Трошина]; Ун-т прокуратуры Рос. Федерации. М., 2023. 428 с. С. 52—61.



7. Полякова Т.А., Троян Н.А. Трансформация государственного управления в Российской Федерации: от кибернетики, информатики к цифровизации // Правовая информатика. № 4. 2025 г. С. 215—226. DOI: 10.24412/1994-1404-2025-4-215-226.
8. Кунев Д.А. Информационно-аналитическая деятельность в органах прокуратуры: становление, развитие, перспективы цифровой трансформации (к 90-летию системы ведомственной аналитики) // Вестник Университета прокуратуры Российской Федерации. № 4 (108). 2025. С. 51—58.
9. Тараканова Л.А., Кулешова С.А., Петросян М.А. Основные направления повышения эффективности прокурорского надзора за исполнением законов // Аграрное и земельное право. 2025. № 5. С. 110—113. DOI: 10.47643/1815-1329\_2025\_5\_110.
10. Шабаров Д.В. Прокуратура г. Санкт-Петербурга. Анализ состояния законности в прокурорской деятельности: теория и практика // Ленинградский юридический журнал. 2022. № 2 (68). С. 158—169.
11. Рокитянский С.Г. Историко-правовое объяснение телеологии и аксиологии российского прокурорского надзора // Вестник Университета им. О.Е. Кутафина (МГЮА). 2024;(1):195-207. DOI: 10.17803/2311-5998.2024.113.1.

**SECTION:**  
CONSTITUTIONAL LAW

## PROBLEMS OF USING AND DEVELOPING SUPERVISORY TACTICS IN THE PROSECUTOR'S OFFICE

*Makh'ianova R.M.*<sup>27</sup>

**Keywords:** *prosecutorial inspections, inspection methodologies, tactical elements, tactical thinking, situational approach, decision-making, professional competence, organizational and administrative documents, digitalization, artificial intelligence, classification of prerequisites.*

### **Abstract**

**The aim of this study:** *is to identify and systematize the prerequisites for employing specific tactics in the supervisory activities of the prosecutor's office — based on findings from previous research — as well as to determine the criteria for their classification and outline directions for the further improvement of prosecutorial supervision.*

**Research methods:** *analysis, generalization, and systematization of scientific and methodological literature, legislation, and organizational-administrative documents of the Prosecutor's Office, as well as classification of the identified prerequisites for employing supervisory tactics.*

**Research results:** *the prerequisites for the development and implementation of tactics at various stages of the supervisory activities of the prosecutor's office, contained in legislative acts, organizational and administrative documents of the prosecutor's office, scientific and methodological literature on prosecutor's supervision, were identified and systematized. Based on a comprehensive analysis of diverse scientific and practical sources, the grounds for classifying the identified prerequisites were determined. As their basis, conditions have been identified that contribute to the conduct of situational analysis, the search, development and implementation of solutions in the course of organizing and conducting inspections outside the criminal legal sphere. In addition, the main directions for the further development of the supervisory activities of the prosecutor's office and its tactical support are outlined, including the development of theoretical provisions, clarification and development of the conceptual framework, digitalization and tactical modeling of supervisory activities, compilation of methods based on a situational approach.*

### **References**

1. Makh'ianova R.M. *Taktika nadzornoj deiatel'nosti organov prokuratury : uch. pos. M. : Voennyi universitet im. kniazia Aleksandra Nevskogo Minoborony Rossii*, 2023. 108 s. ISBN: 978-5-6048563-6-9.

---

<sup>27</sup> **Rimma M. Makh'ianova**, Associate Professor, Department of Military Administration, Administrative and Financial Law, Prince Alexander Nevsky Military University of the Ministry of Defense of the Russian Federation, Moscow, Russian Federation.  
E-mail: [r@9099177842.ru](mailto:r@9099177842.ru)

2. Makh'ianova R.M. Takticheskoe myshlenie prokurora: poniatie, sodержanie i vliianie na sostoianie zakonnosti // Rossiiskii iuridicheskii zhurnal. 2024. No. 5. S. 117—128. DOI: 10.34076/20713797\_2024\_5-117.
3. Makh'ianova R.M. Osnovopolagaiushchie elementy taktiki nadzornoj deiatel'nosti prokuratury // Teoriia gosudarstva i prava. No. 1 (48). 2026. S. 219—231. DOI: 10.47905/MATGIP\_2026\_1\_48\_219.
4. Makh'ianova R.M. Taktika nadzornoj deiatel'nosti prokuratury: poriadok razrabotki i realizatsii // Lex russica. No. 78 (6). 2025. S. 67—77. DOI: 10.17803/1729-5920.2025.223.6.067-077.
5. Besschasnyi S.A. Perspektivy razvitiia — tsifrovizatsiia prokurorskogo nadzora // Pravovoe regulirovanie prokurorskoj deiatel'nosti: istoriia i novatsii (Sukharevskie chteniia) : sb. mat. VIII Vseros. nauch.-prakt. konf. (Moskva, 7 okt. 2022 g.) / Pod obshch. red. R.V. Zhubrina; [pod nauch. red. A.Iu. Vinokurova; sost. O.V. Bobrova, E.A. Nepomniashchaia, N.V. Troshina]; Un-t prokuratury Ros. Federatsii. M., 2023. 428 s. S. 20—31.
6. Ergashev E.R. O nekotorykh aspektakh strategii i taktiki tsifrovoi transformatsii rossiiskoi prokuratury // Pravovoe regulirovanie prokurorskoj deiatel'nosti: istoriia i novatsii (Sukharevskie chteniia) : sb. mat. VIII Vseros. nauch.-prakt. konf. (Moskva, 7 okt. 2022 g.) / Pod obshch. red. R.V. Zhubrina; [pod nauch. red. A.Iu. Vinokurova; sost. O.V. Bobrova, E.A. Nepomniashchaia, N.V. Troshina]; Un-t prokuratury Ros. Federatsii. M., 2023. 428 s. S. 52—61.
7. Poliakova T.A., Troian N.A. Transformatsiia gosudarstvennogo upravleniia v Rossiiskoi Federatsii: ot kibernetiki, informatiki k tsifrovizatsii // Pravovaia informatika. No. 4. 2025 g. S. 215—226. DOI: 10.24412/1994-1404-2025-4-215-226.
8. Kunev D.A. Informatsionno-analiticheskaiia deiatel'nost' v organakh prokuratury: stanovlenie, razvitie, perspektivy tsifrovoi transformatsii (k 90-letiiu sistemy vedomstvennoi analitiki) // Vestnik Universiteta prokuratury Rossiiskoi Federatsii. No. 4 (108). 2025. S. 51—58.
9. Tarakanova L.A., Kuleshova S.A., Petrosian M.A. Osnovnye napravleniia povysheniia effektivnosti prokurorskogo nadzora za ispolneniem zakonov // Agrarnoe i zemel'noe pravo. 2025. No. 5. S. 110—113. DOI: 10.47643/1815-1329\_2025\_5\_110.
10. Shabarov D.V. Prokuratura g. Sankt-Peterburga. Analiz sostoianiia zakonnosti v prokurorskoj deiatel'nosti: teoriia i praktika // Leningradskii iuridicheskii zhurnal. 2022. No. 2 (68). S. 158—169.
11. Rokitianskii S.G. Istoriko-pravovoe ob"iasnenie teleologii i aksiologii rossiiskogo prokurorskogo nadzora // Vestnik Universiteta im. O.E. Kutafina (MGLuA). 2024;(1):195-207. DOI: 10.17803/2311-5998.2024.113.1.



# «ТЕХНОЛОГИИ ЗДРАВООХРАНЕНИЯ», «ТЕХНОЛОГИИ СБЕРЕЖЕНИЯ ЗДОРОВЬЯ», «МЕДИЦИНСКИЕ ТЕХНОЛОГИИ»: СООТНОШЕНИЕ ДЕФИНИЦИЙ В КОНТУРЕ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ<sup>1</sup>

Рыбакова О.С.<sup>2</sup>

**Ключевые слова:** правовой инжиниринг, технологическое развитие, модернизация здравоохранения, государственное управление, искусственный интеллект, цифровые технологии, телемедицина.

## Аннотация

**Цель работы:** исследовать содержательное наполнение дефиниций «технологии здравоохранения», «технологии сбережения здоровья», «медицинские технологии» в правовой доктрине и актах законодательства; определить их соотношение; выявить целесообразность легитимного закрепления; обосновать создание эффективных правовых инструментов правового сопровождения применения технологий в системе здравоохранения

**Методы исследования:** в работе применялись общенаучные методы анализа и синтеза, а также сравнительного анализа. Сфокусировано внимание на системном методе.

**Результаты исследования:** выявлена терминологическая фрагментарность легально закрепления исследуемых категорий, что может порождать правовую неопределенность при оценке их безопасности, эффективности, доступности для участников правоотношений для достижения конституционно-значимых целей обеспечения охраны здоровья. Предложенные в статье подходы могут служить концептуальной основой для дальнейших дискуссий и выработки конкретных нормативных решений, направленных на формирование эффективной регуляторной модели применения технологий в системе здравоохранения.

**Научная новизна:** автором обоснована иерархическая дифференциация исследуемых дефиниций, где «технологии здравоохранения» — наиболее широкая дефиниция, охватывающая организационно-управленческие, санитарно-эпидемиологические, информационно-коммуникационные и иные методы, обеспечивающие функционирование и развитие системы здравоохранения в целом; «технологии здоровьесбережения» выступает как понятие, предполагающее превентивную и поведенческую составляющую, направленную на сохранение и укрепление здоровья населения; «медицинские технологии» понимается как наиболее содержательно узкая дефиниция, непосредственно связанная с клинической практикой и включающая диагностические, лечебные, хирургические, реабилитационные и иные вмешательства, основанные на применении специализированного оборудования, материалов, биопрепаратов и цифровых алгоритмов.

DOI: 10.24412/1994-1404-2026-3-00-18

## Введение

Объективная необходимость модернизации национальной системы здравоохранения и обеспечения её универсальной доступности детерминируется темпами научно-технического прогресса. Эволюция здравоохранения и параметры доступности медицинской помощи напрямую коррелируют с уровнем технологизации отрасли. Правовая регуляторика призвана следовать за развитием медицинской науки и

клинической практики, где прогрессивные технологические решения выступают не только инструментарием, а гарантией и основополагающим условием обеспечения конституционного права граждан на охрану здоровья и доступ к медицинской помощи [1, с. 52; 2, с. 154—156] (статья 41 Конституции РФ), что придает им статус *conditio sine qua non* (курсив здесь и далее — О.Р.).

<sup>1</sup> Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

<sup>2</sup> **Рыбакова Ольга Сергеевна**, кандидат юридических наук, доцент, доцент кафедры конституционного и муниципального права Университета им. О.Е. Кутафина (МГЮА), Москва, Россия.  
E-mail: [osrybakova@msal.ru](mailto:osrybakova@msal.ru)

Данный подход объективируется в программно-целевых документах модернизации системы здравоохранения. Национальные цели России, традиционно обозначенные в указах главы государства<sup>3</sup>, в части сохранения народонаселения, укрепления общественного здоровья и увеличения ожидаемой продолжительности жизни, коррелируя с приоритетами национальной безопасности<sup>4</sup>, объективируются в качестве их имманентной составляющей, неразрывно сопряжены с задачами долгосрочного планирования и развития технологий<sup>5</sup>, выступая одновременно их целевым ориентиром, и критерием эффективности инновационной политики государства. Стратегия научно-технологического развития России в числе базовых приоритетов называет технологическую модернизацию здравоохранения, путем перехода к «персонализированной, предиктивной и профилактической медицине, высокотехнологичному здравоохранению и технологиям здоровьесбережения», в том числе за счет рационального производства и применения лекарственных препаратов и использования генетических данных и технологий<sup>6</sup>.

**Нормативно-правовое конструирование  
дефиниций «технология сбережения здоровья»,  
«технология здравоохранения»,  
и «медицинская технология»**

Технологизация отечественного здравоохранения успешно реализуется на протяжении нескольких десятилетий. Вместе с тем, следует констатировать отсутствие единого подхода к нормативному закреплению дефиниций «технология здравоохранения», «технология сбережения здоровья», «медицинская технология».

<sup>3</sup> Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собрание законодательства РФ. 13.05.2024. № 20. Ст. 2584; Указ Президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» (документ утратил силу) // Собрание законодательства РФ. 27.07.2020. № 30. Ст. 4884 и др.

<sup>4</sup> Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 05.07.2021. № 27 (Ч. II). Ст. 5351; Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» (документ утратил силу) // Собрание законодательства РФ. 04.01.2016. № 1 (Ч. II). Ст. 212 и др.

<sup>5</sup> Указ Президента РФ от 08.11.2021 № 633 «Об утверждении Основ государственной политики в сфере стратегического планирования в Российской Федерации» // Собрание законодательства РФ. 15.11.2021. № 46. Ст. 7676; Указ Президента РФ от 28.11.2018 № 680 (ред. от 01.07.2025) «О развитии генетических технологий в Российской Федерации» (вместе с «Положением о совете по реализации Федеральной научно-технической программы развития генетических технологий на 2019—2030 годы») // Собрание законодательства РФ. 03.12.2018. № 49 (Ч. VI). Ст. 7586; Постановление Правительства РФ от 29.03.2019 № 377 (ред. от 04.03.2026) «Об утверждении государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации» // Собрание законодательства РФ. 15.04.2019. № 15 (Ч. III). Ст. 1750.

<sup>6</sup> Указ Президента РФ от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации» // Собрание законодательства РФ. 04.03.2024. № 10. Ст. 1373.

Согласно позиции ВОЗ, для обозначения технологий, применяемых в сфере охраны здоровья человека, используется термин *health technology* (англ. *технология здоровья, здоровьесбережения, медицинская технология*), который по своему содержанию выступает обобщающим понятием к различным технологиям, применяемым в здравоохранении. В Резолюции Всемирной ассамблеи здравоохранения WHA60.29 — «Health technologies 60<sup>th</sup> World Health Assembly»<sup>7</sup> (Технологии здравоохранения), принятой в 2007 году на 60-й сессии, отмечается, что Health technologies включают применение систематизированных знаний, навыков и умений в виде методов, устройств, лекарственных средств, вакцин, процедур и систем, разработанных в целях решения какой-либо проблемы здравоохранения и улучшения качества жизни.

Детальный анализ документа позволяет прийти к выводу, что по своему содержанию Health technologies включают широкий инструментарий (знания, методы, устройства, средства и т. п.), направленный как на обеспечение реализации права на охрану здоровья индивида, так и на разработку, внедрение, применение технологических решений в сфере управления и организации системы здравоохранения в целом. В Резолюции констатируется системообразующая роль технологий в обеспечении устойчивого функционирования и эволюционного развития национальных систем здравоохранения. Технологический фактор системы здравоохранения квалифицируется в качестве имманентного условия эффективности процессов профилактики, диагностики, терапевтического вмешательства и восстановительного лечения пациентов, при этом акцент сделан на технологиях медицинского назначения (*Medical Technologies*), которым придан статус решающего инструментария в противодействии наиболее значимым угрозам общественному здоровью. Аналогичный подход к пониманию технологий здравоохранения отражен в документах Международной сети агентств по оценке технологий здравоохранения (INANTA), где технологии здравоохранения понимаются как «вмешательство, разработанное с целью профилактики, диагностики или лечения заболеваний, укрепления здоровья, обеспечения реабилитации или организации оказания медицинской помощи»<sup>8</sup>.

Российский законодатель сознательно либо вынужденно дистанцируется от закрепления легальной дефиниции «технология здравоохранения», что обусловлено объективным расширительным подходом к пониманию технологий, применяемых в сфере здравоохранения. Согласимся, что развитие технологий здравоохранения значительно опережает правовое

<sup>7</sup> World Health Assembly WHA60.29: Health technologies 60th World Health Assembly [pdf 38.43kb]. URL: <https://www.emro.who.int/health-biomedical-devices/strategy/resolutions.html> (дата обращения: 13.04.2026).

<sup>8</sup> См.: Глоссарий Международной сети агентств по оценке медицинских технологий. URL: <https://htaglossary.net/List-all-terms> (дата обращения: 12.07.2026).



регулирование данной сферы общественных отношений [3, с. 63], в связи с чем, попытка легальной фиксации содержательного наполнения технологии здравоохранения может необоснованно сдерживать внедрение новых (неучтенных в дефиниции) разработок и технологий в систему здравоохранения.

Программные документы, определяющие приоритеты технологической модернизации здравоохранения, помимо технологий, напрямую обеспечивающих реализацию права на охрану здоровья человека, включают управленческие решения, трансформируя процессы организации управления в системе здравоохранения, коммуникации, сбора, хранения, обработки информации и др. Стратегия развития здравоохранения на период до 2030 года<sup>9</sup> определяет технологическую модернизацию здравоохранения в числе базовых инструментов обеспечения национальной безопасности в сфере охраны здоровья. Стратегическим направлением в области цифровой трансформации здравоохранения обозначены следующие: «достижение высокого уровня показателя «цифровая зрелость» участников реализации стратегического направления; ускоренный переход сектора здравоохранения на новые управленческий и технологический уровни посредством полного перехода к «цифровым двойникам», создание единой платформенной экосистемы на основе целостных и однородных первичных данных»<sup>10</sup>.

Мероприятия по развитию и внедрению технологий искусственного интеллекта (ИИ) в систему здравоохранения осуществляются в рамках Национальной стратегии развития искусственного интеллекта на период до 2030 года<sup>11</sup>, по итогам реализации которой должны быть созданы условия для «эффективного взаимодействия государства, организаций, в том числе научных, и граждан в сфере развития искусственного интеллекта, что позволит российским технологиям искусственного интеллекта занять значительную долю мирового рынка» (п.12). Модернизация системы здравоохранения предполагает, прежде всего, цифровую трансформацию по следующим направлениям реализации организационно-правовых и технологических мер в сфере планирования, структурирования, оперативного управления, мониторинга и оценки эффективности функционирования как всей национальной системы здравоохранения, так и её отдельных структурных компонентов [4, с. 187—192]. Цифровая трансформация,

как отмечается в научной литературе, оказывает существенное влияние на развитие информационного общества, находящегося в постоянной динамике, что в значительной степени связано с развитием современных цифровых технологий, являющихся определяющим фактором цифровой экономики и цифровой экосистемы [5—9]. Справедливо утверждение, что «современная трансформация здравоохранения происходит под влиянием таких технологий, как интернет вещей, виртуальная медицинская помощь, удаленный мониторинг, искусственный интеллект, аналитика больших данных, блокчейн, интеллектуальные носимые устройства, платформы, инструменты, позволяющие удаленно собирать, обмениваться и хранить данные, а также делиться актуальной информацией по всей экосистеме здравоохранения, создавая непрерывность оказания медицинской помощи в целях улучшения результатов лечения за счет улучшения медицинской диагностики, принятия решений на основе данных, цифровой терапии, клинических испытаний, самостоятельного управления медицинской помощью и уходом, ориентированного на человека, а также повышения уровня знаний, навыков и компетентности специалистов» [10, с. 3].

Технологическая модернизация представляет собой синергетический процесс системной трансформации здравоохранения, охватывающий цифровизацию управления здоровьем (формирование единой цифровой среды), импортозамещение критической номенклатуры лекарств и изделий, внедрение алгоритмов ИИ в клиническую практику, коммерциализацию разработок нового поколения (персонализированных, биоинженерных и радиофармпрепаратов), а также создание адекватной регуляторной и организационной инфраструктуры для телемедицины и удаленного мониторинга. Достижением обозначенных приоритетов, по оценкам специалистов, направлено на снижение затрат в системе здравоохранения, оптимизацию доступности медицинских услуг (особенно в удаленных районах) с помощью мобильных приложений и телемедицины, оптимизацию рабочего времени медицинского персонала, повышение качества медицинской помощи благодаря использованию технологий искусственного интеллекта и анализа больших данных [11, с. 232; 12; 13], что в совокупности отражают ключевую цели модернизации системы здравоохранения — сбережение здоровья населения через обеспечение конституционного права человека на охрану здоровья и доступ к современным медицинским технологиям.

Стратегия научно-технологического развития Российской Федерации<sup>12</sup>, в числе системообразующих приоритетов и перспектив, наряду с другими, обозначает «переход к персонализированной, предиктивной и профилактической медицине, высокотехнологичному здравоохранению и технологиям здоровьесбережения»

<sup>9</sup> Указ Президента РФ от 08.12.2025 № 896 «О Стратегии развития здравоохранения в Российской Федерации на период до 2030 года» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 09.12.2025.

<sup>10</sup> Распоряжение Правительства РФ от 17.04.2024 № 959-р «Об утверждении стратегического направления в области цифровой трансформации здравоохранения» // Собрание законодательства РФ. 22.04.2024. № 17. Ст. 2388.

<sup>11</sup> Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства РФ. 14.10.2019. № 41. Ст. 5700.

<sup>12</sup> Указ Президента РФ от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации» // Собрание законодательства РФ. 04.03.2024. № 10. Ст. 1373.

(пп. «в» п. 21). Термин «технологии здоровьесбережения» встречается в других программных документах, например, в сфере развития промышленной продукции по реабилитации<sup>13</sup>, ведомственных актах<sup>14</sup>. Содержание термина в документах не раскрывается.

Аналогичный, но не идентичный термин — «технологии сбережения здоровья» используется в другом программно-целевом документе — Стратегии развития здравоохранения<sup>15</sup>, где «сохранение здоровья населения за счет профилактических мероприятий, внедрение технологий сбережения здоровья на популяционном уровне, включая здоровое старение и активное долголетие» обозначены среди основных задач развития здравоохранения в Российской Федерации (пп. 2 п. 14). Данная дефиниция входит в наименование национального проекта «Новые технологии сбережения здоровья», который объединяет несколько федеральных проектов, связанных по своему целеполаганию в внедрением технологий: «Управление медицинской наукой», «Технологии разработки медицинских изделий, лекарственных средств и платформ нового поколения», «Биомедицинские и когнитивные технологии будущего», «Регенеративная биомедицина, технологии превентивной медицины, обеспечивающие активное и здоровое долголетие», «Развитие производства наиболее востребованных лекарственных препаратов и медицинских изделий»<sup>16</sup>.

Исходя из содержания приведенных документов и паспорта нацпроекта, можно сделать вывод, что дефиниции «технологии здоровьесбережения» и «технология сбережения здоровья» используются как синонимичные и взаимозаменяемые и представляют собой системно организованную, научно-обоснованную и нормативно обеспеченную совокупность методов, средств и организационных решений, направленных на сохранение, укрепление и восстановление здоровья человека на всех этапах жизненного цикла, реализуемую через интеграцию фундаментальных биомедицинских исследований, инженерных разработок, клинической практики и производственных мощностей в единый инновационный цикл с приоритетом превентивных стратегий и персонализированных подходов.

Анализ федеральных законодательных актов позволяет констатировать использование различных терми-

нов, обозначающих технологии, применяемые в сфере здоровьесбережения (табл. 1).

Приведенный обзор демонстрирует упоминание различных технологий (технологии искусственного интеллекта, информационные, биомедицинские, когнитивные, телемедицинские, генетические и др.), что позволяет идентифицировать их как совокупность технологий, применяемых в сфере охраны здоровья человека, которые соотносятся с дефиницией «технологии здоровьесбережения» как часть и целое.

Национальный стандарт (ГОСТ)<sup>17</sup> вводит ещё одну дефиницию — «медицинские технологии», определяя их как «методы диагностики, лекарственного и нелекарственного лечения, профилактики и реабилитации, системы охраны и укрепления здоровья, использующиеся в здравоохранении» (ч. 3). ГОСТ содержит широкий инструментарий, раскрывающий содержание медицинских технологий, среди которых: «применение лекарств, включая биологические препараты; применение крови и её компонентов; применение специализированного лечебного питания; использование приборов, расходных материалов, технических устройств и мобильных приложений; терапевтические и хирургические процедуры; иные мероприятия и процедуры (в т.ч. школа пациента с определенной патологией, обучение родственников и немедицинских работников процедурам ухода, дистанционные консультации с использованием телекоммуникативных систем и приспособлений); вспомогательные управленческие системы и процедуры (формуляр больницы, аутсорсинг лабораторных исследований, лицензирование деятельности, система электронной записи на прием и др.)» (ч. 3).

Юридико-техническая конструкция ГОСТа обнаруживает категориальную несостоятельность, — в единый семантический ряд поставлены технологии, не имеющие единого экономико-правового базиса (клеточные продукты, организационные протоколы, системы удаленного доступа, управленческие решения и др.). Отсутствие четких дефиниций и критериев дифференциации детерминирует расширительное толкование понимания дефиниции «медицинские технологии» в их корреляции с технологиями в сфере здравоохранения в целом.

В связи с этим положительной оценки заслуживает инициатива Минздрава России по закреплению нормативного определения дефиниции «медицинские технологии» на уровне базового Закона № 323-ФЗ. Согласно паспорту законопроекта, размещенного на федеральном портале, под медицинской технологией предлагается определить «способ осуществления медицинского вмешательства или комплекса медицинских вмешательств, направленных на профилактику, диагностику и лечение заболеваний, медицинскую реабилитацию и имеющих самостоятельное законченное

<sup>13</sup> Распоряжение Правительства РФ от 06.11.2025 № 3143-р «Об утверждении Стратегии развития производства промышленной продукции реабилитационной направленности на период до 2030 года» // Собрание законодательства РФ. 17.11.2025. № 46. Ст. 6934.

<sup>14</sup> Письмо ФМБА России от 24.10.2025 № 32-01/02-3/920 «О направлении Рекомендаций для работодателей по формированию инфраструктуры и алгоритмов действий медицинских работников по внедрению технологий здоровьесбережения на рабочем месте» и др. // СПС «КонсультантПлюс».

<sup>15</sup> Указ Президента РФ от 08.12.2025 № 896 «О Стратегии развития здравоохранения в Российской Федерации на период до 2030 года» // Собрание законодательства РФ. 15.12.2025. № 50. Ст. 7826.

<sup>16</sup> Официальный сайт «Национальные проекты». URL: <https://национальныепроекты.рф/new-projects/tekhnologii-zdorovya/> (дата обращения: 12.07.2026).

<sup>17</sup> Национальный стандарт Российской Федерации «Оценка медицинских технологий. Общие положения», утв. и введен в действие Приказом Росстандарта от 11.06.2014 № 568-ст. М. : Стандартинформ, 2015.

**Обзор НПА в части закрепления положений о технологиях здоровьесбережения**

| НАИМЕНОВАНИЕ НПА                                                                                                                                                                    | ИЗВЛЕЧЕНИЕ <...>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» <sup>1</sup> (далее — Закон № 323-ФЗ)                                          | телемедицинские технологии — «информационные технологии, обеспечивающие дистанционное взаимодействие медицинских работников между собой, с пациентами и (или) их законными представителями, идентификацию и аутентификацию указанных лиц, документирование совершаемых ими действий при проведении консилиумов, консультаций, дистанционного медицинского наблюдения за состоянием здоровья пациента» (ч. 22 ст. 2)                                                                                                                                                                                                                                                            |
|                                                                                                                                                                                     | высокотехнологичная медицинская помощь — «часть специализированной медицинской помощи, включает в себя применение новых сложных и (или) уникальных методов лечения, а также ресурсоемких методов лечения с научно доказанной эффективностью, в том числе клеточных технологий, роботизированной техники, информационных технологий и методов геномной инженерии, разработанных на основе достижений медицинской науки и смежных отраслей науки и техники» (п. 3 ч. 1 ст. 34)                                                                                                                                                                                                   |
|                                                                                                                                                                                     | вспомогательные репродуктивные технологии — «методы лечения бесплодия, при применении которых отдельные или все этапы зачатия и раннего развития эмбрионов осуществляются вне материнского организма (в том числе с использованием донорских и (или) криоконсервированных половых клеток, тканей репродуктивных органов и эмбрионов), а также суррогатное материнство» (ч. 1 ст. 55)                                                                                                                                                                                                                                                                                           |
| Федеральный закон от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» <sup>2</sup>                                                                                           | лекарственные средства — «вещества или их комбинации, вступающие в контакт с организмом человека или животного <...>, применяемые для профилактики, диагностики, лечения заболевания, реабилитации <...> методами синтеза или с применением <i>биологических технологий</i> » (п. 1 ст. 4).                                                                                                                                                                                                                                                                                                                                                                                    |
| Федеральный закон 28.12.2024 № 523-ФЗ «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» <sup>3</sup> | <i>Содержит широкое определение технологий</i> , под которыми понимается «совокупность научно и практически обоснованных методов, средств, операций и (или) процессов, необходимых для преобразования энергии, вещества, информации в целях производства одного или нескольких видов продукции, выполнения работ, оказания услуг» (п. 15 ст. 3).                                                                                                                                                                                                                                                                                                                               |
| Указ Президента РФ от 18.06.2024 № 529 «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоёмких технологий» <sup>4</sup>            | среди важнейших наукоёмких критических технологий называет: биомедицинские и когнитивные технологии здорового и активного долголетия (п. 3); технологии разработки лекарственных средств и платформ нового поколения (биотехнологических, высокотехнологичных и радиофармацевтических лекарственных препаратов) (п. 4); технологии персонализированного, лечебного и функционального питания для здоровьесбережения (п. 5); технологии разработки медицинских изделий нового поколения, включая биогибридные, бионические технологии и нейротехнологии (п. 6); среди важнейших наукоёмких сквозных технологий — технологии искусственного интеллекта социальной сферы (п. 25). |
| Национальная стратегия развития искусственного интеллекта на период до 2030 года <sup>5</sup>                                                                                       | <i>технологии искусственного интеллекта</i> — совокупность технологий, включающая в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта                                                                                                                                                                                                                                                                                                                                                                                                         |
| Федеральная научно-техническая программа развития генетических технологий на 2019— 2030 годы», утв. Постановлением Правительства РФ от 22.04.2019 № 479 <sup>6</sup>                | основная цель Программы — «комплексное решение задач ускоренного развития <i>генетических технологий</i> , в том числе <i>технологий генетического редактирования</i> , и создание научно-технологических заделов и продуктов для медицины, сельского хозяйства и промышленности, а также совершенствование мер предупреждения чрезвычайных ситуаций биологического характера и контроля в этой области, разработка механизмов оперативного внедрения в промышленное производство полученных прикладных результатов деятельности в области <i>генетических технологий</i> ».                                                                                                   |

<sup>1</sup> Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 29.12.2025) «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. 28.11.2011. № 48. Ст. 6724.

<sup>2</sup> Федеральный закон от 12.04.2010 № 61-ФЗ (ред. от 29.12.2025) «Об обращении лекарственных средств» // Собрание законодательства РФ, 19.04.2010. № 16. Ст. 1815.

<sup>3</sup> Федеральный закон 28.12.2024 № 523-ФЗ «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 30.12.2024. № 53 (Ч. I). Ст. 8533.

<sup>4</sup> Указ Президента РФ от 18.06.2024 № 529 «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоёмких технологий» // Собрание законодательства РФ. 24.06.2024. № 26. Ст. 3640.

<sup>5</sup> Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства РФ. 14.10.2019. № 41. Ст. 5700.

<sup>6</sup> Постановление Правительства РФ от 22.04.2019 № 479 (ред. от 05.09.2025) «Об утверждении Федеральной научно-технической программы развития генетических технологий на 2019—2030 годы» // Собрание законодательства РФ. 29.04.2019. № 17. Ст. 2108.

значение, являющийся совокупностью научно и практически обоснованных методов, операций, процессов и (или) средств, включая разрешенные к применению лекарственные препараты, медицинские изделия, биомедицинские клеточные продукты, необходимые для преобразования вещества, энергии, информации»<sup>18</sup>. Приведенное определение по своему содержанию приближено к дефиниции «технологии здоровьесбережения» и значительно сужает понимание медицинских технологий, предлагаемое ГОСТом, в отличие от которого, исключает деятельность в сфере управления, организации системы здравоохранения и коммуникации, что, полагаем, является обоснованным.

### Доктринальные подходы к разграничению исследуемых дефиниций

Исследуемые дефиниции, их содержательное наполнение и отраслевая идентификация устойчиво находятся в фокусе доктринальных изысканий представителей юридической науки, специализирующихся в сфере конституционного, административного, медицинского и био права. В правовой доктрине данные категории традиционно интерпретируются как совокупность методов, средств и процессов, применяемых в системе здравоохранения, и, по сути, охватывают как технологии в узком смысле (инструментальные, аппаратные), так и технологии в широком — организационно-управленческом и профилактическом аспектах.

Определенный интерес представляет подход Д.О. Мешкова, согласно которому *медицинских технологий*, применяемые в конкретных медицинских целях (диагностика, профилактика, лечение и др.), и *технологии в сфере здравоохранения* в целом, не идентичные категории. Ученым предлагается рассматривать «медицинские технологии» и «технологии здравоохранения» как часть и целое, ввиду того что «технологии здравоохранения» значительно шире и включают весь комплекс инструментов, применяемых в системах здравоохранения: управление, логистику, информационные системы и медицинские технологии. В то время как «медицинские технологии (вмешательства, интервенции) непосредственно взаимодействуют с пациентом или здоровым человеком при диагностике, профилактике или лечении. Медицинские технологии включают, но не ограничиваются диагностическими инструментами (опросниками, приборами, реактивами, средствами получения биологических образцов и т. п.), лекарственными препаратами (профилактическими вакцинами, химическими и генно-инженерными биологическими препаратами) и средствами их доставки, хирургическими операциями и радиационной терапией, а также инновационными технологиями, например, транс-

ляционной терапией» [14, с. 66—67]. Выделение медицинских технологий из общей системы технологий в системе здравоохранения вполне оправдано целями их применения.

Данный подход просматривается в исследованиях А.А. Мохова, где медицинские технологии предлагается определить, как «методы, способы, приемы воздействия на объект (организм человека, его системы, органы, ткани, клетки) для достижения задач конкретного медицинского вмешательства или их совокупности (диагностика, лечение, профилактика, реабилитация и др.)»<sup>19</sup> [15, с. 243]. Ученый обосновывает формирования «жесткого каркаса, на основе которого формируется общий, а также специальные правовые режимы отраслевых технологий (там, где это необходимо), а именно, наличие общего типа отраслевых технологий (технологии здравоохранения) позволяет разделить их на роды (например, медицинские, управленческие и некоторые иные) и виды (например, оперативные и иные инвазивные и неинвазивные вмешательства, продуктовые (лекарственные препараты, медизделия и др.))» [15, с. 243—244].

Отдельные виды технологий, например, телемедицинские, по мнению ученых могут относиться, и к технологиям здравоохранения, и к медицинским технологиям, а именно: «1) телемедицинская услуга как форма оказания медицинской помощи, порядок предоставления которой регламентирован положениями приказа Минздрава России № 965н<sup>20</sup>; 2) оказание медицинской помощи с использованием телемедицинских технологий как отдельный самостоятельный вид медицинской деятельности; 3) телемедицинская технология как инновационная цифровая технология, регулируемая нормами экспериментального правового режима в соответствии со статьей 3 (ч. 11) Закона № 323-ФЗ», что детерминирует дифференцированный подход к их правовому регулированию [16, с. 761—762].

Наряду с перечисленными выше, в научной литературе предлагаются смежные термины (табл. 2):

Категоризация медицинских технологий также базироваться также по критерию доступности для пациента, способу правовой интеграции в систему обязательного медицинского страхования (ОМС) или добровольного медицинского страхования (ДМС). Исходя из приведенного выделяются: «1) медицинские технологии, входящие в программы государственных гарантий (ОМС), отказ медицинской организации от предоставления которых может быть основанием

<sup>19</sup> Мохов А.А. Стратегически значимые медицинские технологии: правовой аспект // Государство и право. 2020. № 11. С. 106—114. DOI: 10.31857/S102694520012528-1.

<sup>20</sup> Приказ Минздрава России от 30.11.2017 № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий», документ утратил силу в связи с принятием приказа Минздрава Приказ Минздрава России от 11.04.2025 № 193н «Об утверждении Порядка организации и оказания медицинской помощи с применением телемедицинских технологий» (документ утратил силу) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 15.05.2025.

<sup>18</sup> Паспорт проекта Федерального закона «О внесении изменений в Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации». URL: <https://regulation.gov.ru/projects/163230/> (дата обращения: 12.07.2026).



Таблица 2

| НАИМЕНОВАНИЕ ТЕРМИНА                                                        | СОДЕРЖАТЕЛЬНОЕ НАПОЛНЕНИЕ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Здоровьесберегающие технологии<br>(Р.В. Амелин, Л.В. Бессонов) <sup>7</sup> | 1) технологии управления в сфере медицины (включая планирование, учет, контроль, оказание государственных и муниципальных услуг в сфере здравоохранения); 2) технологии электронного документооборота; 3) телемедицинские технологии; 4) технологии анализа медицинских данных и принятия медицинских решений (включая технологии «больших данных» и искусственного интеллекта, которые могут быть выделены и в отдельные подгруппы);                                                                                                               |
| Электронная медицина<br>(Н.Н. Штыкова) <sup>8</sup>                         | «совокупность информационных (телекоммуникационных) технологий, применяемых в рамках информационного процесса, участниками которого выступают федеральные и региональные органы в сфере здравоохранения, медицинские учреждения, фармацевтические учреждения, медицинские работники и пациенты с целью распознавания, лечения и предупреждения болезней, сохранения и укрепления здоровья и трудоспособности людей, продления жизни»;                                                                                                               |
| Цифровая медицина<br>(А.А. Карцхия) <sup>9</sup>                            | «а) искусственный интеллект (artificial intelligence), который обеспечивает новые решения для диагностики и лечения; б) большие данные (bigdata), которые создают облачные хранилища и служат основой предиктивной аналитики; в) телемедицина и программные приложения, особенно востребованные в эпоху эпидемии; г) блокчейн-технология (blockchain tech), обеспечивающая безопасность и достоверность сведений и обработку данных; д) медицинский интернет вещей (IoT), формирующий экосистему устройств и датчиков для защиты здоровья человек»; |

<sup>7</sup> Амелин Р.В., Бессонов Л.В. О некоторых вопросах правового регулирования телемедицинских технологий // Информационное право. 2019. № 2. С. 21—25.

<sup>8</sup> Штыкова Н.Н. Сущность и проблемы реализации электронной медицины (на примере Владимирской области) // Медицинское право. 2014. № 5. С. 23.

<sup>9</sup> Карцхия А.А. Формирование цифрового здравоохранения как вызов времени // Право и цифровая экономика. 2021. № 3. С. 39. DOI: 10.17803/2618-8198.2021.13.3.039-046.

для иска о некачественном оказании помощи; 2) медицинские технологии, не входящие в ОМС, предоставление которых может осуществляться по договору ДМС (или платных медицинских услуг); 3) экспериментальные (инновационные) медицинские технологии, также не входящие в ОМС, имеющие особый правовой режим, предполагающий подписание информированного добровольного согласия пациента, который предупреждается о возможных рисках» [4, с. 196].

Правовая доктрина, определяя содержательное наполнение исследуемых дефиниций, традиционно интерпретирует технологии как совокупность методов, средств и процессов, применяемых в системе здравоохранения. В фокусе ученых остается реализация вопросов, связанных с разработкой понятийного аппарата в условиях развития технологий [17; 18, с. 150], как необходимого условия защиты прав граждан и национальных интересов в информационной сфере. При этом принципиальное значение для их понятийной идентификации имеет критерий сферы интеграции: в узком смысле технологии понимаются как инструментально-аппаратные и программно-технические решения, интегрируемые непосредственно в клиническую практику (диагностический, лечебный и реабилитационный процессы); в широком же смысле они охватывают организационно-управленческие, превентивные и санитарно-эпидемиологические механизмы, интегрируемые в систему управления здравоохранением и популяционное здоровьесбережение.

## Выводы

Проведенное исследование позволяет сформулировать ряд концептуальных выводов, имеющих как доктринальное, так и прикладное значение для совершенствования правового регулирования.

Современное состояние нормативной базы характеризуется терминологической фрагментарностью и отсутствием легально закрепленных дефиниций ключевых технологических категорий — «технологии здравоохранения», «технологии здоровьесбережения» и «медицинские технологии», что порождает множественность доктринальных интерпретаций, одновременно, затрудняет оценку их безопасности, эффективности и соответствия критериям доказательной медицины.

Полагаем, что научно обоснованное нормативное закрепление рассматриваемых категорий должно строиться на принципе иерархической дифференциации: 1) «технологии здравоохранения» — как наиболее широкая дефиниция, охватывающая организационно-управленческие, санитарно-эпидемиологические, информационно-коммуникационные и иные методы, обеспечивающие функционирование и развитие системы охраны здоровья в целом; 2) «технологии здоровьесбережения» — как понятие, акцентирующее превентивную и поведенческую составляющую, направленную на сохранение и укрепление здоровья населения; 3) «медицинские технологии» — как наиболее содержательно узкая дефиниция, непосред-

ственно связанная с клинической практикой и включающая диагностические, лечебные, хирургические, реабилитационные и иные вмешательства, основанные на применении специализированного оборудования, материалов, биопрепаратов и цифровых алгоритмов и т. д.

С позиций правовой регуляtorики закрепление указанных дефиниций требует глубокого научного обоснования, базирующегося на: системном анализе существующих доктринальных подходов к определению

технологий как объектов правового регулирования; сравнительно-правовом исследовании зарубежных моделей легализации аналогичных категорий; учете межотраслевого характера данных понятий; прогнозировании регуляторных последствий введения тех или иных дефинитивных конструкций для субъектов медицинской деятельности, производителей медицинских изделий, разработчиков цифровых решений и, прежде всего, для пациентов как конечных благополучателей технологического прогресса.

## Литература

1. Дородонова Н.В. Права и свободы человека в векторе конституционализации национального законодательства // Российская правовая система: в поисках национальной идентичности: сб. докл. XIV Московской юридической недели. В 6 ч. Москва, 26—29 ноября 2024 года. М. : ИЦ Университета им. О.Е. Кутафина (МГЮА), 2025. С. 51—54.
2. Цифровизация и биотехнологии в обеспечении права на здоровье в условиях чрезвычайных ситуаций / В.В. Комарова, А.В. Басова, О.А. Белов [и др.]. М. : ООО «Проспект», 2024. 304 с.
3. Шалберкина М.Н. Совершенствование законодательства в сфере здравоохранения: путь к решению проблем или их образованию // Конституционное и муниципальное право. 2025. № 4. С. 60—64. DOI: 10.18572/1812-3767-2025-4-60-64.
4. Технологическое лидерство в России: готовность к изменениям и ответственность за будущее: монография / Под ред. О.Ю. Рыбакова. М. : Проспект, 2026.
5. Проблемы и перспективы правового обеспечения информационной безопасности и цифрового суверенитета / Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов [и др.]. М. : Институт государства и права РАН, 2025. 228 с.
6. Рыбаков О.Ю. Право и целостность правовой системы в эпоху политических и технологических трансформаций // Юридическое образование и наука. 2025. № 9. С. 17—22. DOI: 10.18572/1813-1190-2025-9-17-22.
7. Троян Н.А. Влияние современных платформенных решений как ключевого инструмента государственного управления в условиях цифровой трансформации // Мониторинг правоприменения. 2025. № 1 (54). С. 36—44. DOI: 10.24412/2226-0692-2025-1-36-44.
8. Троян Н.А. Влияние цифровых технологий на процессы государственного управления // Правовая информатика. 2024. № 3. С. 180—187. DOI: 10.24682/1994-1404-2024-3-180-187.
9. Ценность права в условиях цифровой реальности / О.Ю. Рыбаков, М.А. Беляев, Ю.Ю. Ветютнев [и др.]. М. : Проспект, 2026. 312 с.
10. Карцхия А.А. Медицинское право и цифровое здравоохранение: новые перспективы // Медицинское право. 2026. № 1. С. 2—6.
11. Берсенева И.И., Сашко А.А. Роль телемедицины и цифровых технологий в снижении затрат на здравоохранение // Экономика и управление: проблемы, решения. 2025. Т. 6. № 12 (164). С. 231—238. DOI: 10.36871/ek.ur.p.r.2025.12.06.026.
12. Современное состояние развития телемедицины в России: правовое и законодательное регулирование / Р.Е. Петрова, Н.А. Шеяфетдинова, А.А. Соловьев [и др.] // Профилактическая медицина. 2019. Т. 22. № 2. С. 5—9. DOI: 10.17116/profmed2019220215.
13. Нормативно-правовое регулирование рабочего времени медицинских работников: необходимость, возможности и защита прав / Р.Е. Петрова, О.Ю. Рыбаков, Н.А. Шеяфетдинова [и др.] // Профилактическая медицина. 2020. Т. 23. № 3. С. 20—26. DOI: 10.17116/profmed20202303120.
14. Мешков Д.О. Рациональное использование медицинских технологий : монография. М. : ИПУ РАН, 2022. 206 с.
15. Мохов А.А. Современным технологиям здравоохранения — адекватное правовое обеспечение // Правовая политика и правовая жизнь. 2025. № 2. С. 240—248. DOI: 10.24412/1608-8794-2025-2-240-248.
16. Инновационная юриспруденция : учебник / В.В. Блажеев, М.В. Мажорина, В.Б. Агафонов [и др.]. М. : ООО «Проспект», 2025. 912 с.
17. Полякова Т.А., Минбалеев А.В., Наумов В.Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. № 1. 2025. С. 160—173. DOI: 10.31857/S1026945225010148.
18. Троян Н.А. Правовое регулирование цифровых платформ и экосистемы государственных услуг: вектор развития экономики данных в цифровую эпоху // Правовая информатика. 2026. № 1. С. 145—152. DOI: 10.24412/1994-1404-2026-1-00-15.

# “HEALTH TECHNOLOGIES”, “HEALTHCARE TECHNOLOGIES”, “MEDICAL TECHNOLOGIES”: THE RELATIONSHIP OF DEFINITIONS IN THE CONTOUR OF LEGAL REGULATION<sup>21</sup>

Rybakova O.S.<sup>22</sup>

**Keywords:** legal engineering, technological development, healthcare modernization, public administration, artificial intelligence, digital technologies, telemedicine.

## Abstract

**Purpose of the work:** to examine the substantive content of the definitions of “health technologies,” “healthcare technologies,” and “medical technologies” in legal doctrine and legislation; to determine their relationship; to identify the feasibility of their legitimate consolidation; and to substantiate the creation of effective legal instruments for legally supporting the use of technologies in the healthcare system.

**Methods used in the study:** general scientific methods of analysis and synthesis, as well as comparative analysis, are used in the research. A focus is placed on the systems approach.

**Results:** The terminological fragmentation of the legally defined categories under study was identified, which may generate legal uncertainty when assessing their safety, effectiveness, and accessibility for participants in legal relations to achieve constitutionally significant health protection goals. The approaches proposed in this article can serve as a conceptual basis for further discussions and the development of specific regulatory solutions aimed at creating an effective regulatory model for the application of technologies in the healthcare system.

**Research novelty:** The author substantiates a hierarchical differentiation of the definitions under study, where “health technologies” is the broadest definition, encompassing organizational, managerial, sanitary, epidemiological, information, communication, and other methods that ensure the functioning and development of the healthcare system as a whole; “healthcare technologies” is a concept that implies a preventive and behavioral component aimed at maintaining and improving public health; “medical technologies” is understood as the most substantively narrow definition, directly related to clinical practice and including diagnostic, therapeutic, surgical, rehabilitative, and other interventions based on the use of specialized equipment, materials, biopreparations, and digital algorithms.

## References

1. Dorodonova N.V. Prava i svobody cheloveka v vektore konstitutsionalizatsii natsional'nogo zakonodatel'stva // Rossiiskaia pravovaia sistema: v poiskakh natsional'noi identichnosti: sb. dokl. XIV Moskovskoi iuridicheskoi nedeli. V 6 ch. Moskva, 26–29 noiabria 2024 goda. M. : ITs Universiteta im. O.E. Kutafina (MGluA), 2025. S. 51—54.
2. Tsifrovizatsiia i biotekhnologii v obespechenii prava na zdorov'e v usloviakh chrezvychainykh situatsii / V.V. Komarova, A.V. Basova, O.A. Belov [i dr.]. M. : OOO “Prospekt”, 2024. 304 s.
3. Shalberkina M.N. Sovershenstvovanie zakonodatel'stva v sfere zdavookhraneniia: put' k resheniiu problem ili ikh obrazovaniu // Konstitutsionnoe i munitsipal'noe pravo. 2025. No. 4. S. 60—64. DOI: 10.18572/1812-3767-2025-4-60-64.
4. Tekhnologicheskoe liderstvo v Rossii: gotovnost' k izmeneniiam i otvetstvennost' za budushchee: monografiia / Pod red. O.Iu. Rybakova. M. : Prospekt, 2026.
5. Problemy i perspektivy pravovogo obespecheniia informatsionnoi bezopasnosti i tsifrovogo suvereniteta / T.A. Poliakova, A.V. Minbaleev, V.B. Naumov [i dr.]. M. : Institut gosudarstva i prava RAN, 2025. 228 s.
6. Rybakov O.Iu. Pravo i tselostnost' pravovoi sistemy v epokhu politicheskikh i tekhnologicheskikh transformatsii // Iuridicheskoe obrazovanie i nauka. 2025. No. 9. S. 17—22. DOI: 10.18572/1813-1190-2025-9-17-22.

<sup>21</sup> The research was conducted in frame of the federal academic leadership program Priority 2030.

<sup>22</sup> **Olga S. Rybakova**, Ph.D. (Law), Associate Professor, Department of Constitutional and Municipal Law, Kutafin Moscow State Law University (MSAL), Moscow, Russia.  
E-mail: [osrybakova@msal.ru](mailto:osrybakova@msal.ru)

7. Troian N.A. Vliianie sovremennykh platformennykh reshenii kak kliuchevogo instrumenta gosudarstvennogo upravleniia v usloviakh tsifrovoi transformatsii // Monitoring pravoprimeneniia. 2025. No. 1 (54). S. 36—44. DOI: 10.24412/2226-0692-2025-1-36-44.
8. Troian N.A. Vliianie tsifrovyykh tekhnologii na protsessy gosudarstvennogo upravleniia // Pravovaia informatika. 2024. No. 3. S. 180—187. DOI: 10.24682/1994-1404-2024-3-180-187.
9. Tsennost' prava v usloviakh tsifrovoi real'nosti / O.lu. Rybakov, M.A. Beliaev, Iu.Iu. Vetutnev [i dr.]. M. : Prospekt, 2026. 312 s.
10. Kartskhiia A.A. Meditsinskoe pravo i tsifrovoe zdravookhranenie: novye perspektivy // Meditsinskoe pravo. 2026. No. 1. S. 2—6.
11. Bersenev I.I., Sashko A.A. Rol'telemeditsiny i tsifrovyykh tekhnologii v snizhenii zatrat na zdravookhranenie // Ekonomika i upravlenie: problemy, resheniia. 2025. T. 6. No. 12 (164). S. 231—238. DOI: 10.36871/ek.up.p.r.2025.12.06.026.
12. Sovremennoe sostoianie razvitiia telemeditsiny v Rossii: pravovoe i zakonodatel'noe regulirovanie / R.E. Petrova, N.A. Sheiafetdinova, A.A. Solov'ev [i dr.] // Profilakticheskai meditsina. 2019. T. 22. No. 2. S. 5—9. DOI: 10.17116/profmed2019220215.
13. Normativno-pravovoe regulirovanie rabochego vremeni meditsinskikh rabotnikov: neobkhodimost', vozmozhnosti i zashchita prav / R.E. Petrova, O.lu. Rybakov, N.A. Sheiafetdinova [i dr.] // Profilakticheskai meditsina. 2020. T. 23. No. 3. S. 20—26. DOI: 10.17116/profmed20202303120.
14. Meshkov D.O. Ratsional'noe ispol'zovanie meditsinskikh tekhnologii : monografiia. M. : IPU RAN, 2022. 206 s.
15. Mokhov A.A. Sovremennym tekhnologiiam zdravookhraneniia — adekvatnoe pravovoe obespechenie // Pravovaia politika i pravovaia zhizn'. 2025. No. 2. S. 240—248. DOI: 10.24412/1608-8794-2025-2-240-248.
16. Innovatsionnaia iurisprudentsiia : uchebnik / V.V. Blazheev, M.V. Mazhorina, V.B. Agafonov [i dr.]. M. : OOO "Prospekt", 2025. 912 s.
17. Poliakova T.A., Minbaleev A.V., Naumov V.B. Sovremennye priority razvitiia informatsionnogo prava: pravovoe obespechenie gosudarstvennogo suvereniteta i informatsionnoi bezopasnosti v informatsionnom prostranstve Rossii // Gosudarstvo i pravo. No. 1. 2025. S. 160—173. DOI: 10.31857/S1026945225010148.
18. Troian N.A. Pravovoe regulirovanie tsifrovyykh platform i ekosistemy gosudarstvennykh uslug: vektor razvitiia ekonomiki dannykh v tsifrovuiu epokhu // Pravovaia informatika. 2026. No. 1. S. 145—152. DOI: 10.24412/1994-1404-2026-1-00-15.





# ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПРОКУРОРСКОГО НАДЗОРА ЗА ИСПОЛНЕНИЕМ ЗАКОНОВ В СФЕРЕ ПРОФИЛАКТИКИ ДЕВИАНТНОГО ПОВЕДЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ

Рябоконе В.П.<sup>1</sup>

**Ключевые слова:** цифровая трансформация, информационно-аналитическая работа, искусственный интеллект, межведомственное взаимодействие, государственные информационные системы, правовое регулирование, организация надзора, профилактика правонарушений, состояние законности, мониторинг интернет-пространства, прокурорская проверка.

## Аннотация

**Цель работы** состоит в разработке теоретических положений и практических рекомендаций, а также выработке предложений организационного и методического характера по организации прокурорского надзора за исполнением законов в сфере профилактики девиантного поведения несовершеннолетних, направленных на повышение эффективности надзорной деятельности.

**Методы исследования.** В работе использованы общенаучные методы (системно-структурный анализ, формальная логика) и частно-научные методы: формально-юридический, сравнительно-правовой, статистический и социологический (анкетирование). Эмпирическую базу составили результаты анкетирования 114 прокурорских работников из всех федеральных округов Российской Федерации, анализ организационно-распорядительных документов Генеральной прокуратуры и прокуратур субъектов Российской Федерации, а также обобщение практики прокурорского надзора в сфере профилактики девиантного поведения несовершеннолетних.

**Результаты исследования.** Установлено, что действующие организационно-распорядительные документы Генерального прокурора Российской Федерации и прокуроров субъектов Российской Федерации носят фрагментарный характер и ориентированы преимущественно на профилактику правонарушений, не охватывая всей полноты профилактики девиантного поведения, что подтверждается запросом практических работников на комплексное организационно-методическое сопровождение. Доказано, что организация прокурорского надзора в рассматриваемой сфере представляет собой многокомпонентную систему мер, включающую планирование, информационно-аналитическую работу, кадровое и методическое обеспечение, контроль и оценку эффективности. Обосновано, что в условиях цифровой трансформации возрастает значение альтернативных источников информации, а внедрение технологий искусственного интеллекта требует осмотровительного подхода и ведомственного регулирования. Разработаны предложения по совершенствованию организации надзора, включая подготовку единого организационно-распорядительного документа, который позволит закрепить приоритетные направления надзорной деятельности, систематизировать организационные подходы и укрепить межведомственное взаимодействие. Полученные результаты могут быть использованы как в научных исследованиях, так и в практической деятельности органов прокуратуры при организации надзора в рассматриваемой сфере.

DOI: 10.24412/1994-1404-2026-3-00-19

## Введение и постановка задачи

В условиях глубокой цифровой трансформации общественных отношений, деформации правового сознания несовершеннолетних и роста аутоагрессивных проявлений среди молодежи и других форм девиантного поведения<sup>2</sup>, особую актуальность приобретает поиск новых подходов к организации прокурор-

ского надзора за исполнением законов в сфере профилактики девиантного поведения несовершеннолетних, что позволит не только повысить эффективность надзорной деятельности и качество реагирования на нарушения, но и создать условия для становления формирующейся личности [1].

<sup>2</sup> Концепция развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года: утв.

распоряжением Правительства Российской Федерации от 22.03.2017 № 520-р // Собрание законодательства РФ. 2017. № 14. Ст. 2130.

<sup>1</sup> **Рябоконе Вера Пантелеевна**, аспирант Университета прокуратуры Российской Федерации, г. Москва, Россия.  
E-mail: vera\_ryabokon@list.ru

Цифровая среда становится одним из ключевых факторов формирования девиантного поведения, нередко перерастающего в уголовно наказуемые деяния. Подросток, попадая под влияние деструктивной информации через интернет, социальные сети и мессенджеры, сталкивается с пропагандой суицида, радикальных течений и криминальных ценностей, вовлекается в буллинг, кибербуллинг и противоправную деятельность вплоть до участия в диверсиях и террористических актах. Социальные сети выступают одним из основных каналов вовлечения молодежи в экстремистскую деятельность, что создает серьезные риски распространения экстремизма среди российских пользователей [2]. Такое поведение деформирует правосознание несовершеннолетних, закрепляет противоправные установки и создает реальную угрозу их жизни, здоровью и развитию. При этом интернет-пространство отличается высокой скоростью распространения информации и возможностью быстрого воспроизводства запрещенного контента даже после его блокировки, что создает благоприятные условия для вовлечения несовершеннолетних в деструктивные сообщества [3].

В то же время отсутствие в законе легального определения девиантного поведения несовершеннолетнего и механизмов ранней профилактики, а также недостаточная научная проработка надзора в данной сфере правоотношений определяют необходимость исследования его организационных основ [4].

Традиционно организация прокурорского надзора ассоциируется с налаживанием взаимодействия. Однако за этой, безусловно важной, составляющей нередко упускаются иные, не менее значимые элементы: планирование, информационно-аналитическое обеспечение, кадровое и методическое сопровождение, оценка эффективности.

Наиболее полно такое многокомпонентное понимание организации отражается в определении Ю.Е. Винокурова, который рассматривает ее как совокупность внутрисистемных мероприятий, обеспечивающих надлежащее осуществление органами прокуратуры возложенных на них функций и иных направлений деятельности<sup>3</sup>. Данное определение применимо и к организации прокурорского надзора по обеспечению законности в сфере профилактики девиантного поведения несовершеннолетних, под которой следует понимать совокупность внутрисистемных мероприятий, направленных на оптимизацию и повышение эффективности надзорной деятельности, в настоящее время не имеющей под собой целостной правовой основы.

Вопросы организации надзора в рассматриваемой сфере регулируются приказом Генерального прокурора Российской Федерации от 13.12.2021 № 744 «Об организации прокурорского надзора за исполнением законодательства о несовершеннолетних, соблюде-

нием их прав и законных интересов» и приказом от 16.01.2012 № 7 «Об организации работы органов прокуратуры Российской Федерации по противодействию преступности».

Кроме того, прокурорами субъектов Российской Федерации принимаются организационно-распорядительные документы, регулирующие отдельные вопросы организации надзора за исполнением законов в сфере профилактики безнадзорности и правонарушений несовершеннолетних, а также межведомственного взаимодействия и иных направлений профилактики девиантного поведения несовершеннолетних.

Однако действующие организационно-распорядительные документы Генерального прокурора Российской Федерации, а также прокуроров субъектов Российской Федерации, носят фрагментарный характер и ориентированы преимущественно на профилактику безнадзорности и правонарушений, тогда как понятие «профилактика девиантного поведения несовершеннолетних» и «профилактика безнадзорности и правонарушений несовершеннолетних» не являются тождественными [5]. Девиантное поведение несовершеннолетних по своему содержанию значительно шире и включает систему мер, направленных не только на предупреждение противоправных действий, но и на выявление, коррекцию иных форм отклоняющегося поведения: зависимостей, агрессивных и суицидальных проявлений, поведения, создающего угрозу жизни и здоровью ребенка.

При этом вне должного регулирования остаются вопросы комплексного межведомственного взаимодействия, раннего выявления факторов девиантного поведения, координации субъектов профилактики и оценки эффективности надзорной деятельности.

Результаты анкетирования прокурорских работников подтверждают устойчивый запрос на совершенствование организации надзора. В числе приоритетных направлений респонденты назвали распространение положительного опыта и внедрение передовых разработок в деятельность органов прокуратуры (62,2%), увеличение штата прокурорских работников (60,5%), развитие взаимодействия с контролирующими, правоохранительными органами и профильными некоммерческими организациями, в том числе молодежными волонтерскими движениями (45,7%), а также совершенствование научно-методического обеспечения (20,8%)<sup>4</sup>.

Все это актуализирует необходимость не только законодательных изменений, связанных с формированием целостного подхода к организации надзора

<sup>3</sup> Винокуров Ю.Е., Винокуров А.Ю. Прокурорский надзор : учебник для вузов / Под ред. Ю.Е. Винокурова. 18-е изд., перераб. и доп. М. : Юрайт, 2026. С. 48.

<sup>4</sup> Опрос проводился посредством анкетирования проходивших в 2024—2025 г. обучение на факультете профессиональной переподготовки и повышения квалификации Университета прокуратуры Российской Федерации по программе повышения квалификации старших прокуроров, прокуроров управлений (отделов) прокуратур субъектов Российской Федерации, осуществляющих надзор за исполнением законодательства о несовершеннолетних, соблюдением их прав и законных интересов. Всего опрошено 114 человек.

за исполнением законов в сфере профилактики девиантного поведения несовершеннолетних, но и разработки организационно-распорядительного документа Генерального прокурора Российской Федерации, который на ведомственном уровне восполнил бы существующий правовой пробел и задал единые организационные ориентиры для прокуроров, осуществляющих надзор на данном направлении, сконцентрировав их внимание на наиболее актуальных проблемах, включая профилактику незаконного потребления психоактивных веществ, предупреждение суицидального поведения, интернет-зависимости, агрессивного и иного опасного поведения несовершеннолетних. Очевидно, что этот перечень не является исчерпывающим, поскольку девиантное поведение постоянно трансформируется, а значит, и подходы к его профилактике не могут оставаться неизменными.

### **Решение поставленной задачи Организация надзора: понятие и структура**

Решение обозначенных проблем требует четкого представления о том, на чем должна строиться организация надзора в рассматриваемой сфере. Ее фундамент составляют не только традиционные элементы: планирование, контроль, взаимодействие с органами государственной власти, местного самоуправления и общественными институтами, но и тесное взаимодействие с иными подразделениями органов прокуратуры, информационно-аналитическая работа, кадровое и методическое обеспечение работников, оценка эффективности. Именно эти компоненты в совокупности способны обеспечить системность и результативность надзорной деятельности.

В то же время эффективная организация надзора невозможна без глубокого понимания природы девиантного поведения. Прокурор, осуществляющий надзор в этой сфере, должен не только проводить проверку причин и условий, способствующих формированию девиантного поведения, но и в каждом случае учитывать социальные и психологические характеристики как несовершеннолетних, так и членов их семей, устанавливать факторы, влияющие на социализацию подростков, ведущих к формированию девиаций и на этой основе организовывать свою работу.

### **Направления совершенствования организации надзора Информационно-аналитическая работа**

Эффективная организация надзора за исполнением законов в сфере профилактики девиантного поведения несовершеннолетних немыслима без информационно-аналитической работы. Она предполагает сбор, систематизацию и анализ данных о состоянии законности, что позволяет определять приоритеты надзорной деятельности, повышать ее эффективность, а также улучшать качество подготовки и проведения прове-

рок и применения адекватных мер реагирования. Качественная аналитика позволяет переходить от реактивного реагирования к превентивной модели управления рисками, когда элементы предиктивной логики становятся частью организации надзорной [6].

В практике прокурорского надзора основным информационным источником выступают статистические данные о преступности несовершеннолетних, жалобы и обращения граждан, материалы уголовных дел и доследственных проверок по фактам совершения преступлений несовершеннолетними и в отношении них<sup>5</sup>, материалы административной практики. Однако для организации надзора за исполнением законов в сфере профилактики девиантного поведения этого недостаточно.

К числу дополнительных значимых источников необходимо отнести: результаты мониторинга интернет-пространства; публикации в средствах массовой информации; сведения о детях с доправонарушаемыми формами поведения, в том числе пропускающих занятия без уважительных причин в образовательных организациях, употребляющих табачную продукцию, проявляющих интернет-зависимость, кибербуллинг, аутоагрессию (суицидальные проявления), радикализм, самовольные уходы, агрессивное поведение, включая буллинг; данные о семьях в социально опасном положении; учетно-профилактические карточки (дела); практика привлечения к ответственности, данные о помещении несовершеннолетних в специальные учебно-воспитательные учреждения и центры временного содержания; информация из КУСП и иных учетных документов, а также сводки о происшествиях и информация из государственных систем, включая ГИС «Профилактика», ФГИС «Моя школа».

Необходимость поиска альтернативных источников информации, в том числе, позволяющих компенсировать дефицит межведомственного обмена, обусловлена также наличием проблем взаимодействия между органами и учреждениями системы профилактики и прокуратуры в части своевременного информирования о фактах нарушения прав несовершеннолетних с девиантным поведением, на что указали 36,9% опрошенных прокурорских работников<sup>6</sup>.

Поступающая в прокуратуру информация требует систематизации, что позволяет эффективно использовать ее при планировании проверок на следующее полугодие, подготовке аналитических материалов и информировании органов власти о состоянии законности.

Прокуроры могут вести соответствующие накопительные дела по поднадзорным объектам (органам

<sup>5</sup> Огурцова М.Л. Прокурорский надзор за соблюдением жилищных прав несовершеннолетних : дис. ... канд. юрид. наук. М., 2015. С. 81.

<sup>6</sup> Опрос проводился посредством анкетирования проходивших в 2024—2025 г. обучение на факультете профессиональной переподготовки и повышения квалификации Университета прокуратуры Российской Федерации по программе повышения квалификации старших прокуроров, прокуроров управлений (отделов) прокуратур субъектов Российской Федерации, осуществляющих надзор за исполнением законодательства о несовершеннолетних, соблюдением их прав и законных интересов. Всего опрошено 114 человек.

и учреждениям системы профилактики), содержащие статистические отчеты, справки о проверках и копии актов реагирования. Целесообразным представляется формирование баз данных о фактах совершения несовершеннолетними суицидов, их попыток, самовольных уходах как из дома, так и из учреждений с круглосуточным пребыванием, а также ЦВСНП и специальных учебно-воспитательных учреждений закрытого типа, о фактах их вовлечения в криминальную субкультуру.

Как уже было отмечено, важным информационным ресурсом является ГИС «Профилактика», функционирующая с 5 февраля 2025 года. Она содержит сведения о несовершеннолетних, находящихся в трудной жизненной ситуации, социально опасном положении и ходе индивидуальной профилактической работы с несовершеннолетними с девиантным поведением. Использование этой системы позволяет выявлять факты ненадлежащего межведомственного взаимодействия, несвоевременного обмена информацией между субъектами профилактики, случаи жестокого обращения с детьми, а также преступления и правонарушения, совершенные несовершеннолетними и в отношении них.

Систематический сбор информации о состоянии законности в сфере профилактики девиантного поведения несовершеннолетних позволяет отслеживать динамику и структуру правонарушаемости, анализировать факторы, влияющие на нее, а также выявлять новые и более опасные формы противоправной активности на основе данных статистики и эмпирической информации<sup>7</sup>. Состояние законности в сфере защиты прав несовершеннолетних, познаваемое через ее индикаторы, позволяет корректировать надзорную деятельность с учетом факторов, провоцирующих девиантное поведение<sup>8</sup>.

Оценка этих индикаторов строится на аналитических приемах, среди которых наиболее востребованным является сравнительный анализ. В практике прокурорского надзора он предполагает сопоставление текущих показателей с аналогичными показателями прошлых лет; сравнение показателей по территориальному принципу, например, показателей прокуратуры города, района со средними показателями по субъекту Российской Федерации (показателей прокуратуры субъекта Российской Федерации со средними показателями по федеральному округу); сравнение показателей до и после изменения факторов, влияющих на состояние законности (например, введение ответственности за продажу несовершеннолетним никотинсодержащей продукции или потенциально опасных газосодержащих товаров).

Анализ состояния законности в сфере профилактики девиантного поведения несовершеннолетних требует использования данных социальной статистики различных ведомств. Прокурорам следует обращать внимание на абсолютные и относительные показатели преступности несовершеннолетних: количество расследованных преступлений, долю тяжких и особо тяжких преступлений, групповую преступность, структуру по видам. Важное значение имеют сведения о несовершеннолетних, в отношении которых проводилась индивидуальная профилактическая работа<sup>9</sup>, а также о лицах, состоящих на различных видах профилактического учета в органах и учреждениях системы профилактики, о результатах работы этих органов.

Не менее значимы сведения о результатах работы с родителями (иными законными представителями), не исполняющими обязанности по воспитанию детей либо отрицательно влияющими на их поведение, о несовершеннолетних, доставленных в органы внутренних дел или находившихся в розыске, о помещенных в центры временного содержания для несовершеннолетних правонарушителей, а также об участии подразделений органов внутренних дел в выявлении несовершеннолетних, совершивших правонарушения и противоправные деяния<sup>10</sup>.

На современном этапе информационно-аналитическая работа прокурора приобретает новые черты, обусловленные цифровой трансформацией органов прокуратуры. Если ранее прокуроры сталкивались с определенными трудностями оперативного получения информации и ее недостаточным объемом, то сегодня ситуация принципиально иная: налажено электронное взаимодействие с государственными органами, расширены каналы поступления данных, прокуроры имеют доступ к различным информационным базам, что создает основу для более глубокого и оперативного анализа состояния законности в сфере профилактики девиантного поведения несовершеннолетних.

Важную роль в обеспечении законности играет мониторинг интернет-пространства на предмет выявления запрещенного контента, в том числе содержащего признаки цифрового насилия в отношении несовершеннолетних [7]. Он проводится как силами прокуроров, так и с привлечением специалистов (психологов, педагогов, IT-специалистов).

В отдельных прокуратурах субъектов Российской Федерации уделяется внимание расширению технологических возможностей выявления запрещенной

<sup>7</sup> Сушина Т.Е. Детерминанты и индикаторы состояния законности // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. № 1 (51). С. 20.

<sup>8</sup> См.: Капинус О.С., Андреев Б.В., Казарина А.Х. К вопросу о методологии и методике оценки эффективности прокурорского надзора // Вестник Академии Генеральной прокуратуры Российской Федерации. 2012. № 1 (27). С. 23.

<sup>9</sup> Приказ Росстата от 17.10.2023 № 516 «Об утверждении формы федерального статистического наблюдения № 1-КДН «Сведения о деятельности комиссии по делам несовершеннолетних и защите их прав по профилактике безнадзорности и правонарушений несовершеннолетних» с указаниями по ее заполнению».

<sup>10</sup> Сводный отчет по России. Отчет о результатах работы территориальных органов МВД России по предупреждению и пресечению безнадзорности и правонарушений несовершеннолетних // Официальный сайт МВД России. URL: <https://мвд.рф/открытые-данные/7727739372-MVDGIAC312>



информации, а также обеспечению оперативного информационного взаимодействия с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, автоматизации процесса ее блокирования (направления информации для блокировки).

В целях принятия дополнительных мер по предотвращению распространения в сети «Интернет» запрещенной информации в ряде регионов проводилась опытная эксплуатация программы для ЭВМ «Информационно-аналитический комплекс по противодействию незаконным материалам в сети Интернет «ОКО», позволяющей выявлять контент с призывами к экстремистской и террористической деятельности, пропагандирующий суицидальное поведение, в том числе среди несовершеннолетних, а также иные нарушения закона. Хотя в настоящее время этот комплекс не используется, его применение показывает, что повсеместное внедрение подобных информационно-аналитических механизмов может рассматриваться как перспективное направление цифровизации надзорной деятельности.

### **Цифровая трансформация и искусственный интеллект**

Приказом Генерального прокурора Российской Федерации от 11.09.2025 № 621 утверждена Концепция цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2030 года. Ее реализация предполагает использование технологий искусственного интеллекта, в частности, для выявления признаков нарушений на основе анализа оцифрованных данных объектов надзора, работы с обращениями граждан, а также прогнозирования перспективных направлений прокурорской деятельности.

Внедрение технологий искусственного интеллекта в ГИС «Профилактика» позволит повысить уровень координации деятельности органов и учреждений системы профилактики. Такая система способна автоматически сопоставлять сведения различных ведомств, выявлять случаи неполноты профилактической работы и отсутствия необходимого реагирования со стороны уполномоченных органов.

Планом мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям с использованием информационно-коммуникационных технологий, утвержденного распоряжением Правительства Российской Федерации от 14.08.2025 № 2207-р, предусмотрено применение технологий искусственного интеллекта, нейронных сетей и машинного обучения для выявления в сети «Интернет» запрещенной информации, в том числе причиняющей вред здоровью и развитию несовершеннолетних, с последующим ограничением доступа к ней. Ожидается, что это позволит повысить эффективность такой работы.

В этих целях Роскомнадзором еще в 2023 году запущена система автоматического поиска запрещенного

контента «Окукус», которая автоматически выявляет экстремистскую тематику, призывы к массовым незаконным мероприятиям, суициду, пронаркотический контент, пропаганду деструктивных идеологий<sup>11</sup>.

В Китайской Народной Республике также используются новейшие технологии ограничения доступа к запрещенной информации. Там внедрена комплексная система для мониторинга, фильтрации и блокировки интернет-контента для пользователей внутри страны, цель которой — контроль информации и ограничение доступа к веб-сайтам и онлайн-сервисам, признаваемым властями вредными, включая порнографию, азартные игры или насилие<sup>12</sup>. Особый интерес представляет система распознавания лиц «Полуночный патруль», которая автоматически блокирует несовершеннолетним доступ к интернету в ночное время (с 22:00 до 8:00), что позволяет бороться с игроманией и интернет-зависимостью.

Технологии искусственного интеллекта используются в Китае и для раскрытия киберпреступлений. Примером может служить создание в г. Куньшань инновационной команды «Искусственный интеллект (AI) полиции», состоящей из 35 офицеров, которые используют более 220 интеллектуальных моделей на основе больших данных, для оперативного выявления мошеннических схем и отслеживания денежных потоков [8].

Вопросы противодействия киберпреступлениям, в том числе с участием несовершеннолетних, актуальны и для Российской Федерации. Так, впервые в Красноярском крае против несовершеннолетней девушки завели уголовное дело за посредничество в мошеннических банковских переводах (дропперство)<sup>13</sup>. Внедрение подобных технологий могло бы повысить раскрываемость таких преступлений.

Цифровая трансформация будет способствовать повышению эффективности деятельности органов прокуратуры по защите прав несовершеннолетних, прозрачности информационного сопровождения надзорной деятельности и повышению доверия граждан. Вместе с тем она сопряжена с рядом рисков: сохранностью и целостностью данных, используемых в деятельности прокурорских работников; искажениями в работе моделей искусственного интеллекта («галлюцинации», ошибки валидации), отсутствием должного контроля при разработке моделей искусственного интеллекта и неверной интерпретацией полученных результатов, использованием недостоверных данных для обучения алгоритмов, отсутствием методологии оценки эффективности применения искусственного интеллекта, а также этическими

<sup>11</sup> Российская газета. URL: <https://rg.ru/2023/02/13/chto-takoe-okulus-i-zachem-on-nuzhen-roskomnadzoru.html> (дата обращения: 08.09.2025).

<sup>12</sup> Сетевое издание «РБК». URL: <https://trends.rbc.ru/trends/industry/66c6ec999a7947690e6811b7> (дата обращения: 05.09.2025).

<sup>13</sup> Сетевое издание «РБК». URL: <https://www.rbc.ru/rbcfreenews/68be80f69a79479406c894f0> (дата обращения: 15.07.2026).

вопросами его использования [9]. В рамках использования технологий искусственного интеллекта возможны технические сбои и сохраняются риски кибербезопасности [10]. Модели искусственного интеллекта способны за секунды создавать контент, что создает угрозу распространения запрещенной информации и генерации ошибочных сведений [11].

Учитывая эти риски, назрела необходимость разработки правил использования искусственного интеллекта в деятельности органов прокуратуры, в том числе в рамках организации надзора за исполнением законов в сфере профилактики девиантного поведения несовершеннолетних.

### Организационное обеспечение надзорной деятельности

Завершающим этапом информационно-аналитической работы является использование результатов анализа для совершенствования работы прокуроров по надзору за исполнением законов в сфере профилактики девиантного поведения несовершеннолетних, в том числе путем обсуждения состояния законности на заседаниях коллегий, межведомственных и оперативных совещаниях, а также включение в планы работы проверок исполнения законов или анализа состояния законности в рассматриваемой сфере.

Важным элементом организации надзора выступает ее тщательное планирование, под которым следует понимать деятельность работников органов прокуратуры по разработке и реализации основных ее направлений для достижения целей и задач по обеспечению законности в установленные сроки<sup>14</sup>. Планы работы утверждаются на полугодие и в них целесообразно предусматривать наименование объекта проверки, законодательство, подлежащее проверке, сроки и исполнителей. Мотивированные предложения же о включении тех или иных мероприятий в план готовятся на основе анализа состояния законности с учетом требований организационно-распорядительных документов и решений коллегий. При планировании целесообразно выделять зоны повышенного внимания и концентрировать на них усилия прокурорских работников.

Основаниями для включения в план проверочных мероприятий могут являться факты систематического невыполнения органами государственной власти субъектов Российской Федерации, органами местного самоуправления, осуществляющими полномочия в сфере профилактики девиантного поведения несовершеннолетних, законных требований прокурора, ухудшение состояния законности или неудовлетворительные показатели преступности несовершеннолетних.

Неотъемлемой составляющей организации надзора является повышение квалификации прокурорских работников, включая стажировки в вышестоящих прокуратурах и обучение в Университете прокуратуры. Эффективной организации надзора также способствует внутреннее взаимодействие между прокурорами различных направлений, осуществляющими надзор за соблюдением прав несовершеннолетних, за исполнением законов и за процессуальной деятельностью органов предварительного расследования. Значимую роль играет контроль исполнения поручений руководителя прокуратуры субъекта Российской Федерации, прокуратуры города и района, организационно-распорядительных документов и решений коллегий, выполнения плановых мероприятий, а также проверка соблюдения требований к качеству и срокам подготовки документов.

Изучение положительного опыта прокуратур субъектов Российской Федерации позволяет выделить основные направления совершенствования организации надзора за исполнением законов в сфере профилактики девиантного поведения несовершеннолетних: взаимодействие с прокурорами иных сфер законодательства, формирование реестров и баз данных о происшествиях с участием несовершеннолетних и факторах риска (суицидов, попыток суицидов, самовольных уходов и др.), создание межведомственных рабочих групп по отдельным направлениям надзора, подготовка информационных писем и методических рекомендаций, оказание практической помощи нижестоящим прокуратурам, повышение квалификации и проведение стажировки прокурорских работников, использование института наставничества для оказания помощи прокурорским работникам — молодым специалистам и использование информационных технологий.

### Результаты и выводы

Таким образом, организация прокурорского надзора за исполнением законов в сфере профилактики девиантного поведения несовершеннолетних представляет собой многокомпонентную систему мер, направленных на оптимизацию и повышение эффективности надзорной деятельности, включающую планирование, информационно-аналитическую работу, кадровое и методическое обеспечение, контроль и оценку эффективности. Действующие ведомственные акты фрагментарны и не охватывают всей полноты профилактики девиантного поведения, что подтверждается запросом практических работников на комплексное организационно-методическое сопровождение.

В условиях цифровой трансформации возрастает значение альтернативных источников информации, а внедрение технологий искусственного интеллекта требует осмотрительного подхода и ведомственного регулирования.

Решение выявленных проблем видится в разработке единого организационно-распорядительного

<sup>14</sup> Основы организации и управления в органах прокуратуры Российской Федерации : учебник / под ред. А.Ф. Смирнова. М. : Ин-т повышения квалификации руковод. кадров Ген. прокуратуры Рос. Федерации, 2005. С. 34.

документа, который закрепит приоритетные направления прокурорского надзора, систематизирует подходы и укрепит межведомственное взаимодействие.

Предложенные в статье подходы имеют практическое подтверждение и могут быть использованы как

в научных исследованиях по проблемам организации надзора, так и в практической работе органов прокуратуры при совершенствовании надзора за исполнением в сфере профилактики девиантного поведения несовершеннолетних.

## Литература

1. Жубрин Р.В., Ережипалиев Д.И. Обеспечение законности в сфере профилактики правонарушений несовершеннолетних средствами прокурорского надзора // Законность. 2021. № 6. С. 3—7.
2. Кириченко А.В. Правовое регулирование распространения информации в социальных сетях, запрещённых в Российской Федерации // Мониторинг правоприменения. 2024. № 1. С. 50—55.
3. Атагимова Э.И. Информационная составляющая в системе мер профилактики распространения идеологии терроризма и экстремизма в молодёжной среде // Правовая информатика. 2024. № 1. С. 50—57.
4. Рябоконт В.П. Понятие и содержание деятельности прокуратуры по обеспечению законности в сфере профилактики девиантного поведения несовершеннолетних // Вестник Университета прокуратуры Российской Федерации. 2025. № 5 (109). С. 161—181.
5. Рябоконт В.П. Профилактика девиантного поведения несовершеннолетних: междисциплинарный подход и правовые критерии для целей прокурорской деятельности // Законы России: опыт, анализ, практика. 2025. № 12. С. 95—99.
6. Кунев Д.А. Информационно-аналитическая деятельность в органах прокуратуры: становление, развитие, перспективы цифровой трансформации (к 90-летию системы ведомственной аналитики) // Вестник Университета прокуратуры Российской Федерации. 2025. № 4 (108). С. 52—58.
7. Ережипалиев Д.И. Характеристика цифрового насилия в отношении несовершеннолетних, роль прокуратуры в его предупреждении // Вестник Саратовской государственной юридической академии. 2025. № 4 (159). С. 221—229.
8. Антонян Е.А. Китайский опыт борьбы с преступлениями в сфере информационных технологий // Вестник Университета им. О.Е. Кутафина (МГЮА). 2025. № 5. С. 148—158.
9. Мацкевич И.М. Использование технологий искусственного интеллекта в деятельности органов прокуратуры // Законность. 2026. № 4. С. 33—36.
10. Андрианова Н.Г. Правовой режим применения искусственного интеллекта в денежно-кредитной сфере // Правовая информатика. 2026. № 1. С. 100—110.
11. Карцхия А.А., Макаренко Г.И. Правовые проблемы применения искусственного интеллекта в России // Правовая информатика. 2024. № 1. С. 4—19.

**SECTION:**  
**CONSTITUTIONAL LAW**

# FEATURES OF ORGANIZING PROSECUTORIAL SUPERVISION OVER THE IMPLEMENTATION OF LAWS IN THE FIELD OF PREVENTING DEVIANT BEHAVIOR AMONG MINORS

*Ryabokon V.P.<sup>15</sup>*

**Keywords:** digital transformation, information and analytical work, artificial intelligence, interdepartmental cooperation, state information systems, legal regulation, organization of supervision, prevention of offenses, state of legality, monitoring of the Internet space, prosecutorial inspection.

<sup>15</sup> **Vera P. Ryabokon**, Ph.D. student at the University of the Prosecutor's Office of the Russian Federation, Moscow, Russia.  
E-mail: [vera\\_ryabokon@list.ru](mailto:vera_ryabokon@list.ru)

### Abstract

**Purpose of work** is to develop theoretical concepts and practical recommendations, as well as to formulate proposals of an organizational and methodological nature for organizing prosecutorial supervision over the enforcement of laws in the area of preventing deviant behavior among minors, aimed at increasing the effectiveness of supervisory activities.

**Research method.** The study employs general scientific methods (systemic-structural analysis, formal logic) and specific scientific methods: formal-legal, comparative-legal, statistical, and sociological (questionnaire survey). The empirical basis consists of the results of a questionnaire survey of 114 prosecutorial employees from all federal districts of the Russian Federation, an analysis of the organizational and administrative documents of the General Prosecutor's Office and the prosecutor's offices of the constituent entities of the Russian Federation, as well as a synthesis of the practice of prosecutorial supervision in the field of preventing deviant behavior among minors.

**Results of the study.** It has been established that the existing organizational and administrative documents of the Prosecutor General of the Russian Federation and the prosecutors of the constituent entities of the Russian Federation are fragmentary in nature and are primarily focused on the prevention of offenses, without covering the full scope of prevention of deviant behavior, which is confirmed by the request from practitioners for comprehensive organizational and methodological support. It has been proven that the organization of prosecutorial supervision in the area under consideration is a multi-component system of measures that includes planning, information and analytical work, personnel and methodological support, monitoring, and assessment of effectiveness. It has been substantiated that in the context of digital transformation, the importance of alternative sources of information is growing, and the implementation of artificial intelligence technologies requires a cautious approach and departmental regulation. Proposals have been developed to improve the organization of supervision, including the preparation of a unified organizational and administrative document that will make it possible to consolidate the priority areas of supervisory activities, systematize organizational approaches, and strengthen interdepartmental cooperation. The results obtained can be used both in scientific research and in the practical activities of prosecutorial bodies when organizing supervision in the area under consideration.

### References

1. Zhubrin R.V., Erezhipaliev D.I. Obespechenie zakonnosti v sfere profilaktiki pravonarushenii nesovershennoletnikh sredstvami prokurorskogo nadzora // Zakonnost'. 2021. No. 6. S. 3—7.
2. Kirichenko A.V. Pravovoe regulirovanie rasprostraneniia informatsii v sotsial'nykh setiakh, zapreshchennykh v Rossiiskoi Federatsii // Monitoring pravoprimeneniia. 2024. No. 1. S. 50—55.
3. Atagimova E.I. Informatsionnaia sostavliaiushchaia v sisteme mer profilaktiki rasprostraneniia ideologii terrorizma i ekstremizma v molodezhnoi sfere // Pravovaia informatika. 2024. No. 1. S. 50—57.
4. Riabokon' V.P. Poniatie i sodержanie deiatel'nosti prokuratury po obespecheniiu zakonnosti v sfere profilaktiki deviantnogo povedeniia nesovershennoletnikh // Vestnik Universiteta prokuratury Rossiiskoi Federatsii. 2025. No. 5 (109). S. 161—181.
5. Riabokon' V.P. Profilaktika deviantnogo povedeniia nesovershennoletnikh: mezhdistsiplinarnyi podkhod i pravovye kriterii dlia tselei prokurorsko deiatel'nosti // Zakony Rossii: opyt, analiz, praktika. 2025. No. 12. S. 95—99.
6. Kunev D.A. Informatsionno-analiticheskaia deiatel'nost' v organakh prokuratury: stanovlenie, razvitie, perspektivy tsifrovoi transformatsii (k 90-letiiu sistemy vedomstvennoi analitiki) // Vestnik Universiteta prokuratury Rossiiskoi Federatsii. 2025. No. 4 (108). S. 52—58.
7. Erezhipaliev D.I. Kharakteristika tsifrovogo nasiliia v otnoshenii nesovershennoletnikh, rol' prokuratury v ego preduprezhdenii // Vestnik Saratovskoi gosudarstvennoi iuridicheskoi akademii. 2025. No. 4 (159). S. 221—229.
8. Antonian E.A. Kitaiskii opyt bor'by s prestupleniiami v sfere informatsionnykh tekhnologii // Vestnik Universiteta im. O.E. Kutafina (MGlUa). 2025. No. 5. S. 148—158.
9. Matskevich I.M. Ispol'zovanie tekhnologii iskusstvennogo intellekta v deiatel'nosti organov prokuratury // Zakonnost'. 2026. No. 4. S. 33—36.
10. Andrianova N.G. Pravovoi rezhim primeneniia iskusstvennogo intellekta v denezhno-kreditnoi sfere // Pravovaia informatika. 2026. No. 1. S. 100—110.
11. Kartskhiia A.A., Makarenko G.I. Pravovye problemy primeneniia iskusstvennogo intellekta v Rossii // Pravovaia informatika. 2024. No. 1. S. 4—19.





# ПРАВОВЫЕ ПРОБЛЕМЫ ИДЕНТИФИКАЦИИ ДЕСТРУКТИВНОЙ ИНФОРМАЦИИ В СЕТИ «ИНТЕРНЕТ»<sup>1</sup>

Чудесенко А.В.<sup>2</sup>

**Ключевые слова:** идентификация, системы искусственного интеллекта, информационная безопасность, дипфейки, деструктивная информация, маркировка контента, синтетический контент, идентификационные маркеры, цифровые платформы.

## Аннотация

**Цель:** выявить и систематизировать актуальные правовые проблемы, связанные с идентификацией деструктивного контента в глобальной сети «Интернет», а также исследовать системные коллизии, возникающие при квалификации информационных материалов в качестве деструктивного контента и установлении факта их системного деструктивного воздействия, с учетом положений современного российского и зарубежного законодательства, судебной практики и доктринальных источников.

**Методы исследования:** сравнительно правовой метод и методы анализа и синтеза в процессе генезиса современных информационных технологий, в том числе и технологий искусственного интеллекта (ИИ).

**Результаты исследования:** Обоснована необходимость критического осмысления таких категорий, как «идентификация деструктивной информации», «деструктивное информационное воздействие», «дипфейки». Отдельно проанализированы проблемы, связанные с использованием автоматизированных систем мониторинга (ИИ) для идентификации деструктивного контента, включая вопросы их ошибок и ответственности. Выявлено, что алгоритмы машинного обучения, несмотря на высокую скорость обработки данных, демонстрируют существенные ограничения в разграничении маркеров определения деструктивной информации от допустимой для распространения. Анализ показывает, что традиционные подходы к идентификации часто не учитывают контекстуальные и культурные особенности распространения контента, что важно для юридической квалификации категории деструктивной информации. Установлено, что некорректная классификация и отсутствие идентификационных маркеров может нарушать права граждан, а делегирование ответственности разработчикам или операторам систем остается законодательно неурегулированным, что создает серьезные вызовы для правоприменительной практики.

**Новизна:** установлена необходимость разработки механизмов совершенствования российского законодательства и правоприменительной практики в условиях развития технологий ИИ, применяемых для идентификации деструктивной информации. Предполагается алгоритм использования технологий ИИ как дополнительных технических инструментов идентификации деструктивной информации, распространяемой в различных источниках.

DOI: 10.24412/1994-1404-2026-3-00-20

## Введение

Цифровая трансформация общественных отношений привела не только к расширению возможностей создания и распространения информации, но и к качественному изменению самой структуры информационного воздействия. Пользователь сети «Интернет» взаимодействует уже не с относительно обо-

зримым массивом сообщений, подготовленных редакциями средств массовой информации или индивидуальными авторами, а с непрерывно обновляемой средой, содержание которой формируется одновременно людьми, алгоритмическими рекомендательными системами и генеративными моделями. В этих условиях

<sup>1</sup> Статья написана в рамках Государственного задания FMUZ-2024-0035 «Обеспечение цифрового суверенитета и информационной безопасности правовыми средствами».

<sup>2</sup> Чудесенко Антон Вадимович, аспирант Института государства и права Российской академии наук (ИГП РАН), младший научный сотрудник сектора информационного права и международной информационной безопасности ИГП РАН, г. Москва, Российская Федерация.

E-mail: a.chudesenko@mail.ru

дефицит времени и навыков для проверки источника, контекста и достоверности контента становится самостоятельным фактором уязвимости личности. Поэтому проблема деструктивного контента не исчерпывается наличием отдельного запрещенного материала: она связана также со скоростью его воспроизводства, масштабом адресного распространения и способностью цифровой инфраструктуры придавать ему видимость достоверного сообщения.

В соответствии с положениями Стратегии национальной безопасности Российской Федерации (Указ Президента РФ от 02.07.2021 № 400)<sup>3</sup> указанные процессы развиваются в условиях, когда обеспечение информационной безопасности, укрепление государственного суверенитета и достижение технологической независимости отнесены к числу приоритетов государственной политики. Стратегия национальной безопасности Российской Федерации указывает на распространение заведомо недостоверной информации, пропаганду противоправного поведения и использование информационно-коммуникационных технологий для деструктивного воздействия на личность, общество и государство. В свою очередь, Стратегия научно-технологического развития Российской Федерации<sup>4</sup> связывает ответ на большие вызовы с освоением передовых цифровых технологий, обработкой больших данных и созданием отечественных технологических решений. Следовательно, применение искусственного интеллекта (ИИ) в информационной сфере имеет двойственную правовую природу: те же инструменты, которые увеличивают производительность создания контента и позволяют имитировать реальные объекты, могут использоваться для автоматизированного выявления противоправных материалов, проверки их происхождения и снижения нагрузки на ресурсы, осуществляющие идентификацию и модерацию деструктивной информации [1, с. 85].

В настоящее время обеспечение развития научно-технологической политики непосредственно связано с обеспечением государственного, информационного и технологического суверенитета. Т.А. Полякова и Н.А. Троян справедливо рассматривают научно-технологическую политику не как изолированное направление поддержки инноваций, а как механизм формирования собственной инфраструктуры развития, способной обеспечить национальные интересы в условиях цифровой трансформации [2, с. 195]. Такой подход особенно значим применительно к системам анализа контента: зависимость от иностранных моделей, закрытых наборов данных и непрозрачных критериев модерации способна воспроизводить внешние цен-

ностные и правовые установки внутри национального информационного пространства.

Одновременно возрастает криминогенное использование цифрового контента. Т.А. Полякова и А.А. Смирнов отмечают ускоренное изменение форм киберпреступности, ее транснациональный характер и необходимость межотраслевого развития правовых средств противодействия [3, с. 238].

Важно отметить, что развитие генеративных технологий производства синтетического контента существенно снижает стоимость производства правдоподобных аудиовизуальных подделок и любых других видов информации. Опубликованные в августе 2026 г. результаты отраслевого опроса показывают, что ИИ при подготовке контента используют 73% опрошенных компаний и 45% опрошенных блогеров<sup>5</sup>. Эти данные характеризуют распространенность инструмента среди участников конкретного исследования, но не долю синтетических материалов в сети «Интернет». Тем не менее они подтверждают, что машинная генерация перестала быть исключительной практикой и требует устойчивого режима правового регулирования.

В корпоративном секторе эта проблема дополняется рисками компрометации деловой переписки, подмены управленческих распоряжений и воздействия на работников. А.А. Карцхия и Г.И. Макаренко связывают современную парадигму кибербезопасности с соединением признаков организованной и экономической преступности, совершаемой с использованием цифровой техники, программного обеспечения и ИИ-агентов [4, с. 151].

Прежде чем перейти к рассмотрению возможностей применения систем искусственного интеллекта в решение задачи идентификации и борьбы с распространением деструктивной информации следует определить правовой режим идентификации и подходы к определению данного понятия.

### Идентификация деструктивной информации и маркировка синтетического контента как информационно-правовая задача

При анализе проблем идентификации необходимо обеспечить комплексное понимание дефиниции процесса идентификации. По мнению В.Б. Наумова, идентификация — информационный процесс, направленный на установление субъектного и (или) объектного состава общественных отношений на основе идентификатора или их совокупности в соответствии с содержанием отношений и их правовой природой [5, с. 11]. Таким образом, идентификация представляется как комплексный технологический и юридический процесс, включающий в себя определенные критерии, определяемые

<sup>3</sup> Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 11.10.2025.

<sup>4</sup> Указ Президента РФ от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации» // Собрание законодательства РФ. 2024. № 10. Ст. 1373.

<sup>5</sup> Игнатьев Д. Более 70% компаний и почти половина блогеров используют ИИ для создания контента // Ведомости. 11.08.2026. URL: <https://www.vedomosti.ru/media/articles/2026/08/11/1220163-bolee-70-kompanii-i-pochti-polovina-bloggerov-ispolzuyut-ii> (дата обращения: 31.08.2026).

идентификатором. В вопросе определения деструктивности информации идентификационные маркеры могут определяться по критериям достоверности информации, наличия в ней элементов, направленных на нанесения ущерба национальным интересам и иным критериям определенных концептуальными положениями о информационно-психологической безопасности и защиты от деструктивного информационного воздействия, определенных как цели реализации национальной политики обеспечения информационного суверенитета Российской Федерации.

Необходимо также отличать объект идентификации от предмета оценки. Объектом идентификации является конкретный информационный материал, его источник, автор, распространитель, изображенное лицо, использованная модель либо совокупность технических признаков происхождения. Состояние защищенности личности, общества и государства не может быть «идентифицировано» как единица контента; оно является предметом системной оценки на основе показателей риска, распространенности угроз, устойчивости инфраструктуры и эффективности правоприменения. Такое разграничение имеет методологическое значение: автоматизированная система способна присвоить материалу вероятностный класс, однако вывод об уровне информационно-психологической безопасности требует более широкого междисциплинарного анализа.

Практическая сложность идентификации определяется масштабом информационного оборота. По сообщению представителя Роскомнадзора, опубликованному «Ведомостями», в 2025 г. доступ был ограничен к 1,289 млн материалов против 810,5 тыс. в 2024 г.<sup>6</sup>; мониторинг охватывал крупнейшие социальные сети, видеосервисы и мессенджеры. Эта динамика не доказывает пропорционального роста объема противоправной информации, поскольку на показатель влияют расширение мониторинга, изменение перечней запрещенного контента и совершенствование средств обнаружения. Однако она демонстрирует, что проверка каждого материала исключительно вручную организационно невозможна. В результате ИИ приобретает значение инфраструктурного средства осуществления отбора и выделения критически важных маркеров деструктивного контента, а не автономного субъекта осуществления юридической квалификации.

Особенно сложной задачей при идентификации деструктивного и синтетического контента является обнаружение дипфейков. Поэтому перспективной представляется не ставка на один универсальный детектор, а сочетание нескольких источников доказательственной информации: анализа физических и биометрических несоответствий, проверки аудио-характеристик, сопоставления с известными образцами существую-

щего контента, исследования метаданных и цепочки происхождения, а также оценки контекста публикации. В.Б. Наумов обоснованно связывает противодействие дипфейкам с развитием института идентификации, обеспечением достоверности информации и доверия к цифровым коммуникациям, предлагая несколько информационно-правовых моделей и специальные изменения информационного законодательства [6, с. 143].

Принятие Федерального закона № 243-ФЗ стало первым системным шагом федерального законодателя к регулированию разработки, внедрения и применения больших фундаментальных моделей ИИ. Закон определяет ИИ, большую фундаментальную модель, состав данных, обучение модели и ее разработчика, затрагивает вопросы и идентификации, и маркировки контента, созданного с применением технологий ИИ. Статья 9 указанного закона носит наименование «Маркировка информационного материала, созданного с применением больших фундаментальных моделей искусственного интеллекта». Сам факт появления этой статьи имеет принципиальное значение: законодатель признал информационное предупреждение самостоятельным средством обеспечения прозрачности происхождения контента. Вместе с тем содержание нормы не позволяет утверждать, что в России уже введена универсальная обязательная маркировка ИИ-контента. Часть 1 статьи 9 предусматривает, что лицу, применяющему большую фундаментальную модель для создания материала в аудио- и (или) визуальной форме, обеспечивается возможность размещения предупреждения. Согласно части 2 формат, содержание и порядок его размещения устанавливаются соглашением между пользователем и лицом, предоставляющим возможность применения модели. Часть 3 обязывает владельца крупного сайта, информационной системы или программы, отвечающих указанным в законе критериям аудитории и функционального назначения, обеспечить пользователям возможность размещения такого предупреждения<sup>7</sup>. Таким образом, статья 9 закрепляет обязанность создать техническую возможность, но не прямую обязанность автора воспользоваться ею. Закон также не запрещает намеренное удаление технического маркера и не устанавливает специального состава ответственности за распространение немаркированного синтетического материала. Отсылочная статья 11 говорит об ответственности в соответствии с законодательством Российской Федерации, однако сама по себе не образует достаточного основания для санкции, если конкретная нарушенная обязанность и состав правонарушения не закреплены в иных нормах.

Важно обратить внимание и на срок вступления в силу данных законодательных положений. Федеральный закон № 243-ФЗ в основной части вступает в силу 1 сентября 2026 г., тогда как статьи 8—10, включая

<sup>6</sup> РКН в 2025 году удалил на 59% больше запрещенных материалов // Коммерсант. 19.01.2026. URL: <https://www.kommersant.ru/doc/8361576> (дата обращения: 31.08.2026).

<sup>7</sup> Федеральный закон от 26.07.2026 № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации», ч. 1.2 ст. 13.

регулирование маркировки, начинают действовать с 1 марта 2027 г. Переходный период представляется возможным использовать для подготовки согласованного регулирования, поскольку предоставление платформами несовместимых между собой предупреждений не позволит обеспечить процедуру устойчивой идентификации контента.

### **Искусственный интеллект в идентификации и модерации деструктивной информации**

Массовый информационный оборот объективно требует перехода от последовательной ручной проверки к гибридной модели модерации. Использование систем искусственного интеллекта потенциально снижает трудозатраты человека на просмотр заведомо огромного массива информации и позволяет направить квалифицированных специалистов на сложные случаи регулирования. В этом смысле автоматизация является не отказом от правовой оценки, а способом сохранить ее возможность при объеме данных, который превышает человеческие ресурсы.

На практике российская система мониторинга уже развивается по пути функционального разделения анализа текста, изображений, видео и прогнозной аналитики с использованием технологий автоматизации. В открытых источниках системы «Мир», «Окулус» и «Вебрь» описываются как инструменты сбора и текстового анализа, распознавания аудиовизуальных материалов и прогнозного выявления угроз<sup>8</sup>. Независимо от конкретных технических характеристик этих решений дальнейшее развитие должно ориентироваться не только на увеличение количества обработанных единиц контента, но и на проверяемое качество. Учитывая ранее описанные объемы распространения деструктивной информации, «ручная» обработка входящего информационного потока является физически сложной задачей. Поэтому использование систем ИИ может быть представлено как дополнительная вычислительная мощность для выполнения поставленных задач.

Применение систем ИИ способно повысить точность обнаружения деструктивной информации лишь при соблюдении двух условий: детекторы должны непрерывно обновляться и проверяться на новых типах генерации, включая материалы, специально созданные для обхода обнаружения; техническая вероятность не должна автоматически преобразовываться в юридический факт. Такой порядок позволяет согласовать автоматизацию с подходом, обеспечивающим защиту интересов и прав человека в условиях такого стремительного развития технологий. Развиваемое В.Б. Наумовым право на отказ от цифровых технологий

направлено на защиту человека как объективно слабой стороны и предполагает возможность выбора в тех правоотношениях, где безальтернативное применение технологии способно существенно затронуть права и свободы [7, с. 29]. Однако указанное право не означает запрета на автоматизированный анализ общедоступного контента или требования проверять весь информационный поток исключительно вручную. В сфере модерации содержанием гарантии должно стать не право исключить материал из машинного сканирования, а право на уведомление о применении автоматизированного решения, получение понятного основания ограничения и рассмотрение возражения человеком, когда мера затрагивает доступ к информации, аккаунт, репутацию или иные законные интересы пользователя. В научной модели безопасного ИИ в обязательном порядке предусматривают право на отказ, доверие, безопасность и постоянное развитие предметного законодательства образуют взаимосвязанные элементы, а не взаимоисключающие требования [8, с. 6]. Следует отметить, что развитие правового регулирования маркировки и автоматизированной модерации деструктивной информации целесообразно осуществлять посредством согласованного пакета изменений.

Представляется возможным внести дополнения в Федеральный закон № 243-ФЗ: в статье 3 следует определить категории «синтетический информационный материал», «существенное преобразование» и «дипфейк» [9, с. 12]. Статью 9 следует дополнить обязательной маркировкой публично распространяемого синтетического аудио- и визуального материала, если его характер способен сформировать у обычного пользователя представление о достоверном отображении реального лица, события или высказывания.

Следующим шагом может быть представлено дополнение положений ФЗ-149. Для владельцев социальных сетей, видеохостингов и иных крупных платформ следует установить обязанности: принимать и сохранять совместимые маркеры происхождения; отображать предупреждение в интерфейсе; не удалять его при технической обработке файла; предоставлять средство сообщения о поддельном изображении или голосе; проводить проверку по обращению изображенного лица; обеспечивать человеческий пересмотр значимого решения; публиковать агрегированную отчетность о выявлении и маркировке. В законе следует разграничить маркировку, ограничение рекомендательного распространения и ограничение доступа как меры разной интенсивности. Наличие синтетического происхождения само по себе может обосновывать предупреждение, но не автоматическую блокировку.

Также следует обратить внимание на процесс совершенствования национального законодательства в части разработки подзаконных актов [10, с. 18]. Правительство Российской Федерации, используя полномочие устанавливать требования по предотвращению рисков применения больших фундаментальных

<sup>8</sup> Количество удаленных РКН запрещенных материалов в 2025 году выросло на 59% // Ведомости. 19.01.2026. URL: <https://www.vedomosti.ru/technology/news/2026/01/19/1170082-kolichestvo-udalennih-rkn-zapreshchennih> (дата обращения: 31.08.2026).



моделей, может определить категории материалов, подлежащих обязательной маркировке, общие исключения и распределение компетенции федеральных органов<sup>9</sup>. Минцифры России возможно наделить полномочием утвердить единые требования к содержанию и визуальному формату предупреждения, составу машиночитаемых сведений, совместимости платформенных интерфейсов и устойчивости технического маркера. Роскомнадзору — утвердить методику контроля исполнения требований, правила проведения контрольных испытаний, показатели качества автоматизированного обнаружения, формы отчетности и порядок взаимодействия с платформами. Технические параметры могут развиваться в национальных стандартах, однако обязательные элементы, влияющие на права и обязанности, должны иметь прямое нормативное основание.

Предлагаемое распределение функций не означает уравнивание национального законодательства и внутренних правил цифровых платформ в смысле их равенства. Внутренние правила являются частным регулятором и должны приводиться в соответствие с императивными требованиями российского права. Вместе с тем законодательство должно учитывать техническую архитектуру платформ и обеспечивать их специфику. Оптимальной является модель, при которой федеральный закон определяет обязанность, субъектов, основания, основные права и последствия; Правительство — риск-категории и общую процедуру; Минцифры — технологический формат; Роскомнадзор — контрольную методику; платформы — конкретную реализацию интерфейса и внутренний порядок рассмотрения обращений в установленных пределах.

### **Заключение**

Проведенный анализ позволяет констатировать системный характер возникающих информационных, технических и правовых, стоящих перед правовой системой РФ в сфере идентификации деструктивного контента и информационного воздействия. Существующая парадигма регулирования, основанная на устаревших подходах, демонстрирует свою недостаточную эффективность перед создаваемыми в огромных масштабах единицами деструктивного контента, наносящих ущерб защищенности общества и государственным интересам [11, с. 229]. Для преодоления возникшей коллизии необходима комплексная модернизация по следующим направлениям.

1) Первоочередным законодательным решением представляется согласованный пакет поправок в Федеральные законы № 243-ФЗ и № 149-ФЗ. В них следует закрепить понятия «синтетического материала» и дипфейка, установить обязательную маркировку «высокорискового» публичного аудио- и визуального контента;

определить обязанности крупных платформ сохранять и отображать маркеры, принимать обращения и обеспечивать финальное утверждение решения человеком. Предлагается определить законодательстве обязательные маркеры идентификации деструктивного контента, к числу которых могут быть отнесены: видимое предупреждение, машиночитаемые метаданные/cookie-данные и файлы, устойчивое свидетельство происхождения (источника происхождения контента — человек или ИИ). Такое сочетание повысит качество идентификации даже при удалении одного из элементов.

2) Представляется возможным внесение изменений в акты стратегического планирования и точечные изменения действующих федеральных законов в части расширения понятий «цифровой», «когнитивной зависимости», «медиасуверенитета», «когнитивного суверенитета». Представляется важным закрепить установить обязанности для владельцев крупных информационных, социальных и сетевых платформ по выявлению и маркировке контента, содержащего элементы скрытого психологического воздействия, а также контента, созданного с помощью ИИ-инструментов. Их обязанности могут быть расширены и закреплены в рамках редакции ФЗ-149 и КоАП РФ в части разработки редакции специализированных составов, относящихся к реализации положений ст. 9 ФЗ-244 с определением границ ответственности указанных субъектов.

3) Реализация развития использование технологий искусственного интеллекта для идентификации и модерации информации, обладающей деструктивным воздействием. Помимо этого, необходимо обеспечить развитие собственных LLM-моделей искусственного интеллекта, расположенных на российских серверах и обучаемых с особенностями восприятия контента и информации в рамках российской ментальной среды [12, с. 35]. Комплексное развитие и поддержка собственных информационных систем и систем ИИ позволит повысить защищенность национального суверенитета в условиях вызовов и угроз, а также поддержать и укрепить уровень информационной безопасности и защиты национальных интересов государства. Такой комплексный подход, сочетающий технологическое развитие, законодательное совершенствование и формирование цифровой культуры, позволит обеспечить информационную безопасность личности и общества в условиях развивающейся цифровой эпохи.

<sup>9</sup> Федеральный закон от 26.07.2026 № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации», п. 4 ч. 2 ст. 5.

Литература

1. Полякова Т.А., Минбалеев А.В., Наумов В.Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. 2025. № 1. С. 160—173. DOI: 10.31857/S1026945225010148. EDN: HKYGV1.
2. Полякова Т.А., Троян Н.А. Научно-технологическая политика как механизм обеспечения государственного суверенитета в условиях цифровой трансформации // Государство и право. 2026. № 5. С. 193—203. DOI: 10.7868/S2713039826050164.
3. Полякова Т.А., Смирнов А.А. Противодействие киберпреступности в новой цифровой реальности: вызовы и правовые решения // Государство и право. 2026. № 2. С. 236—246. DOI: 10.7868/S2713039826020184.
4. Карцхия А.А., Макаренко Г.И. Кибербезопасность: корпоративно-правовой аспект // Вопросы кибербезопасности. 2026. № 2 (72). С. 149—156. DOI: 10.21681/2311-3456-2026-2-149-156.
5. Наумов В.Б. Институт идентификации в информационном праве : автореф. дис. ... д-ра юрид. наук: 12.00.13 / Наумов Виктор Борисович. М. : ИГП РАН, 2020. С. 11.
6. Наумов В.Б. Борьба с дипфейками: информационно-правовые модели и законодательные решения // Государство и право. 2026. № 4. С. 142—147. DOI: 10.7868/S2713039826040130.
7. Наумов В.Б. Право на отказ от цифровых технологий в сфере искусственного интеллекта // Вестник Университета им. О.Е. Кутафина (МГЮА). 2024. № 10 (122). С. 26—36. DOI: 10.17803/2311-5998.2024.122.10.026-036.
8. Карцхия А.А., Ивлиев Г.П. Современное понимание искусственного интеллекта: правовой аспект // Интеллектуальная собственность. Промышленная собственность. 2025. № 4. С. 4—12.
9. Наумов В.Б. Десять идей для законопроекта о безопасном искусственном интеллекте в России // Юрист. 2026. № 5. С. 10—17. DOI: 10.18572/1812-3929-2026-5-10-17.
10. Карцхия А.А., Макаренко Г.И. Правовые проблемы применения искусственного интеллекта в России // Правовая информатика. 2024. № 1. С. 4-19. DOI: 10.21681/1994-1404-2024-1-4-19.
11. Карцхия А.А., Макаренко Г.И. Актуальные тренды в развитии искусственного интеллекта // Правовая информатика. 2025. № 3. С. 219-231. DOI: 10.24412/1994-1404-2025-3-00-24.
12. Атабеков А.Р. Обеспечение автономности принятия решения искусственным интеллектом для целей публичных правоотношений // Административное и муниципальное право. 2023. № 1. С. 29-36. DOI: 10.7256/2454-0595.2023.1.39893.

SECTION:  
CONSTITUTIONAL LAW

## LEGAL PROBLEMS OF IDENTIFYING DESTRUCTIVE INFORMATION ON THE INTERNET

Chudesenko A.V.<sup>10</sup>

**Keywords:** *identification, artificial intelligence systems, information security, deepfakes, destructive information, content labeling, synthetic content, identification markers, digital platforms.*

### Abstract

**Purpose of the work:** *to identify and systematize current legal issues related to the identification of destructive content on the global Internet, as well as to examine systemic conflicts arising in the qualification of information materials as destructive content and in establishing the fact of their systemic destructive impact, taking into account the provisions of modern Russian and foreign legislation, judicial practice, and doctrinal sources.*

**Research methods:** *comparative legal method and methods of analysis and synthesis in the context of the genesis of modern information technologies, including artificial intelligence technologies.*

---

<sup>10</sup> Anton V. Chudesenko, Ph.D. student at the Institute of State and Law of the Russian Academy of Sciences (ISL RAS), Junior Researcher at the Sector of Information Technology Law and International Information Security of the ISL RAS, Moscow, Russian Federation.  
E-mail: [a.chudesenko@mail.ru](mailto:a.chudesenko@mail.ru)

**Research results:** The necessity of a critical rethinking of such categories as “identification of destructive information,” “destructive information impact,” and “deepfakes” has been substantiated. The problems associated with the use of automated monitoring systems (artificial intelligence) for identifying destructive content, including issues of their errors and liability, are analyzed separately. It has been revealed that machine learning algorithms, despite their high data processing speed, demonstrate significant limitations in distinguishing markers for identifying destructive information from content permissible for distribution. The analysis shows that traditional identification approaches often fail to take into account the contextual and cultural features of content dissemination, which is important for the legal qualification of the category of destructive information. It has been established that incorrect classification and the absence of identification markers may violate citizens’ rights, while the delegation of responsibility to developers or system operators remains legally unregulated, creating serious challenges for law enforcement practice.

**Novelty:** the necessity of developing mechanisms for improving Russian legislation and law enforcement practice in the context of the development of artificial intelligence technologies used for identifying destructive information is established. An algorithm is proposed for using artificial intelligence technologies as additional technical tools for identifying destructive information disseminated through various sources.

## References

1. Poliakova T.A., Minbaleev A.V., Naumov V.B. Sovremennye priority razvitiia informatsionnogo prava: pravovoe obespechenie gosudarstvennogo suvereniteta i informatsionnoi bezopasnosti v informatsionnom prostranstve Rossii // Gosudarstvo i pravo. 2025. No. 1. S. 160—173. DOI: 10.31857/S1026945225010148. EDN: HKYGVl.
2. Poliakova T.A., Troian N.A. Nauchno-tekhnologicheskaya politika kak mekhanizm obespecheniia gosudarstvennogo suvereniteta v usloviakh tsifrovoy transformatsii // Gosudarstvo i pravo. 2026. No. 5. S. 193—203. DOI: 10.7868/S2713039826050164.
3. Poliakova T.A., Smirnov A.A. Protivodeistvie kiberprestupnosti v novoi tsifrovai real’nosti: vyzovy i pravovye resheniia // Gosudarstvo i pravo. 2026. No. 2. S. 236—246. DOI: 10.7868/S2713039826020184.
4. Kartskhiia A.A., Makarenko G.I. Kiberbezopasnost’: korporativno-pravovoi aspekt // Voprosy kiberbezopasnosti. 2026. No. 2 (72). S. 149—156. DOI: 10.21681/2311-3456-2026-2-149-156.
5. Naumov V.B. Institut identifikatsii v informatsionnom prave : avtoref. dis. ... d-ra iurid. nauk: 12.00.13 / Naumov Viktor Borisovich. M. : IGP RAN, 2020. S. 11.
6. Naumov V.B. Bor’ba s dipfeikami: informatsionno-pravovye modeli i zakonodatel’nye resheniia // Gosudarstvo i pravo. 2026. No. 4. S. 142—147. DOI: 10.7868/S2713039826040130.
7. Naumov V.B. Pravo na otkaz ot tsifrovyykh tekhnologii v sfere iskusstvennogo intellekta // Vestnik Universiteta im. O.E. Kutafina (MGLuA). 2024. No. 10 (122). S. 26—36. DOI: 10.17803/2311-5998.2024.122.10.026-036.
8. Kartskhiia A.A., Ivliev G.P. Sovremennoe ponimanie iskusstvennogo intellekta: pravovoi aspekt // Intellektual’naia sobstvennost’. Promyshlennaia sobstvennost’. 2025. No. 4. S. 4—12.
9. Naumov V.B. Desiat’ idei dlia zakonoproekta o bezopasnom iskusstvennom intellekte v Rossii // Iurist. 2026. No. 5. S. 10—17. DOI: 10.18572/1812-3929-2026-5-10-17.
10. Kartskhiia A.A., Makarenko G.I. Pravovye problemy primeneniia iskusstvennogo intellekta v Rossii // Pravovaia informatika. 2024. No. 1. S. 4—19. DOI: 10.21681/1994-1404-2024-1-4-19.
11. Kartskhiia A.A., Makarenko G.I. Aktual’nye trendy v razvitii iskusstvennogo intellekta // Pravovaia informatika. 2025. No. 3. S. 219—231. DOI: 10.24412/1994-1404-2025-3-00-24.
12. Atabekov A.R. Obespechenie avtonomnosti priniatiia resheniia iskusstvennyi intellektom dlia tselei publitskikh pravootnoshenii // Administrativnoe i munitsipal’noe pravo. 2023. No. 1. S. 29—36. DOI: 10.7256/2454-0595.2023.1.39893.



# ЦИФРОВЫЕ ЛОГИСТИЧЕСКИЕ ПЛАТФОРМЫ И АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ<sup>1</sup>

Сморчкова Л.Н.<sup>2</sup>

**Ключевые слова:** цифровые платформы, хозяйственные связи, логистика, административно-правовое регулирование, государственное воздействие, Национальная цифровая транспортно-логистическая платформа.

## Аннотация

**Цель:** проанализировать цифровые логистические платформы как средство организации хозяйственных связей в данной сфере экономических отношений, как потенциальный предмет правового регулирования и как инструмент административно-правового упорядочивания и контроля в логистике.

**Методы:** системный и экспертный анализ, сравнительно-правовой, формально-юридический методы.

**Результат:** Доказана актуальность правового регулирования отношений, складывающихся при организации, функционировании и посредничестве цифровых логистических платформ, активно используемых в настоящее время хозяйствующими субъектами при ведении своей деятельности, с учетом их существующего многообразия и видовых особенностей. Выявлена необходимость создания прозрачности отношений участников логистических цепочек путем ведения электронного документооборота, ведение различного рода реестров, прослеживаемости совершаемых сделок и иных юридически значимых действий. Показана значимость правового участия государства как с целью упорядочивания логистической сферы посредством использования административно-правовых средств, так и целью осуществления правового контроля деятельности участников логистических отношений посредством создания и внедрения Национальной цифровой транспортно-логистической платформы Российской Федерации «ГосЛог». Сделан вывод, что государственная платформа «ГосЛог» своим функционалом в определенной мере выполняет функцию правового регулятора.

**Практическая ценность:** результаты исследования могут быть учтены при создании и последующем совершенствовании правового регулирования создания и функционирования цифровых логистических платформ как на высшем федеральном уровне, так и в подзаконном законодательстве.

DOI: 10.24412/1994-1404-2026-3-00-21

## Введение

Современный уровень развития информационных технологий позволяет выстраивать юридически значимые связи между хозяйствующими субъектами, основываясь на совершенно иных механизмах и методах взаимодействия. В этом отношении очень перспективно выглядит такая форма посредничества, как цифровая платформа, которая в соответствии с пунктом 2 статьи 2 Федерального закона от 31 июля 2025 года № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации»<sup>3</sup>

(далее — Федеральный закон о платформенной экономике) представляет собой информационную систему (также возможно сайт в сети «Интернет» или программу для ЭВМ), обеспечивающую технические, организационные, информационные и иные возможности для взаимодействия неограниченного круга лиц, в том числе в целях обмена информацией и ее распространения, продажи товаров, выполнения работ, оказания услуг.

Иными словами, цифровая платформа — это такой информационный (цифровой) ресурс, использование которого облегчает формирование между заинтересованными субъектами устойчивых связей на основе

<sup>3</sup> Собрание законодательства Российской Федерации, № 31 от 4 августа 2025 г., ст. 4643.

<sup>1</sup> Публикация подготовлена в рамках выполнения НИР № FMUZ-2024-0040 «Обеспечение устойчивого экономического развития Российской Федерации средствами административно-правового регулирования», предусмотренной государственным заданием ИГП РАН, и является служебным произведением ИГП РАН.

<sup>2</sup> **Сморчкова Лариса Николаевна**, доктор юридических наук, доцент, ведущий научный сотрудник сектора административного права и административного процесса Института государства и права РАН, Москва, Российская Федерация.

E-mail: l.smorchkova@mail.ru



повышенной доступности информации о потенциальных контрагентах и предоставляемых ими товарах и услугах, а также инструментария для установления договорных отношений посредством цифрового сервиса, что в свою очередь в целом создает технологические условия для развития бизнеса. А посредством правового регулирования платформенной экономики на высшем федеральном уровне сделан существенный шаг по сокращению дистанции и пробелов в понимании связей и форм взаимодействия между правом и цифровой экономикой, что можно рассматривать как работающий междисциплинарный подход и один из примеров адекватной реакции на современные технологические и социогуманитарные вызовы [1].

В статье будут подробно рассмотрены цифровые логистические платформы, как один из активно развивающихся видов цифровых платформ, в соотношении с существующим административно-правовым регулированием в данной сфере — насколько широко осуществляется правовое воздействие на общественные отношения, возникающие в процессе функционирования логистических правовых платформ, с одной стороны, и насколько логистические правовые платформы могут выступать средством (инструментом) административно-правового регулирования в логистике, с другой.

### **Понятие и виды логистических цифровых платформ**

Цифровые платформы стали одним из наиболее действенных средств внедрения цифровых технологий в реальный бизнес, поскольку позволяют решить такие серьезные задачи, как обработка огромных массивов данных, за счет которых можно составлять портреты своих потребителей и тем самым прогнозировать их поведение и реакцию на различные продукты; формирование целых цифровых экосистем, дающих возможность компаниям более эффективно использовать и управлять этими данными, тем самым создавая конкурентное преимущество на рынке и открывая дополнительные направления для развития и роста [2, с. 26].

Цифровые платформы в настоящее время зарекомендовали себя в качестве устойчивого инструмента организации взаимодействия субъектов экономических отношений, благодаря своей принадлежности к цифровой инфраструктуре, то есть возможности использования цифровых технологий в условиях нового модельного цифрового технологического уклада; направленности на создание ценности для участников хозяйственных связей, поскольку при их взаимодействии на платформе происходит оптимизация стоимости товаров, работ или услуг за счет снижения транзакционных издержек и повышения эффективности сотрудничества; многосторонности возникающих отношений, которое подразумевает возможность параллельного вовлечения нескольких разностатусных

субъектов посредством ресурсов платформы (производителей, покупателей, посредников, перевозчиков, иных участников хозяйственных цепочек) [3, с. 10—11].

Цифровые платформы активно способствуют развитию такого важного сегмента экономики, как электронная торговля, создают благоприятную регуляторную среду на национальном, региональном и глобальном уровнях, что отвечает целям продвижения интересов России как одного из ключевых участников мировой высокотехнологичной торговли, для чего необходимы правовые инструменты и правовые конструкции, направленные на обеспечение ее участникам возможности совершать юридические действия в цифровой среде в предсказуемых, четких и стабильных правовых условиях [4, с. 103].

Цифровые платформы функционируют и активно используются в многих сферах деятельности, хотя правовое регулирование платформенной экономики было пока что осуществлено только применительно к отношениям, возникающим между операторами посреднических цифровых платформ, их партнерами, пользователями и иными лицами в связи с продажей товаров, выполнением работ, оказанием услуг. При этом посредническая цифровая платформа предоставляет технические возможности для размещения заказов и (или) карточек товаров, работ, услуг, совершения сделок, осуществления оплаты товара, работы, услуги пользователем в пользу партнера, но не является специализированной в определенной сфере хозяйственной деятельности.

По оценке ученых, законодатель впервые попытался урегулировать платформенные отношения, основываясь на смешении экономических разработок в области платформенной экономики и технического характера терминологии. Однако ему не удалось создать закон общего характера, нормы которого можно было бы распространить на все виды существующих цифровых платформ, а не только в отношении посреднических, соответствующих требованиям и критериям, установленным в Федеральном законе о платформенной экономике и входящих в реестр посреднических цифровых платформ, указанный Федеральный закон стал всего лишь частью пока еще несистемного регулирования платформенных отношений [5, с. 12; 6, с. 329; 7, с. 72].

В то же время представляется крайне актуальным осуществление целенаправленного правового регулирования платформенной экономики в такой сфере экономической деятельности, как логистика, поскольку она призвана способствовать наиболее эффективно управлению потоками товаров, услуг, информации и ресурсов от первичного поставщика к конечному потребителю, представляет собой длинные и многосложные цепочки хозяйственных связей, в том числе включающие в себя в качестве центрального звена такой особый сегмент, как оказание транспортных услуг.

Сегодня на российском логистическом рынке в качестве готового к использованию продукта представ-

лено некоторое количество<sup>4</sup> цифровых логистических платформ, каждая из которых обладает своими особенностями и предлагает свой набор сервисов. Участники логистических цепочек делают свой выбор в зависимости от своих потребностей и стоящих задач. Само явление цифровых логистических платформ стало предметом исследования преимущественно экономистами и техническими специалистами. Функционирование цифровых платформ безусловно затрагивает права и законные интересы неопределенного круга лиц, что свидетельствует о значимости правового регулирования связанных с их деятельностью общественных отношений. По сути, любые отношения, связанные с оказанием услуг в логистической сфере, в любой момент могут привести к нарушению прав субъектов хозяйственной деятельности. Начало правовому регулированию платформенной экономики уже положено, на следующем этапе необходимо выявить особенности цифровых логистических платформ и общественных отношений, возникающих при их посредничестве как потенциального предмета правового регулирования.

В научной литературе предлагается следующее определение цифровой логистической платформы, в котором достаточно удачно отражены ее основные характеристики и особенности — это «многопользовательский цифровой сервис, формирующий из набора функциональных модулей инфраструктуру для взаимовыгодного взаимодействия нескольких сторон пользователей (производителей, покупателей, перевозчиков, государства), совместно создающих ценность услуги, оптимизирующий взаимодействие участников посредством использования цифровых алгоритмов с целью повышения качества клиентского сервиса, сокращения транзакционных издержек и роста эффективности работы логистической системы» [3, с. 16]. На основе легитимно определенного в Федеральном законе понятия цифровой платформы и данного определения можно сформировать юридически полноценное понятие цифровой логистической платформы, добавив формальные характеристики и закрепив его в нормативной базе.

Возможности цифровизации позволили создавать различного типа цифровые логистические платформы, сервисы которых выполняют определенные задачи. Специалисты классифицируют их по различным основаниям, но не все классификации имеют равное значение для решения вопросов правового регулирования. Так, например, в зависимости от масштаба и уровня использования пользователями цифровой логистической платформы выделяют корпоративные, национальные и международные (межнациональные) цифровые логистические платформы, при том под

национальными понимаются платформы, создаваемые при поддержке государства и направленные на обеспечение развития национальной экономики за счет оптимизации взаимодействий между участниками хозяйственной деятельности, то есть точно являющиеся объектом правового воздействия [8, с. 27—31]. Корпоративные платформы бывают публичные и непубличные. Непубличные платформы предназначены для обслуживания внутренних потребностей компании и, возможно, ее ключевых партнеров, регулирование работы таких платформ вполне может носить локальный характер. Публичные платформы носят открытый характер и направлены на обслуживание неограниченного круга потребителей [9, с. 13—17], значимость правовой регламентации их функционирования имеет высокую степень.

### Состояние и перспективы правового регулирования в сфере функционирования логистических правовых платформ

Как было отмечено ранее, правовое регулирование платформенной экономики в России находится на начальной стадии. Цифровые логистические платформы в этой связи стоит рассматривать, прежде всего, как потенциальный предмет правового регулирования, требующий изучения особенностей общественных отношений, возникающих в процессе их функционирования, выявления интересов участников платформенных отношений, возможностей использования государством цифровых логистических платформ как средства правового регулирования и контроля в логистической сфере.

Многие проблемы, требующие правового решения, связаны с транснациональным характером самих цифровых платформ. Это обуславливает необходимость специального правового регулирования, учитывающего специфику экономической деятельности, осуществляемой посредством этого цифрового ресурса. Использование международных цифровых логистических платформ российскими предпринимателями может быть ограничено доступностью ресурса, а также совместимостью с национальными платформами и их требованиями [10].

Применительно к правовому регулированию отношений, возникающих посредством цифровых логистических платформ, в законодательстве необходимо, прежде всего, необходимо определить тип платформы и степень вмешательства в ее функционирование со стороны государства, а также закрепить их типовые (модельные) характеристики; определить перечень критериев, необходимых для отнесения того или иного цифрового сервиса именно к цифровой логистической платформе, в том числе содержательного (например, эффективность использования) и формального характера (официальная регистрация, вхождение в реестр и т. п.); показатели оценки эффективности цифровой логистической платформы и юридические последствия

<sup>4</sup> Порядка двух десятков активно использующихся платформ по оценке специалистов, однако в отсутствие реестра точное количество оценить невозможно, рынок динамичен: ТОП-16 лучших цифровых логистических платформ в 2026 году. URL: <https://korusconsulting.ru/blog/tekhnologii/top-16-luchshikh-tsifrovyykh-logisticheskikh-platform-v-2026-godu>

несоответствия содержательным и/или формальным критериям, закрепленным в законодательстве.

Есть ещё один непростой вопрос, на который необходимо ответить до того, как приступить к правовому регулированию платформенной экономики в логистической сфере — это его предмет и пределы. Связана эта проблема с очень широким покрытием логистических услуг, в целом охватывающих не только доставку, но и хранение и распределение продукции. В этом аспекте в российских источниках цифровые логистические платформы выделяются, прежде всего, как платформы транспортной логистики и обособляются от торговых цифровых платформ, которые тоже выполняют логистические функции. На сегодняшний день общедепартаментное правовое регулирование платформенной экономики на законодательном уровне идет по пути специализации применительно к отдельному виду платформ. В сфере логистики такой путь, видимо, также оправдан.

Принятое, но еще не апробированное правовое регулирование преимущественно в отношении посреднических правовых платформ следует рассматривать только как начало нового комплекса правовых норм, который в перспективе вполне может сформироваться в самостоятельный межотраслевой правовой институт. В целях защиты прав потребителей товаров (работ, услуг), а также прав и законных интересов самих участников платформенных отношений одновременно с диспозитивным правовым регулированием в указанной сфере был принят целый комплекс административно-правовых норм, обеспечивающих управленческое воздействие государства на функционирование посреднической правовых платформ.

Таким образом, посредством установления обязательных требований к участникам платформенных отношений, закрепления права государства осуществлять контрольно-надзорную деятельность в отношении цифровых платформ, введения обязательного информационного взаимодействия с государственными органами, цифровые платформы сами становятся административно-правовым инструментом воздействия на платформенные отношения и платформенную экономику. Создание национальной цифровой логистической платформы также стало средством правового воздействия на платформенные отношения в логистической сфере.

Так, с целью внедрения специальной информационной системы для оформления перевозок грузов, осуществляемых автомобильным, морским, речным, железнодорожным и воздушным видами транспорта с 1 августа 2024 года по 1 июня 2025 года для на территории Российской Федерации был проведен эксперимент по созданию, апробации и внедрению информационной системы «Национальная цифровая транспортно-логистическая платформа». Этот эксперимент стал частью федерального проекта «Цифровая трансформация транспортной отрасли» в рамках национального проекта «Транспорт».

В соответствии с Положением о проведении на территории Российской Федерации эксперимента по созданию, апробации и внедрению информационной системы «Национальная цифровая транспортно-логистическая платформа» для оформления перевозок грузов», утвержденного постановлением Правительства Российской Федерации от 3 июля 2024 г. № 908, в процессе эксперимента должен был быть определен и согласован с его участниками состав сведений о перевозке грузов, необходимых для включения в информационную систему эксперимента; апробирована технология выдачи разрешительных и товаросопроводительных документов посредством механизма «единое окно»; протестированы технологии сбора, верификации информации о перевозчиках и формирования их рейтинга; отработано информационное взаимодействие информационной системы эксперимента с иными информационными системами взаимодействия, а также разработаны предложения о внесении изменений в законодательство Российской Федерации, регламентирующее перевозку грузов в части перехода на электронный документооборот.

По результатам проведенного эксперимента была создана Национальная цифровая транспортно-логистическая платформа Российской Федерации (НЦТЛП) «ГосЛог». В соответствии со статьей 2.6 Федерального закона от 30 июня 2003 года № 87-ФЗ «О транспортно-экспедиционной деятельности»<sup>5</sup> платформа «ГосЛог» является федеральной государственной информационной системой, функционирующей на основе единых стандартов информационного взаимодействия для всех участников транспортно-логистической деятельности и органов государственного управления, программных, технических средств и информационных технологий, обеспечивающих автоматизированный сбор, обработку, хранение, предоставление, размещение и использование информации о транспортной системе Российской Федерации. Она призвана объединить цифровые логистические сервисы на одной платформе, в том числе в целях реализации принципа «одного окна» и внедрения электронного документооборота на всех этапах грузоперевозок автомобильным, морским, речным, железнодорожным и воздушным транспортом. Положение о платформе «ГосЛог» было утверждено постановлением Правительства Российской Федерации от 14 февраля 2026 года № 139.

Оператором платформы «Гослог» является Министерство транспорта Российской Федерации, его полномочия могут быть возложены на подведомственные

<sup>5</sup> Федеральный закон от 30 июня 2003 года № 87-ФЗ «О транспортно-экспедиционной деятельности» (Собрание законодательства Российской Федерации, № 27 (часть I) от 7 июля 2003 г., ст. 2701) дополнен статьей 2.6 в соответствии с Федеральным законом от 7 июня 2025 года № 140-ФЗ «О внесении изменений в Федеральный закон „О транспортно-экспедиционной деятельности“ и отдельные законодательные акты Российской Федерации», которая вступила в силу с 1 марта 2026 года (Собрание законодательства Российской Федерации, № 23 от 9 июня 2025 г., ст. 2999).

организации. Обладателем информации, размещенной на платформе «ГосЛог», является Российская Федерация, полномочия обладателя этой информации также осуществляет Минтранс России, но в то же время она является общедоступной (за исключением информации, доступ к которой ограничен федеральными законами) и размещается на официальном сайте Минтранса России в информационно-телекоммуникационной сети «Интернет».

Платформенные опции вводятся в действие постепенно. С 1 марта начал работу первый из обязательных реестров: реестр уведомлений о транспортно-экспедиционной деятельности. С 1 сентября 2026 года участники коммерческих грузоперевозок переходят на электронные перевозочные документы (ЭПД) — транспортные накладные, заказы-заявки, экспедиторские поручения и расписки. С 1 марта 2027 года на платформе «ГосЛог» начнет работу реестр для автоперевозчиков с транспортными средствами грузоподъемностью свыше 3,5 тонны, введенный в качестве обязательного Федеральным законом от 29 декабря 2025 года № 520-ФЗ «О допуске к осуществлению перевозок грузов автомобильным транспортом по территории Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации». В перспективе планируется интеграция платформы «ГосЛог» с цифровыми платформами стран БРИКС, ЕАЭС и ШОС для упрощения трансграничных перевозок<sup>6</sup>.

Полноценное функционирование платформы «ГосЛог» и связанная с этим объективная невозможность оказывать транспортные услуги в непрозрачных схемах должно привести к неизбежной легализации всей транспортной отрасли. Государство ожидает значительное сокращение избыточных издержек за счет документооборота по принципу «одного окна», а также ежегодные существенные дополнительные налоговые поступления в бюджет.

### Заключение

В структуре хозяйственных связей логистические взаимоотношения занимают существенное, если не главенствующее место. Цифровые логистические платформы стали современным инструментом организации такого рода взаимодействия субъектов экономической деятельности, что вызывает как потребность правового упорядочивания их создания и функционирования, так и возможность государства оказывать правовое воздействие и осуществлять правовой контроль в данной сфере, используя государственные цифровые логистические платформы в качестве административно-правового инструмента.

Посредством создания национальных цифровых платформ в определенной сфере экономики государ-

ство осуществляет административно-правовое упорядочивание отношений, не только связанных с функционированием данной платформы, но и, по сути, внутри всей хозяйственной отрасли. Ведение электронного документооборота, ведение реестров, прослеживаемость логистических цепочек, возможность осуществлять в отношении субъектов контрольно-надзорную деятельность, прозрачность услуг, их стоимости и качества придают национальной цифровой платформе характер инструмента административно-правового воздействия на ее участников, то есть такого рода платформа выполняет в том числе функцию правового регулятора.

Однако Национальная цифровая транспортно-логистическая платформа Российской Федерации «ГосЛог» является только лишь одним из административно-правовых инструментов, не подменяет и не исключает полноценного правового регулирования общественных отношений в сфере логистики, связанных с функционированием различного рода цифровых логистических платформ, будь то платформа комплексного характера, или специального — только в транспортной сфере, являющейся центральным звеном логистической системы.

<sup>6</sup> Государство берет логистику под контроль: запуск ГосЛогa. URL: <https://companies.rbc.ru/news/IznzpDv4wg/gosudarstvo-beret-logistiku-pod-kontrol-zapusk-gosloga>



## Литература

1. Савенков А.Н. Новый технологический уклад и социогуманитарные вызовы // Государство и право. 2025. № 1. С. 14—36.
2. Бабкин А.В., Михайлов П.А. Цифровые платформы в экономике: понятие, сущность, классификация // Вестник Академии знаний. 2023. № 54. С. 25—36.
3. Егерев Ю.Б., Бахарев В.В. Цифровые логистические платформы как инновационный формат предоставления логистических услуг: критический анализ // Модели, системы, сети в экономике, технике, природе и обществе. 2023. № 2. С. 5—24.
4. Соловяненко Н.И. Правовые инструменты поддержки цифровых торговых процедур и взаимного признания государствами электронных документов в сфере трансграничной торговли // Проблемы экономики и юридической практики. 2025. Т. 21. № 3. С. 98—104.
5. Габов А.В., Саяпин С.П. Платформенные отношения как предмет правового регулирования. // Lex russica. 2025. Т. 78. № 11. С. 9—33.
6. Буланова В.С. Правовое регулирование платформенной экономики // Образование и право. 2026. № 2. С. 327—330.
7. Васиян Р.И. Некоторые аспекты правового регулирования платформенной экономики в Российской Федерации // Российское право: образование, практика, наука. 2025. № 4. С. 67—75.
8. Корчагина Е.В., Еремин К.А., Видинеева Е.В. Цифровые логистические платформы: анализ зарубежного опыта // Журнал правовых и экономических исследований. 2021. № 4. С. 27—31.
9. Корчагина Е.В. Цифровые логистические платформы: подходы к классификации // Журнал правовых и экономических исследований. 2022. № 2. С. 13—17.
10. Барыкин С.Е., Егерев Ю.Б., Корчагина Е.В. [и др.]. Крупнейшие международные цифровые логистические платформы: сравнительный анализ // Омский научный вестник. Сер.: Общество. История. Современность. 2022. Т. 7. № 1. С. 97—103.

SECTION:  
REGULATORY INFORMATICS

# DIGITAL LOGISTICS PLATFORMS AND ADMINISTRATIVE AND LEGAL REGULATION

Smorchkova L.N.<sup>7</sup>

**Keywords:** digital platforms, business relations, logistics, administrative and legal regulation, government influence, National Digital Transport and Logistics Platform.

## Abstract

**Objective:** to analyze digital logistics platforms as a means of organizing business relations in this area of economic relations, as a potential subject of legal regulation, and as a tool for administrative and legal regulation and control in logistics.

**Methods:** systemic and expert analysis, comparative legal methods, and formal legal methods.

**Results:** the relevance of legal regulation of relations arising during the organization, operation, and mediation of digital logistics platforms, their characteristics, and the importance of government legal participation for both streamlining the logistics sector and exercising legal control over the activities of participants in logistics relations are revealed.

**Practical value:** the results of the study can be taken into account in the creation and subsequent improvement of legal regulation of the creation and operation of digital logistics platforms both at the highest federal level and in subordinate legislation.

---

<sup>7</sup> **Larisa N. Smorchkova**, Dr.Sc. (Law), Associate Professor, Leading Researcher at the Sector of Administrative Law and Administrative Procedure of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.  
E-mail: [l.smorchkova@mail.ru](mailto:l.smorchkova@mail.ru)

## References

1. Savenkov A.N. Novyi tekhnologicheskii uklad i sotsiogumanitarnye vyzovy // Gosudarstvo i pravo. 2025. No. 1. S. 14—36.
2. Babkin A.V., Mikhailov P.A. Tsifrovye platformy v ekonomike: poniatie, sushchnost', klassifikatsiia // Vestnik Akademii znaniy. 2023. No. 54. S. 25—36.
3. Egereva Iu.B., Bakharev V.V. Tsifrovye logisticheskie platformy kak innovatsionnyi format predostavleniia logisticheskikh uslug: kriticheskii analiz // Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve. 2023. No. 2. S. 5—24.
4. Solovianenko N.I. Pravovye instrumenty podderzhki tsifrovyykh torgovykh protsedur i vzaimnogo priznaniia gosudarstvami elektronnykh dokumentov v sfere transgranichnoi togovli // Problemy ekonomiki i iuridicheskoi praktiki. 2025. T. 21. No. 3. S. 98—104.
5. Gabov A.V., Saiapin S.P. Platformennye otnosheniia kak predmet pravovogo regulirovaniia. // Lex russica. 2025. T. 78. No. 11. C. 9—33.
6. Bulanova V.S. Pravovoe regulirovanie platformennoi ekonomiki // Obrazovanie i pravo. 2026. No. 2. S. 327—330.
7. Vasiian R.I. Nekotorye aspekty pravovogo regulirovaniia platformennoi ekonomiki v Rossiiskoi Federatsii // Rossiiskoe pravo: obrazovanie, praktika, nauka. 2025. No. 4. S. 67—75.
8. Korchagina E.V., Eremin K.A., Vidineeva E.V. Tsifrovye logisticheskie platformy: analiz zarubezhnogo opyta // Zhurnal pravovykh i ekonomicheskikh issledovaniy. 2021. No. 4. S. 27—31.
9. Korchagina E.V. Tsifrovye logisticheskie platformy: podkhody k klassifikatsii // Zhurnal pravovykh i ekonomicheskikh issledovaniy. 2022. No. 2. S. 13—17.
10. Barykin S.E., Egereva Iu.B., Korchagina E.V. [i dr.]. Krupneishie mezhdunarodnye tsifrovye logisticheskie platformy: sravnitel'nyi analiz // Omskii nauchnyi vestnik. Ser.: Obshchestvo. Istoriia. Sovremennost'. 2022. T. 7. No. 1. S. 97—103.



# ЦИФРОВЫЕ ФИНАНСОВЫЕ АКТИВЫ: РЕГУЛИРОВАНИЕ УЗЛОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Метельков А.Н.<sup>1</sup>

**Ключевые слова:** узел, информационная система, цифровые права, блокчейн, пользователь, нода, валидатор, виртуальная машина, криптовалюта.

## Аннотация

**Цель:** проанализировать регулирование узлов информационной системы в правовых режимах оборота цифровых финансовых активов и защиты информации как взаимодействующих систем юридических средств. Выявить дефекты юридической техники в конструировании отдельных правовых терминов, имеющих техническое содержание, в условиях повышения технологичности и количества компьютерных атак. Сфокусировать основное внимание на рассмотрении соотношения места информационной технологии и человека, использующего ее в альтернативных платёжных системах, и правового регулирования социальных отношений касательно их внедрения на примере совокупности правовых средств, используемых для регулирования цифровых прав и защиты корреспондирующих с ними данных.

**Метод:** с использованием междисциплинарного и сравнительно-правового подходов сопоставляется содержание понятия «узел информационной системы» в федеральных законах. Проведён сравнительный анализ состава элементов понятия «информационной системы» в законодательстве об информации и о цифровых финансовых активах.

**Результат:** обосновано положение об узле информационной системы как объекте, а не субъекте правовых отношений в сфере обращения цифровых финансовых активов. В результате анализа выявлена необходимость согласованного использования дефиниций в части определения элементного состава технической системы и позиционирования по отношению к ней пользователя. Сформулировано предложение по совершенствованию законодательства о цифровых финансовых активах посредством технологии блокчейн в отношении понимания термина «узел информационной системы» в части его «опредмечивания». Установлено, что различные подходы к определению содержания понятия «узел» в российском законодательстве о цифровых финансовых активах создают трудности в обеспечении информационной безопасности. Выработано предложение законодателю отказаться от применения правовой конструкции «пользователь информационной системы как ее узел», заменив ее на схему доступа пользователя к узлу такой системы.

DOI: 10.24412/1994-1404-2026-3-199-207

## Введение и постановка задачи

**И**ntenсивное развитие цифровых технологий опережает правовое регулирование соответствующих общественных отношений. Объективно складывающиеся в информационной сфере и нуждающиеся в таком регулировании социальные отношения сопровождаются коллизиями в терминологическом аппарате, что негативно сказывается на понимании текстов отдельных нормативных правовых актов и реализации на практике мер и мероприятий по обеспечению информационной безопасности (ИБ) и защите информации.

Применение специальной технологии представляет собой характерный признак «цифровых прав и активов, отделяющих их от других объектов гражданского оборота» [1, с. 239]. При проектировании платформ для выпуска и оборота цифровых финансовых активов (ЦФА) субъекты российского цифрового финансового рынка вынуждены решать задачу обеспечения технологического суверенитета в условиях актуальных геополитических вызовов и санкционных ограничений. В частности, требуется оценка некоторых комплаенс-рисков и рисков ИБ, сопряжённых с применением

<sup>1</sup> **Метельков Александр Николаевич**, кандидат юридических наук, доцент, доцент кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России, г. Санкт-Петербург, Российская Федерация.

E-mail: metelkov5178@mail.ru

открытого исходного кода (open-source) модульных архитектур при разработке корпоративных решений на базе распределённых реестров.

Проблема взаимообусловленности совершенствования правовых регуляторов, технических средств и технологий в финансовом праве по-прежнему дискуссионна и не обрела недвусмысленного теоретического разрешения в эпоху цифровизации. Практика показывает, что отсутствие в правовых актах закрепления «чёткой позиции законодателя по цифровому взаимодействию субъектов, его непоследовательность в трактовке статуса «цифровых» субъектов и «цифровых» объектов вносят путаницу и хаос не только в доктринальные позиции цивилистов, но и в судебную практику» [2, с. 45—46]. В киберпространство входят субъекты, то есть администраторы, операторы систем, иные пользователи и их виртуальные отображения (учётные записи, маркеры доступа и т. д.), а также объекты, в основном представляющие собой ресурсы и информационные активы: компоненты среды передачи данных; обработки и хранения информации; управляющих, технологических и исполнительных систем; систем защиты информации [3, с. 85]. Анализ правил операторов информационных систем (ИС), в которых обрабатываются ЦФА, показывает, что определение понятия «узел» (а не «узел ИС», как установлено законодателем) в них изложено противоречиво в качестве объекта, субъекта или их интегрированной сущности. Например, в Правилах ИС ООО «Блокчейн Хаб» (версия 1, 2023) узел распределённого реестра (узел) сначала был определён как комплекс аппаратно-программных средств, обеспечивающий поддержание полного экземпляра данных распределённого реестра в целях обеспечения тождественности информации, содержащейся в ИС, с помощью процедур подтверждения действительности вносимых в неё (изменяемых в ней) записей (п. 1.2.28). Владелец узла распределённого реестра (владелец узла) считался пользователь ИС, владеющий узлом при условии заключения соответствующего договора с оператором ИС (п. 1.2.5). Однако в версии 2 (2024 г.) «узел» определён уже как пользователь, обеспечивающий тождественность информации, содержащейся в Распределённом реестре. В правилах ИС ПАО Сбербанк, понятие «узел» определено как «пользователь, обеспечивающий тождественность информации, содержащейся в Системе, с применением процедур подтверждения действительности, вносимых в неё (изменяемых в ней) записей» (п. 2.1.54), а понятие «нода» как «программно-аппаратный комплекс, обеспечивающий исполнение функций Узла» (п. 2.1.32). В этом примере Сбербанк попытался, на наш взгляд, совместить традиционное техническое понимание узла, как объекта, с пониманием узла законодателем, который установил его в качестве субъекта. Поэтому технический узел системы получил название «нода», чтобы отделить его от субъекта-пользователя. В правилах ИС оператор ИС, в которой осуществляется выпуск ЦФА (ООО «Лайтхаус», ООО «Атомайз»), уходит от примене-

ния термина «узел информационной системы», подменяя его термином «узел валидатора». Узлом валидатора согласно правилам ИС ООО «Лайтхаус», в которой осуществляется выпуск ЦФА (2023, п. 1.42) определён как виртуальная машина, выполняющая функции одобрения транзакций, упорядочивания и (или) записи блоков транзакций в Систему в рамках общего процесса подтверждения Транзакций. Аналогично в правилах ИС ООО «Атомайз» (утв. решением совета директоров ООО «Атомайз», протокол № 60 от 14 мая 2026 г.) узлом валидации названа также «виртуальная машина...».

В то время как законодателем сделана попытка «одушевить» понятие узла, сделать субъектом правоотношений по поводу обращения ЦФА, специалисты в области информационных технологий в основном определились с понятием «узел» ИС. Узлы распределённой компьютерной сети ими рассматриваются с технической точки зрения в виде аппаратно-программного комплекса технических средств, так как в отличие от пользователя ИС узлы сети подключаются и синхронизируются с сетью [4, с. 304], располагают дисковым пространством для хранения информации о цепочке транзакций. В правовом аспекте одноранговые P2P-сети (от англ. peer-to-peer — «равный к равному») могут быть охарактеризованы как децентрализованные информационно-коммуникационные системы, в рамках которых субъекты правоотношений осуществляют непосредственное взаимодействие в отсутствие координирующего субъекта-оператора. Обычно узел таких сетей состоит из нескольких компонентов: модуля IDS, компонента взаимодействия и компонента P2P-связи<sup>2</sup>. Структурно узел включает следующие элементы, имеющие правовое значение: модуль IDS (системы обнаружения вторжений) — техническое средство реализации средства обеспечения ИБ; компонент взаимодействия — механизм координации действий субъектов в рамках распределённой сети; компонент P2P-связи — инфраструктурный элемент, обеспечивающий установление прямого (без посредничества центрального узла) коммуникационного соединения между субъектами сети. Система обнаружения вторжений выполняет функции мониторинга сетевого трафика и фиксации юридически значимых событий (в т.ч. потенциальных актов неправомерного доступа), обеспечивая тем самым режим защиты информации и протоколирование фактов, способных иметь доказательственное значение. Компонент взаимодействия обеспечивает обмен данными, необходимыми для реализации правомочий участников, и поддерживает процедуры, имеющие правовую релевантность (в частности, расчёт показателя доверия как элемента формирования режима добросовестности и оценки правосубъектности контрагента). С юридической точки зрения это соответствует модели равноправных договорных

<sup>2</sup> Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When Intrusion Detection Meets Blockchain Technology: A Review. IEEE Access, 6, p. 10181.



связей, где отсутствует субординация и каждый участник самостоятельно реализует свои полномочия в рамках децентрализованного правопорядка. Следовательно, P2P-сеть предстаёт как пространство горизонтальных правоотношений, где участники выступают автономными субъектами, а технические компоненты сети, включая узлы такой распределенной системы, выполняют функции обеспечения безопасности, координации и коммуникации, то есть реализуют в условиях отсутствия централизованного регулятора ключевые правовые инструменты, обеспечивающие защиту прав участников цифрового оборота, доверие, договорные отношения.

ИС нами рассматривается как объект, объединяющий различные программно-аппаратные средства в системах распределённого реестра, а её взаимодействие с субъектом-пользователем или оператором осуществляется через программно-аппаратный интерфейс. При этом разграничение между категориями субъекта и объекта правоотношений в сфере ЦФА применительно к ИС, узлу ИС. С позиций теории правоотношений субъект является носителем правосубъектности (правоспособности, дееспособности, деликтоспособности), способный своими волевыми действиями порождать, изменять и прекращать юридические последствия. Объект — то, по поводу чего складываются правоотношения и на что направлены субъективные права и юридические обязанности.

Акцент на доступе пользователя к узлу ИС, а не на отождествлении пользователя с узлом ИС, имеет принципиальное значение для правового моделирования режимов доступа, аутентификации, разграничения полномочий и юридической фиксации оснований и пределов такого доступа. В доктрине информационного права это соотносится с категориями «права доступа», «полномочия», «границы правомерного использования» и «юридически значимые действия в электронной среде».

Проблема множественности подходов к определению понятия ИС в российском законодательстве рассматривается в контексте юридической определённости и качества правового регулирования. С позиций теории права неопределённость дефиниций в правовых режимах ЦФА и защиты информации порождает коллизии квалификации, затрудняет правоприменение и снижает эффективность гарантий прав участников оборота ЦФА. В частности, расхождения в понимании содержания категории «информационная система» между нормами финансового и информационного законодательства осложняют выстраивание единого правового режима обеспечения информационной безопасности, поскольку без унифицированной дефиниции невозможно однозначно определить объект защиты, границы правового воздействия и распределение обязанностей по обеспечению безопасности.

### **Узел информационной системы: субъект права или объект?**

Совокупность электронных данных (цифрового кода или обозначения), содержащихся в ИС, законодателем признается цифровой валютой. В связи с этим для точного понимания содержания цифровой валюты важно уяснение компонентов ИС, единого подхода к которому в теории ещё не выработано. В научной литературе доминирует два направления. Сторонники одного включают в состав ИС человека, другие [5, с. 117], наоборот, исключают его из структуры. Появление цифрового рубля и криптовалют, ставших предметом общественных отношений в сфере денежного обращения и расчётов, привело к обособлению в правовом режиме денежного обращения совокупности правовых норм, которые фактически создают «правовой режим цифровых валют» [6, с. 433]. Такие подходы оказывают влияние на практическую реализацию взаимодействия правовых режимов ИБ и денежного обращения.

В основание большинства альтернативных платёжных систем положена технология блокчейн, которая предполагает последовательное формирование, передачу и использование зашифрованной методом криптографии и «упакованной» в блоки информации на основе применения свободного программного обеспечения<sup>3</sup>. Технология блокчейн, которая лежит в основе создания ЦФА и криптовалюты, теоретически представляет собой одноранговую сеть с распределённой базой данных (реестром), информация в которой реплицируется на территориально распределённые программно-аппаратные комплексы, что обеспечивает целостность и сохранность информации. На каждом компьютере сети хранится полная версия цепочки блоков, обновляемая при добавлении очередного блока сразу на всех компьютерах сети. Блокчейн представляют в виде «технологии реестров, при которой существует уникальный код, характеризующий существование документа» [7, с. 96]. В российском сегменте рынка ЦФА по состоянию на 11 августа 2026 г. работают 24 операторов ИС. Среди используемых различных блокчейн-решений получили распространение отечественные платформы «Мастерчейн» (и её обновлённая версия МЧ 2.0) и Waves Enterprise, что свидетельствует о стремлении к импортозамещению и поддержке российских технологических решений в финансовой сфере.

Алгоритмы в ИС, «вступающие во взаимодействие с правом, являются социотехническими нормативно-казуальными регуляторами» [8, с. 10]. Технология блокчейн делает невозможным скрытно изменить зафиксированные в ней данные, а территориальная «распределённость предполагает множество мест хранения данных блокчейна, так что поражение одного узла не повлечёт за собой утрату информации» [9, с. 90]. В статье

<sup>3</sup> Кучеров И.И. Криптовалюта (идеи правовой идентификации и легитимации альтернативных платёжных средств) : монография. М. : Центр ЮрИнфоР, 2018. С. 96.

под узлом информационной системы нами понимается объект — техническое устройство, обеспечивающее передачу данных в сети, доступ к ним пользователей, и участвующее в обработке данных.

Технология блокчейн характеризуется безопасностью и защищенностью, устойчивостью, неизменностью записанных данных, открытостью и прозрачностью, децентрализацией и распределённостью. Алгоритмы блокчейн направлены на формирование последовательных цепочек транзакций. Они не позволяют вносить изменения после совершения транзакций. Это обстоятельство запрещает вносить коррективы в информацию, которая уже была обработана системой. За добавление и проверку новых блоков отвечают майнеры, над которыми отсутствует централизованное управление. Ошибки в коде смарт-контрактов, то есть их уязвимости, способны спровоцировать ряд критических проблем. Среди них — атаки повторного входа (reentrancy), целочисленное переполнение, которое искажает результаты вычислений, а также логические недочёты и сбои в механизме контроля доступа. Кроме того, риски связаны с опорой на временные метки либо псевдослучайные числа. Ещё одна угроза — front-running. Злоумышленник может опередить выгодные транзакции в мемпуле (mempool) — очереди, разместив там свою операцию раньше. Угрозой на уровне консенсуса являются атаки на механизмы, обеспечивающие согласие узлов о состоянии реестра. В сетях с Proof-of-Work (PoW) злоумышленник, контролирующий более 50% вычислительной мощности, может создавать свою цепочку блоков, обгоняя основную. Это позволяет отменять подтверждённые транзакции, проводить двойные траты или блокировать транзакции других участников. В Proof-of-Stake (PoS) для такой атаки нужно контролировать более 50% всех активов в стейкинге, что сложнее, но возможны и другие схемы: long-range-атаки (переписывание истории с нуля), атаки через уязвимости в выборе валидаторов.

Технологии обращения криптовалют обеспечивают пользователям альтернативных платёжных систем условия анонимности и бесконтрольности со стороны государства. В доктрине информационного права субъект информационного потребления (пользователь информации) определяется как правосубъектное лицо (физическое либо юридическое) [10, с. 104], реализующее правомочие на доступ к информации и её последующее использование в целях удовлетворения собственных законных интересов либо фактически осуществляющее такие действия. При этом в нормативной конструкции Федерального закона «Об информации, информационных технологиях и о защите информации» дефиниция понятия «пользователь информации» прямо не закреплена, вследствие чего в теоретико-правовой модели оно выступает родовым (обобщающим) по отношению к видовым категориям — таким, как пользователь информационно-телекоммуникационной сети (в т. ч. сети Интернет), пользователь информационного ресурса,

пользователь поисковой системы и иным аналогичным субъектам информационного обмена.

ЦФА и криптовалюты часто путают, вероятно, потому, что они часто работают на базе блокчейна. ЦФА представляют собой электронные документы, удостоверяющие наличие у их владельца определённых имущественных прав, закреплённых в соответствии с законодательством. Например, право получить определённую сумму (денежное требование), право на дивиденды или долю в капитале непубличной компании, право требовать передачи акций или облигаций. Криптовалюта же сама по себе не даёт никаких имущественных прав — это просто цифровой код, который в законе определяют как совокупность электронных данных. Криптовалюту чаще рассматривают как средство для расчётов или инвестиций, а не как право на какой-то актив. Эмитентом ЦФА является юридическое лицо или индивидуальный предприниматель, который выпустил токен и несёт перед инвесторами обязательства. В большинстве случаев криптовалюты не имеют центрального эмитента. Они создаются децентрализованно (например, через майнинг), и никто лично перед держателями не отвечает, за исключением стейблкоинов, которые привязаны к реальным активам или валютам.

В России выпуск и обращение ЦФА регулируются законом, а сами активы обращаются только на платформах, которые Банк России включил в специальный реестр операторов ИС. С криптовалютами, которые изначально задумывались как децентрализованные системы платежей и расчётов, ситуация иная. В российском правовом поле для них пока формируется отдельный режим. Криптовалюты и ЦФА не разрешены в качестве средства платежа за товары и услуги внутри страны. ЦФА создают для токенизации реальных активов или финансовых инструментов. ЦФА — это не деньги, а цифровая запись о праве, например, на денежное требование, ценную бумагу, долю в капитале или на что-то подобное, а криптовалюта — это сам цифровой «код-средство», за которым нет личного обязательства какого-то одного лица. Электронные деньги, как считает В.П. Перепеченко, представляют собой «технический способ регистрации безналичных денег, сохранения соответствующей информации»<sup>4</sup>. Существующие модели правового регулирования обращения финансовых активов «не обеспечивают полноценной адаптации электронных денежных средств в правовой материи» [6, с. 429—430]. В случае включения в систему в качестве её элемента человека-пользователя возникает проблема расширения комплекса требуемых правовых, организационных и технических мер, направленных не только на защиту информации, но и на обеспечение ИБ. Ключевой становится проблема управления доступом к цифровым данным, особен-

<sup>4</sup> Перепеченко В.П. Деньги, банки, кредит : учеб. пособие. М. : ЗАО «Издательство Экономика», 2008. С. 18.

ность которых состоит в множественности «субъектов, имеющих фактический доступ» [11, с. 147].

С внесением (изменением) записи в ИС на основе распределённого реестра и другие ИС законодатель связывает выпуск, учёт и обращение цифровых прав, называемых ЦФА. Особенность ЦФА заключается в их обращении в любых ИС, «а не в какой-то определённой» [12, с. 47]. Поэтому актуальным становится рассмотрение некоторых коллизий в российском законодательстве, регулирующем оборот ЦФА, связанных с понятием ИС и её структурными элементами. Как известно, при подготовке законопроектов необходимо обращать «внимание на согласованность текста и его частей, и не только внутри самого текста, но и в связи с действующим законодательством<sup>5</sup>. Коллизии в отдельных понятиях вносят инфраструктурный деструктив во взаимодействие правовых режимов в сферах защиты информации и оборота ЦФА, представляющих один из видов преобразованной с опорой на методы криптографического преобразования информации о транзакциях — записях о переводах ЦФА между пользователями.

В законодательстве о ЦФА<sup>6</sup> (далее — Закон о ЦФА) установлено (ст. 5), что понятия «ИС» и «оператор ИС» используются в значениях, определённых Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации). В ст. 2 Закона об информации определены эти понятия и дана дефиниция информационных технологий. Структурными элементами ИС законодатель определил информацию в базах данных, информационные технологии и технические средства.

Состав ИС, согласно Закону об информации, можно формализовать путём представления абстрактной информационной системы ( $IS_{\Phi 3-149}$ ) в виде множества из трёх элементов: I — информации, ТМ — технических средств и ИТ-информационных технологий:

$$IS_{149-\Phi 3} = \{I, TM, IT\} \quad (1).$$

Состав ИС, согласно Закону о ЦФА, также формализуем с помощью указанных элементов с добавлением «узла ИС» — N (node) путём представления в виде множества из четырёх элементов: N узлов, I, ТМ и ИТ:

$$IS_{259-\Phi 3} = \{N, I, TM, IT\} \quad (2).$$

С целью выявления наличия социального элемента или его абстрактного отражения (например, юридиче-

ского лица) в составе ИС проведём структурный анализ её составляющих. Очевидно, при анализе можно сразу же исключить из наших рассуждений информацию и технические средства, так как в «чистом» виде индивид непосредственно в них не присутствует. Вопрос с содержанием информационных технологий требует детального рассмотрения. В соответствии с Законом об информации (ст. 2) информационные технологии охватывают широкие по смыслу «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов». Существуют различные взгляды на наличие в таких технологиях антропологического элемента. Анализ легального понятия «оператор ИС» все расставляет на свои места. Им может быть только гражданин или юридическое лицо, эксплуатирующие ИС и обрабатывающие информацию в её базах данных, то есть оператор ИС не включён в состав ИС. В Законе о ЦФА, однако, законодателем введено понятие узла ИС, под которым понимаются пользователи ИС на основе распределённого реестра. В ст. 2 Федерального закона от 4 августа 2026 г. № 282 «О цифровых валютах и цифровых правах» также определение узлов ИС идентично их дефиниции в Законе о ЦФА. Кроме того, узлы ИС включены и в определение распределённого реестра. В таком случае возникает противоречие и смешение в законодательстве содержания разных по содержанию понятий, названных одним и тем же термином — узел ИС. В нормативном правовом акте Генеральной прокуратуры России<sup>7</sup>, в подзаконных методических материалах ФСТЭК России<sup>8</sup>, в Соглашении об информационном обмене между Федеральной налоговой службой, Федеральной нотариальной палатой и Фондом «Центр инноваций и информационных технологий»<sup>9</sup>, узел вычислительных и информационных ресурсов, включая информационные системы рассматривается как модуль или как технический элемент.

Оператор и пользователь — это субъекты, а IS, IT, ТМ — объекты. Однако законодатель в объект  $IS_{259-\Phi 3}$  включает только субъекта — пользователя ИС, а оператора в её состав не включает.

<sup>7</sup> Приказ Генпрокуратуры России от 11 сентября 2025 № 621 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2030 года, а также о внесении изменений в отдельные организационно-распорядительные документы Генерального прокурора Российской Федерации» // СПС «КонсультантПлюс».

<sup>8</sup> Методический документ «Профиль защиты систем обнаружения вторжений уровня узла шестого класса защиты» (ИТ.СОВ. У6.П3), утвержден ФСТЭК России 6 марта 2012 г. URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-6-marta-2012-g> (дата обращения: 12.08.2026).

<sup>9</sup> Соглашение об информационном обмене между Федеральной налоговой службой, Федеральной нотариальной палатой и Фондом «Центр инноваций и информационных технологий», утв. ФНС России № ЕД-22-26/73@, ФПН, Фондом «Центр инноваций и информационных технологий» 27 декабря 2024 // СПС «КонсультантПлюс».

<sup>5</sup> Юридическая техника : учебное пособие по подготовке законопроектов и иных нормативных правовых актов органами исполнительной власти / ИЗИСП при Правительстве РФ; [Т.Я. Хабриева и др.], под ред. Т.Я. Хабриевой, Н.А. Власенко. М. : Эксмо, 2010. С. 62.

<sup>6</sup> См.: Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 2020. № 31. Ч.1. Ст. 5018.

Сравнение (1) и (2) подтверждает нетождественность понятий информационной системы в Законе о ЦФА и Законе об информации:

$$\{I, TM, IT\} \neq \{N, I, TM, IT\}.$$

Как правило, в правилах ИС выделены следующие категории пользователей: эмитент, инвестор, номинальный держатель, узел, оператор обмена [13, с. 91] и другие.

В Законе о ЦФА используются два понятия, связанные с термином «узел»: «лица, выполняющие функции узлов» ИС и пользователи — «узлы ИС». Их нельзя признать тождественными. Смысл такого раздвоения не ясен применительно к ИС и технологии блокчейн. Введение этих терминов вступает в противоречие со сложившимся пониманием узлов ИС, как чисто технических элементов ИС. В системе «человек — машина» человек взаимодействует с ИС через интерфейс, поэтому включать человека-пользователя системы в качестве её узла с методологической точки зрения, на наш взгляд, нецелесообразно. Пользователь — это лицо, имеющее легальный доступ к узлу ИС, а не сам узел технической системы. Права на ЦФА возникают с момента внесения оператором ИС записи о зачислении активов на счёт конкретного человека. При наличии уникального кода (ключа), открывающего доступ к системе, субъект-пользователь может видеть свои активы и распоряжаться ими. На практике в правилах ИС операторы вынуждены строить конструировании определений терминов, в которых узел (техническое устройство) отделен от человека-пользователя ИС. В правилах информационной системы ООО «Спутник ЦФА» (2026 г.) понятия «узел» (программно-аппаратный комплекс, обеспечивающий выполнение функций валидатора в соответствии с правилами) и «валидатор» (субъект-пользователь, обеспечивающий тождественность информации, содержащейся в Системе, с использованием процедур подтверждения действительности, вносимых в неё (изменяемых в ней) записей) вполне обоснованно разделены, чтобы гармонизировать обычное техническое понимание узла с недостаточно корректным его определением законодателем.

В результате анализа различных подходов к наполнению содержательными элементами понятия ИС и логических рассуждений можно сделать вывод о противоречивости отражения в российском законодательстве структуры рассматриваемого правового понятия в части включения в его состав субъекта права. Такой подход законодателя размывает объективные процессы в социотехнической системе, обрабатывающей ЦФА с помощью компьютерной техники и средств телекоммуникаций, с участием субъекта.

Двусмысленное социально-техническое понимание узлов в сети можно встретить в работах учёных-юристов. Авторы с одной стороны считают, что сетевые узлы «создаются путём свободного присоединения новых членов к существующей группе» [14, с. 149], а с другой утверждают, что для участника сети необхо-

димо «подключение своего узла (компьютера) через индивидуальный адрес к Интернету и источнику питания» [14, с. 149]. В одном случае узел можно рассматривать как логический элемент или даже в качестве социального субъекта, в другом как физический элемент — устройство ИС.

Техническое содержание узла ИС обосновано в статье «Парадокс узлов: защита информации и право цифровой валюты» [15, с. 4—12]. В работе С.С. Еськова [16, с. 3] представлены автоматные модели процессов функционирования узла системы с распределённым реестром на основе цепочки блоков, отличающаяся представлением узла конечным автоматом. Келдыш Н.В.<sup>10</sup> полагает, что основным свойством, отличающим компьютерные сети от автономных компьютеров, является наличие обмена информацией между сетевыми узлами, связанными линиями передачи данных. В таком понимании достаточно сложно представить человека в виде сетевого узла, поэтому введение термина «узел ИС» в законодательство и цифровых финансовых активах нам представляется недостаточно аргументированным.

В теории информации узел представляет собой базовый элемент информационной структуры, выступающий в качестве носителя данных (data unit). Узлы формируют информационные графы — связанные структуры, в которых: каждый узел содержит определённый объём информации (I); связи между узлами реализуются посредством указателей (pointers), кодирующих адреса памяти, то есть формализованные ссылки на физическое или логическое расположение данных в вычислительном пространстве. В контексте сетевых технологий узел интерпретируется как сетевой субъект (network entity) — устройство, обладающее следующими компонентами: уникальным идентификатором (например, IP-адресом), выполняющим функцию аутентифицирующего токена; способностью к информационному обмену — отправке и приёму данных в рамках протокола взаимодействия. В сетевом аспекте узел обозначает устройство в сети, которое может отправлять и получать информацию. С позиции ИБ ключевые аспекты охватывают следующие свойства: целостность данных в узлах обеспечивается механизмами контроля изменений и верификации ссылок; конфиденциальность реализуется через ограничение доступа к указателям и шифрование передаваемой информации; доступность поддерживается резервированием связей и обеспечением устойчивости графовой структуры к отказам отдельных узлов. Таким образом, понятие «узел» объединяет три аспекта: структурно-информационный (хранение и организация данных), коммуникационный (сетевое взаимодействие), аспект ИБ (защита целостности, конфиденциальности и доступности информации).

А.С. Короткина, опираясь на мнения ученых-юристов, вполне обоснованно рассматривает ИС

<sup>10</sup> Келдыш Н.В. Системная защита информации компьютерных сетей : учебное пособие. М. : Мир науки, 2022. С. 5.



как «сложный объект» [17, с. 45]. В рамках исследования такой узел нами классифицируется в качестве объекта права, а не субъекта, поскольку собственно узел лишён воли и правосубъектности и выступает как элемент ИС или информационно-телекоммуникационной сети — технической инфраструктуры, обеспечивающей оборот цифровых финансовых активов и доступ пользователя к аппаратно-программным (техническим) средствам ИС.

В академической и нормативной среде стремятся к полноте. Важно подчеркнуть значение не только «железа» (узлов, каналов), но и общих правил (протоколов) взаимодействия устройств. Поэтому формализовано можно записать следующее соотношение: компьютерная сеть = совокупность узлов + инфраструктура + стандартизированные протоколы. Компьютерную сеть с учётом анализа положений ГОСТ Р ИСО / МЭК 27033-1-2011<sup>11</sup> можно определить как совокупность взаимосвязанных узлов, комплексную инфраструктуру, объединяющую совокупность технических средств, коммуникационных каналов и стандартизированных протоколов, обеспечивающих взаимодействие подключённых устройств и передачу данных. В этом стандарте фокус сделан на безопасности сетей, но базовое понимание инфраструктуры (узлы, каналы, правила взаимодействия) раскрывается именно в таком ключе. В аспекте таких сетей узел (node) рассматривается как элемент сетевой инфраструктуры, то есть устройство или сегмент сети, физически или логически соединённый с иными элементами сетевой системы. В качестве узлов могут выступать конечные устройства (например, персональные компьютеры), а также специализированное сетевое оборудование: коммутаторы, роутеры (маршрутизаторы) и концентраторы. Каждый узел ИС идентифицируется в сети посредством IP адреса, позволяющего осуществлять маршрутизацию и доставку пакетов данных в сетевой среде. Функции узла ИС детерминированы программным обеспечением и характером взаимодействия с другими элементами сети. Сетевая архитектура обладает свойством адаптивности. В случае утраты отдельными узлами ИС способности вносить вклад в достижение целевых функций сети система может быть реконфигурирована посредством исключения таких неработоспособных или нецелевых узлов, интеграции новых элементов. Функционирование узлов ИС носит системный характер. Они выступают неотъемлемыми компонентами сетевой структуры, обеспечивающими транзит информационных потоков по коммуникационным каналам между взаимодействующими элементами сети.

Таким образом, представленная автором позиция опирается на базовые категории теории права (субъект и объект правоотношения, субъективное право, правосубъектность, юридическая техника, правовая

определённость), теорию ИС и направлена на повышение качества правового регулирования в сфере оборота ЦФА за счёт чёткой юридикации ключевых понятий и конструкций. Содержанием ЦФА, согласно российскому законодательству, являются права доступа в ИС, которые согласно ст. 1226 Гражданского кодекса РФ являются интеллектуальными правами.

## **Выводы**

Несогласованность Закона о защите информации с Законом о ЦФА в определении состава ИС может быть преодолена. В целях совершенствования правового регулирования социальных отношений в сфере оборота ЦФА предлагается в профильный закон ввести понятие «доступ к узлам ИС», под которым понимать доступ пользователей ИС на основе распределённого реестра, обеспечивающий тождественность информации, содержащейся в ИС, при условии предусмотренных законом процедур подтверждения вносимых в неё или изменяемых в ней данных о транзакциях. Одновременно исключить непосредственное отождествление пользователя ИС (субъектов) с узлом ИС (объектом).

Предлагаем для целей Закона о ЦФА под пользователями ИС понимать не узлы ИС, а установленные оператором права доступа в ИС на основе распределённого реестра, обеспечивающие тождественность информации, содержащейся в указанной ИС, посредством процедур подтверждения действительности вносимых в неё (изменяемых в ней) записей. Такое предложение может быть закреплено законодателем в п. 8 ст. 1 Закона, вместо недостаточно корректного, на наш взгляд, определения узла ИС. Пользователем ИС, в которой обрабатываются ЦФА, может выступать юридическое лицо, индивидуальный предприниматель или физическое лицо, при условии, что указанное лицо:

- 1) соответствует требованиям, установленным законодательством Российской Федерации, включая нормативные акты Банка России, к пользователям ИС;
- 2) включено в Реестр пользователей ИС;
- 3) обладает правами доступа к ИС, предоставленными в форме уникального кода.

Предлагаемым методологическим подходом в совершенствовании законодательства о ЦФА является наделение пользователя информационной системы определёнными правами доступа к её узлу без отождествления субъекта-пользователя с таким узлом. Это позволит гармонизировать понимание ИС в законодательстве об информации с Законом о ЦФА.

<sup>11</sup> ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.

## Литература

1. Тумаков А.В. Цифровые финансовые активы как объект цифрового гражданского оборота // Цифровые финансовые активы: вопросы правоприменения. М. : Издательская группа «Юрист», 2025. С. 235—243.
2. Василевская Л.Ю. Деликтная ответственность за нарушение цифровых прав: проблемы и перспективы развития // Цифровые финансовые активы: вопросы правоприменения. М. : Издательская группа «Юрист», 2025. С. 41—49.
3. Зегжда Д.П. Теоретические основы киберустойчивости и практики прогностической защиты от кибератак : монография. СПб. : Политех-Пресс, 2022. 490 с.
4. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Д.П. Зегжды. М. : Горячая линия — Телеком, 2022. 560 с.
5. Метельков А.Н. Понятие информационной системы: технические и нормативно-правовые аспекты // Правовая информатика. 2025. № 2. С. 112—118.
6. Андриевский К.В. Финансово-правовые режимы : дис. ... д-ра юрид. наук : 12.00.04. М., 2022. 503 с.
7. Токолов А.В. Правовое регулирование информационных отношений в сфере оборота цифровых финансовых активов : дис. ... канд. юрид. наук : 12.00.13. М., 2022. С. 43.
8. Порываева Н.Ф. Алгоритмизация права : дис. ... канд. юрид. наук : 12.00.01. М., 2022. 186 с.
9. Жужжалов М.Б. Блокчейн и международно-правовой режим деятельности в киберпространстве // Правоведение. 2019. Т. 63. № 1. С. 62—96. DOI: 10.21638/spbu25.2019.104.
10. Гаврилова Ю.А. Конституционализация информационной безопасности в российском праве: проблема совершенствования теоретической модели // Вестник РУДН. Серия: Юридические науки. 2023. Т. 27. № 1. С. 97—116.
11. Мефодьева К.А. Цифровые данные как объект гражданско-правового регулирования в Германии, США и России : дис. ... канд. юрид. наук : 12.00.03. М., 2019. 228 с.
12. Рождественская Т.Э., Гузнов А.Г. Цифровые финансовые активы: проблемы и перспективы правового регулирования // Актуальные проблемы российского права. 2020. Т. 15. № 6. С. 43—54.
13. Перепеляева Л.В. Цифровые финансовые активы и другие цифровые права. 3-е изд., доп. М. : Nova Creative Group, 2024. 405 с.
14. Гончаров А.И., Садков А.Н., Садков В.А., Давудов Д.А. Цифровая валюта в современной России: юридическое содержание и место в обороте // Право. Журнал Высшей школы экономики. 2023. Том 16. № 3. С. 128—153.
15. Метельков А.Н. Парадокс узлов: защита информации и право цифровой валюты // Защита информации. Инсайд. 2021. № 6. С. 4—12.
16. Еськов С.С. Специальное математическое и программное обеспечение взаимного информационного согласования в системах распределенного реестра : автореф. дис. ... канд. техн. наук : 05.13.11. Воронеж, 2020. 18 с.
17. Короткина А.С. Информационные системы как объект права // Закон и право. 2002. № 5. С. 43—50.

SECTION:  
REGULATORY INFORMATICS

# DIGITAL FINANCIAL ASSETS: REGULATION OF INFORMATION SYSTEM NODES

Metel'kov A.N.<sup>12</sup>

**Keywords:** node, information system, digital rights, blockchain, user, node, validator, virtual machine, cryptocurrency.

## Abstract

**Purpose of work:** To analyze the regulation of information system nodes in the legal regimes governing the circulation of digital financial assets and information protection as interacting systems of legal means. To identify shortcomings in legal techniques in the construction of individual legal terms with technical content, given the increasing technological

<sup>12</sup> **Aleksandr N. Metel'kov**, Ph.D. (Law), Associate Professor at the Department of Applied Mathematics and Information Technology Security of the Saint Petersburg University of the Russian State Fire Service of the Ministry of Civil Defence, Emergencies and Disaster Relief of the Russian Federation, Saint Petersburg, Russian Federation.  
E-mail: [metelkov5178@mail.ru](mailto:metelkov5178@mail.ru)

*sophistication and frequency of cyberattacks. To focus on the relationship between information technology and the individual using it in alternative payment systems, and the legal regulation of social relations regarding their implementation, using the example of a set of legal means used to regulate digital rights and protect associated data.*

**Research methods:** *Using interdisciplinary and comparative legal approaches, the author compares the content of the concept of “information system node” in federal laws. A comparative analysis of the elements of the concept of “information system” in legislation on information and on digital financial assets is conducted.*

**Results of the study:** *The author substantiates and proves the position of an information system node as an object, rather than a subject, of legal relations in the sphere of digital financial asset circulation. The analysis revealed the need for consistent use of definitions regarding the elemental composition of a technical system and the user’s positioning in relation to it. A proposal has been formulated for improving legislation on digital financial assets using blockchain technology regarding the understanding of the term “information system node” in terms of its “objectification”. It has been established that different approaches to defining the concept of “node” in Russian legislation on digital financial assets create difficulties in ensuring information security. A proposal has been developed for the legislator to abandon the legal construct of “user of an information system as its node”, replacing it with a user access scheme for a node of such a system.*

## References

1. Tumakov A.V. Tsifrovye finansovye aktivy kak ob’ekt tsifrovogo grazhdanskogo oborota // Tsifrovye finansovye aktivy: voprosy pravoprimereniia. M. : Izdatel’skaia gruppa “Iurist”, 2025. S. 235—243.
2. Vasilevskaia L.Iu. Deliktnaia otvetstvennost’ za narushenie tsifrovyykh prav: problemy i perspektivy razvitiia // Tsifrovye finansovye aktivy: voprosy pravoprimereniia. M. : Izdatel’skaia gruppa “Iurist”, 2025. S. 41—49.
3. Zegzhda D.P. Teoreticheskie osnovy kiberustoychivosti i praktiki prognosticheskoi zashchity ot kiberatak: monografiia. SPb. : Politekh-Press, 2022. 490 s.
4. Kiberbezopasnost’ tsifrovoi industrii. Teoriia i praktika funktsional’noi ustoychivosti k kiberatakam / Pod red. D.P. Zegzhdy. M. : Goriachaia liniia — Telekom, 2022. 560 s.
5. Metel’kov A.N. Poniatie informatsionnoi sistemy: tekhnicheskie i normativno-pravovye aspekty // Pravovaia informatika. 2025. No. 2. S. 112—118.
6. Andrievskii K.V. Finansovo-pravovye rezhimy : dis. ... d-ra iurid. nauk : 12.00.04. M., 2022. 503 s.
7. Tokolov A.V. Pravovoe regulirovanie informatsionnykh otnoshenii v sfere oborota tsifrovyykh finansovykh aktivov : dis. ... kand. iurid. nauk : 12.00.13. M., 2022. C. 43.
8. Poryvaeva N.F. Algoritmizatsiia prava : dis. ... kand. iurid. nauk : 12.00.01. M., 2022. 186 s.
9. Zhuzhzhlov M.B. Blokchein i mezhdunarodno-pravovoi rezhim deiatel’nosti v kiberprostranstve // Pravovedenie. 2019. T. 63. No. 1. S. 62—96. DOI: 10.21638/spbu25.2019.104.
10. Gavrilova A.A. Konstitutsionalizatsiia informatsionnoi bezopasnosti v rossiiskom prave: problema sovershenstvovaniia teoreticheskoi modeli // Vestnik RUDN. Seriya: Iuridicheskie nauki. 2023. T. 27. No. 1. S. 97—116.
11. Mefod’eva K.A. Tsifrovye dannye kak ob’ekt grazhdansko-pravovogo regulirovaniia v Germanii, SShA i Rossii : dis. ... kand. iurid. nauk : 12.00.03. M., 2019. 228 s.
12. Rozhdestvenskaia T.E., Guznov A.G. Tsifrovye finansovye aktivy: problemy i perspektivy pravovogo regulirovaniia // Aktual’nye problemy rossiiskogo prava. 2020. T. 15. No. 6. S. 43—54.
13. Perepelieva L.V. Tsifrovye finansovye aktivy i drugie tsifrovye prava. 3-e izd., dop. M. : Nova Creative Group, 2024. 405 s.
14. Goncharov A.I., Sadkov A.N., Sadkov V.A., Davudov D.A. Tsifrovaia valiuta v sovremennoi Rossii: iuridicheskoe soderzhanie i mesto v oborote // Pravo. Zhurnal Vysshei shkoly ekonomiki. 2023. Tom 16. No. 3. S. 128—153.
15. Metel’kov A.N. Paradoks uzlov: zashchita informatsii i pravo tsifrovoi valiuty // Zashchita informatsii. Insaid. 2021. No. 6. S. 4—12.
16. Es’kov S.S. Spetsial’noe matematicheskoe i programmnoe obespechenie vzaimnogo informatsionnogo soglasovaniia v sistemakh raspredelenno reestra : avtoref. dis. ... kand. tekhn. nauk : 05.13.11. Voronezh, 2020. 18 s.
17. Korotkina A.S. Informatsionnye sistemy kak ob’ekt prava // Zakon i pravo. 2002. No. 5. S. 43—50.



# ОБОСНОВАННОСТЬ ЭКСПЕРТНОЙ ОЦЕНКИ ПРОГРАММ И МЕТОДИК ИСПЫТАНИЙ

Шелестович О.А.<sup>1</sup>, Свистунов А.В.<sup>2</sup>

**Ключевые слова:** испытательная документация, требования к информационным системам, прослеживаемость требований, нормативные требования, эталонная проверка, достаточность проверки, верификация экспертного вывода, искусственный интеллект, большие языковые модели.

## Аннотация

**Цель работы.** Определить правила обоснованной оценки ПМИ: когда предусмотренная проверка может быть признана достаточной, когда выявленный недостаток служит основанием для замечания и когда оценку следует отложить из-за неполноты исходных документов, в том числе если описание проверки распределено между несколькими документами.

**Метод исследования.** Исследование основано на декомпозиции процесса экспертной оценки ПМИ и формализации условий, связывающих применимое требование, проверяемый результат, эталонную проверку, документарное покрытие и экспертное решение. Сформулированные условия проверены на контрастных учебных случаях, моделирующих полное, распределенное и недостаточное описание проверки, а также неполноту исходных документов.

**Результаты исследования.** Сформулированы условия обоснованной оценки испытательной документации, связывающие применимое требование, самостоятельный проверяемый результат, эталонную проверку, содержание представленных документов и экспертное решение. Разграничены наличие в документации релевантного текста и достаточность предусмотренной проверки для подтверждения обязательного результата. Определены условия учета распределенного описания проверки в нескольких связанных документах и проверки предполагаемого недостатка до формирования замечания, включая поиск возможного альтернативного покрытия и повторную оценку исходного толкования требования. Показано, что неполнота исходных документов, неустановленная применимость требования или неразрешенное противоречие должны сохраняться как неопределенность и не преобразовываться в недостаток испытательной документации. Формализованные отношения используются как условия допустимости положительной оценки и проекта замечания, но не заменяют содержательного анализа применимости требования, достаточности процедуры и существенности выявленного недостатка. Предложенные положения имеют методологический характер и проиллюстрированы учебными случаями; их практическая результативность, межэкспертная согласованность и полнота выявления применимых источников требуют отдельной эмпирической проверки.

DOI: 10.24412/1994-1404-2026-3-208-218

## Введение и постановка задачи

Программа и методика испытаний связывает требования к информационной системе с действиями, по результатам которых предполагается установить их выполнение. При экспертизе необходимо выяснить, позволяют ли предусмотренные проверки получить и подтвердить обязательные результаты. Число сценариев, ссылок и форм протоколов само по себе на этот вопрос не отвечает.

Исходное требование может устанавливать отображение пользователю статуса успешной загрузки, тогда как ПМИ предусматривает лишь загрузку файла и результат «загрузка выполнена». Тематическая связь очевидна, но из нее не следует, что наблюдение пользовательского статуса включено в проверку.

Возможна и обратная ошибка: необходимое действие содержится в обязательной общей процедуре,

<sup>1</sup> Шелестович Олеся Александровна, ведущий системный аналитик Управления проектирования и разработки информационных систем филиала публично-правовой компании «Роскадастр» Центр информационных технологий «Роскадастр-Инфотех», Москва, Россия.

E-mail: ShelestovichOA@kadastr.ru

<sup>2</sup> Свистунов Андрей Васильевич, кандидат технических наук, старший научный сотрудник, руководитель проектов Управления проектирования и разработки информационных систем филиала публично-правовой компании «Роскадастр» Центр информационных технологий «Роскадастр-Инфотех», Москва, Россия.

E-mail: SvistunovAV@kadastr.ru



а способ фиксации — в связанной форме протокола. Отсутствие описания в самом сценарии тогда не доказывает недостатка. Требуется оценить совокупность документов и условия ее применения.

Для правовой информатики существенна связь оценки с нормативными и договорными основаниями. При переходе к проверяемому результату необходимо сохранять условия применимости, обязательные свойства и содержание отсылочных положений. Иначе точная ссылка может сопровождать неверное толкование требования.

Ближайшую методологическую основу составляют две работы, опубликованные в журнале «Правовая информатика». О.А. Шелестович рассматривает восстановление процессов деятельности из проверенного корпуса источников: отбор по применимости, выделение самостоятельных предписаний и экспертное подтверждение интерпретаций [1]. Для экспертизы ПМИ существенны сохранение происхождения требования и различие установленного основания и предварительной интерпретации. Единица анализа в этой работе — процесс деятельности; в настоящем исследовании — предусмотренная проверка самостоятельного результата.

А.В. Свистунов и Д.В. Митавский рассматривают сквозную прослеживаемость, связывающую предписание применимого источника с соответствующим процессом деятельности, решением о его автоматизации, требованием к информационной системе и подтверждением его выполнения. В этой модели уже разграничены процедура проверки, доказательство, документ-носитель и подтверждение соответствия; предусмотрены анализ изменений и аудит доказательного контура [2]. Эти положения принимаются как опубликованная основа. При оценке ПМИ необходимо установить, соответствует ли представленная Исполнителем испытательная документация требованиям контракта и иных применимых источников: предусмотрены ли все необходимые проверки, достаточны ли их содержание и порядок выполнения для подтверждения требуемых результатов и обосновано ли конкретное замечание при выявленном несоответствии. Наличие связанных объектов само по себе этого решения не определяет.

Смежные составляющие этой задачи рассматриваются и в других российских исследованиях. В.В. Грибова, Д.В. Жданов и Е.Е. Помников предлагают модель нормативных знаний, учитывающую контекст и зависимости положений в строительной области [3]. Эта работа дает основание рассматривать формализацию нормативного содержания и связей как уже развиваемое направление. Ее предмет, однако, отличается от оценки того, достаточно ли предусмотренных в ПМИ проверок для обоснованного экспертного заключения.

В исследовании И.М. Малиновского и соавторов обсуждаются управление требованиями, атрибуты источников, версии, согласование и матрицы соответствия в авиадвигателестроении [4]. Для рассматриваемой задачи существенно, что требование и подтверждающая

информация могут быть связаны и организованы систематически. Наличие такой организации не снимает вопроса о содержательной достаточности конкретной проверки. Сравнение функций систем управления требованиями также не является проверкой эффективности предлагаемого здесь метода.

Ближе к предмету испытательной документации находятся работы, связывающие выявление требований с последующим тестированием и прослеживаемостью. Е.А. Герлиц, Д.С. Кильдишев и А.В. Хорошилов рассматривают выявление функциональных требований из документации программного интерфейса для задач функционального тестирования [5]. Б.А. Позин и Г.Н. Циперман рассматривают прослеживаемость требований как основу проектирования функционально-логической архитектуры программной системы [6]. Для настоящей задачи существенно сохранение связи между исходным требованием и объектами последующей проверки; сама прослеживаемость, однако, не определяет достаточность конкретной процедуры ПМИ.

К.А. Шишин, И.В. Муравьев и Е.К. Куликов исследуют автоматическую генерацию модульных тестов с учетом контекста Java-приложений [7]. Эта работа подтверждает возможность автоматизации отдельных операций формирования тестов, но решает иную задачу: тест создается для программной реализации, тогда как в настоящем исследовании оценивается уже представленная испытательная документация относительно независимо определенного состава необходимых проверок.

О. Kosenkov и соавторы в систематическом обзоре требований к регуляторному соответствию программных систем рассматривают роль инженерии требований, связанные проблемы и практики, а также ее взаимодействие с другими процессами жизненного цикла [8]. Для экспертизы ПМИ это подтверждает необходимость связывать применимые внешние требования с объектами разработки и проверки, но не дает самостоятельного критерия достаточности испытательной процедуры.

А. Murugesan и соавторы исследуют автоматизированный семантический анализ assurance cases — структурированных аргументов, связывающих утверждения и свидетельства [9]. Для настоящей работы существенна сама идея проверки не только наличия отдельных элементов, но и связей между ними. Вместе с тем корректность исходного толкования применимого требования остается отдельной содержательной задачей.

R. Kato и соавторы в критическом обзоре самокоррекции языковых моделей показывают зависимость результата от типа обратной связи и отмечают более надежные результаты при наличии внешней обратной связи [10]. Это существенно при проверке предполагаемого недостатка с применением языковых моделей: повторный запрос к той же модели не должен трактоваться как независимое подтверждение исходного вывода.

В совокупности эти исследования охватывают отдельные составляющие рассматриваемой задачи — выявление и прослеживаемость требований, регуляторное со-

## Исследовательские направления и задача обоснования оценки ПМИ

| Направление и источник                               | Результат, существенный для постановки задачи                                                            | Что необходимо дополнительно определить для оценки ПМИ                                                   |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Установление требований по источникам [1, 3, 5]      | Отбор применимого содержания, выделение предписаний и функциональных требований, учет контекстных связей | Как из установленного требования определить самостоятельный проверяемый результат и необходимую проверку |
| Прослеживаемость и управление требованиями [2, 4, 6] | Связи между источниками, требованиями, решениями и подтверждением; учет версий и изменений               | Когда совокупность связанных фрагментов ПМИ содержательно достаточна для проверки                        |
| Автоматизация формирования тестов [7]                | Генерация тестов с учетом программного контекста                                                         | Как отделить создание новой проверки от экспертизы уже представленной ПМИ                                |
| Инженерия регуляторных требований [8]                | Систематизация проблем и практик обеспечения соответствия программных систем внешним требованиям         | Как применимое требование используется как основание оценки конкретной испытательной процедуры           |
| Семантический анализ аргументации [9]                | Проверка структуры утверждений, связей и свидетельств в assurance cases                                  | Как обосновать переход от найденных фрагментов к экспертному выводу о достаточности или недостатке       |
| Самокоррекция языковых моделей [10]                  | Зависимость самопроверки от типа и надежности обратной связи                                             | Как проверять предполагаемый недостаток без подмены независимой проверки повторным ответом модели        |

ответствие, формирование тестов, проверку аргументации и машинную самопроверку. Предмет настоящей работы уже: условия, при которых содержание ПМИ позволяет обоснованно признать проверку достаточной, подтвердить конкретный недостаток либо сохранить нерешенный вопрос.

Сопоставление этих направлений с задачей настоящего исследования представлено в таблице 1.

Прослеживаемость, формализация нормативных знаний, автоматизация тестирования и машинная поддержка анализа не рассматриваются в настоящей работе как новые сами по себе. Рассмотренные исследования показывают существование самостоятельных решений для этих задач [1—10]. Предлагаемое решение сосредоточено на условиях перехода от применимого требования к оценке уже предусмотренной проверки ПМИ и к обоснованию конкретного экспертного решения. Отсутствие полного аналога в отобранных работах не используется как доказательство мирового приоритета.

Исследовательский вопрос состоит в том, какие условия позволяют различить три возможных результата документарной экспертизы ПМИ: признание предусмотренной проверки достаточной, подтверждение существенного недостатка и сохранение неопределенности, препятствующей обоснованной оценке. Для решения этой задачи рассматривается последовательная связь между применимым требованием, самостоятельным проверяемым результатом, эталонной проверкой, содержанием представленной Исполнителем документации и экспертным решением. Условия перехода между этими элементами формализуются и раскрываются на учебных случаях, включающих локальное и распре-

деленное описание проверки, недостаточность предусмотренной процедуры и отсутствие документа, необходимого для установления содержания требования.

Предлагаемое решение связывает три группы условий: установление необходимой проверки на основе применимых требований, оценку ее обеспечения совокупностью положений ПМИ и связанных документов, а также проверку предполагаемого недостатка путем поиска возможного альтернативного покрытия до формирования замечания. По отношению к рассмотренным исследованиям это позволяет конкретизировать задачу именно для экспертизы испытательной документации: необходимый состав проверок определяется до сопоставления с документацией Исполнителя, а отрицательная оценка требует проверки возможного альтернативного покрытия.

## РЕШЕНИЕ ПОСТАВЛЕННОЙ ЗАДАЧИ

## Предмет оценки и применимость исходных оснований

Предмет метода — достаточность программы и методики испытаний вместе со связанными сценариями, общими процедурами, приложениями и формами протоколов. Далее этот комплект обозначается как ПМИ. Оценивается предусмотренная проверка самостоятельного результата, а не документ или число ссылок.

Область оценки задается объектом, этапом работ, видом испытаний, требованиями и редакциями документов. Положительный вывод относится к предусмотренной проверке. Он не подтверждает проведение испытания или соответствие системы требованию.

Недостаток ПМИ также не доказывает отсутствия функции в системе.

Исходным основанием может выступать положение договора, технического задания, применимого нормативного правового, нормативно-технического или методического документа. Для его использования требуется установить не только реквизиты, но и конкретное содержание, относящееся к рассматриваемому объекту и условиям. Упоминание документа в общем перечне не заменяет такого установления. Вместе с тем содержание требования может быть распределено: один документ задает обязанность, другой определяет обязательный состав результата или порядок его оценки. Исключение второго документа способно изменить смысл первого.

Отбор источников по редакции, применимости и роли в исследуемой области опирается на подход О.А. Шелестович [1]. Критерии выделения предписаний используются с учетом иной задачи: самостоятельность процесса и самостоятельность проверяемого результата не тождественны.

При восстановлении требования необходимо сохранять условия, ограничения, исключения и содержание документов, к которым оно отсылает. Современные исследования *regulatory requirements engineering* рассматривают выявление и анализ внешних требований как самостоятельную часть обеспечения соответствия программных систем [8]. Для каждого включенного положения необходимо объяснить, какой существенный элемент оно добавляет. Такая полнота относится к установленной области экспертизы и не означает получения всех существующих источников по теме.

Например, требование предоставить результат загрузки «в порядке, установленном приложением» не позволяет до получения приложения заключить, что обязательным является именно отображение статуса на экране пользователя. В равной мере отсутствие этого приложения не позволяет исключить соответствующую обязанность. До выяснения содержания основания возникает нерешенный вопрос. Замечание об отсутствии проверки экранного статуса в такой ситуации было бы преждевременным: обязательность самого результата еще не установлена.

Применимость источника необходимо отличать от отнесения проверки к конкретному виду контроля. Документ, определяющий обязательный состав результата, может быть необходим для понимания требования, даже если отдельная проверка одного его свойства не относится к рассматриваемой опытной эксплуатации. Сначала восстанавливается полное содержание требования, затем определяется, какие его результаты должны подтверждаться в установленной области испытаний. Сужение области контроля не должно незаконно обеднять исходное требование.

Договорная область экспертизы и юридическая применимость требований также не тождественны. Настоящий метод не устанавливает универсального порядка определения юридической силы документов

и не предполагает, что договорный перечень исчерпывает все обязательные требования. Потенциально применимое основание вне согласованного предмета работы должно быть отмечено и рассмотрено отдельно. Вывод о достаточности ПМИ ограничивается той областью, для которой применимость и содержание оснований действительно установлены.

Связь с основанием должна позволять восстановить, почему результат обязателен для данного объекта и какие его свойства проверяются. Эта же связь обосновывает замечание: эксперт указывает, какое требование нельзя надлежащим образом оценить по представленной документации.

### Независимый эталон как основание сравнения

Метод включает две стадии. На первой стадии по требованиям контракта и применимым положениям иных документов, уточняющих их содержание, формируется необходимый состав проверяемых результатов и условий их подтверждения. На второй стадии этот состав сопоставляется с ПМИ Исполнителя. Проверяемая документация не должна определять обязательный состав результатов первой стадии.

Результат первой стадии — внутренний эталон проверки. Это основание сравнения, а не образец оформления для Исполнителя. Эталон не задает структуру документов и способ реализации системы, если они не установлены применимым требованием.

Независимость означает формирование эталона из оснований до сопоставления с ПМИ. Она не гарантирует безошибочности толкования. Разделение заданий одного эксперта или программного средства не доказывает независимости ошибок; соблюдение установленного порядка должно быть проверяемо по материалам работы.

Самостоятельный результат допускает отдельный вывод о соответствии. Загрузка данных и отображение пользователю ее статуса связаны одной операцией, но подтверждают разные свойства: совпадение загруженных записей с исходными не доказывает наблюдения статуса.

Условие, параметр или критерий не становятся отдельной проверкой автоматически. Условие «после успешной загрузки» сохраняется при оценке отображения. Разделять проверки следует там, где нужны самостоятельные выводы, а объединять — когда единая процедура и свидетельства позволяют принять общее решение без потери смысла.

Эталонная проверка определяет основание, результат, исходные условия и данные, действия, критерий и предполагаемый способ фиксации. Обязательные варианты и исключения сохраняются в объеме полного требования.

Состав и подробность описания зависят от способа проверки. Для анализа наличия раздела документа и наблюдения поведения системы нужны разные действия. Элемент существен, если без него нельзя

обосновать проведение проверки или оценку результата. Общая формулировка «работает корректно» не заменяет признака соответствия.

Различение процедуры, свидетельства, его документального носителя и решения о соответствии следует модели Свистунова и Митавского [2]. Здесь оно применяется к планируемому испытанию: оценка ПМИ касается возможности получить свидетельство, а не признания уже полученного доказательства.

В эталоне указывается предполагаемый вид свидетельства, а не полученный результат. Протокол может связывать операцию, наблюдение и заключение. Скриншот допустим как один из способов фиксации, но его обязательность нельзя выводить из предпочтения эксперта.

До сопоставления проверяются основания эталона, представление обязательных результатов, допустимость объединений и отсутствие добавленных свойств. Редакция фиксируется. Новое существенное основание требует явного пересмотра эталона и затронутых оценок; скрытая подгонка под ПМИ недопустима.

### Условия достаточности и допустимости экспертного вывода

Вторая стадия начинается с поиска фрагментов, относящихся к эталонной проверке. Найденная связь — кандидат на покрытие. Для вывода о достаточности необходимо проверить содержание действий, критериев и фиксации результата.

Возможность представления одного объекта в нескольких документах уже предусмотрена в модели прослеживаемости [2]. Для экспертизы требуется дополнительно оценить обязательность их совместного применения и содержательную согласованность.

Документарное покрытие — обеспечение эталонной проверки положениями ПМИ и связанных документов. Оно может быть локальным или распределенным: это характеристика размещения содержания, а не его достаточности.

Для распределенного покрытия должны выполняться дополнительные условия связи. Фрагменты относятся к рассматриваемой операции и совместимым редакциям документов; их совместное применение обязательно в заданном контексте; между ними нет противоречия, влияющего на вывод; недостающее действие или критерий не восстанавливаются догадкой. Общая форма протокола сама по себе не доказывает обязательность наблюдения, если сценарий и общая процедура такого действия не предусматривают.

Формализацию этих условий удобно ограничить несколькими обозначениями. Пусть  $q$  — эталонная проверка,  $E(q)$  — множество ее существенных элементов,  $D$  — фиксированный доступный комплект испытательной документации, а  $F \subseteq D$  — совокупность рассматриваемых фрагментов. Обозначим через  $B(q)$  установленность и достаточность основания проверки; через  $A(F, q)$  — обязательность и согла-

сованность применения фрагментов к этой проверке; через  $C(F, e)$  — содержательное обеспечение элемента  $e$  данными фрагментами. Наконец,  $U$  означает наличие критической неразрешенности в основаниях соответствующего вывода.

Эти отношения требуют содержательного обоснования. Например, отношение  $C(F, e)$  для наблюдения статуса должно опираться на предусмотренное действие и доступный оценке результат, а не только на наличие в тексте слова «статус». В отличие от инструментального анализа формальной аргументации [9], здесь не реализован автоматический вывод из модели. Формулы ниже описывают условия допуска проекта оценки; они не являются алгоритмом проверки смысла и не доказывают полноты системы решений.

Условие допуска положительной документарной оценки записывается следующим образом:

$$\text{Sufficient}(q, D) \Leftarrow B(q) \wedge \exists F \subseteq D \left[ A(F, q) \wedge \bigwedge_{e \in E(q)} C(F, e) \right] \wedge \neg U.$$

В этой записи  $\neg U$  означает установленное отсутствие блокирующей неопределенности. Неизвестное значение необходимого условия не разрешает вывод. Формальная запись оставляет открытыми проверку полноты  $E(q)$  и учет противоречащих обязательных положений вне выбранного  $F$ ; эти вопросы нельзя считать решенными одним наличием подтверждающих фрагментов.

Отрицательная оценка не получается простым отрицанием положительной. Ненайденное покрытие может означать дефицит, неполный поиск, недоступность документа или неясность основания. Причину требуется установить.

Пусть  $G(g, q, D)$  означает установленный существенный дефицит  $g$ , препятствующий проверке результата  $q$  по комплексу  $D$ , а  $K(g, q, D)$  — выполненное рассмотрение альтернативного покрытия, не устранившее данный дефицит. Тогда условие формирования проекта замечания имеет вид:

$$\text{DraftRemark}(g, q, D) \Leftarrow B(q) \wedge G(g, q, D) \wedge K(g, q, D) \wedge \neg U.$$

Для  $G$  указываются конкретный дефицит и его существенность; для  $K$  — рассмотренные альтернативы и причины, по которым они не устранили дефицит. Вывод ограничен установленным корпусом. Конечный поиск не доказывает отсутствия неизвестных документов.

У Шелестович предусмотрен второй эксперт для спорных случаев и сохранение неподтвержденного статуса до согласования [1]. Здесь предполагаемый недостаток подвергается дополнительной проверке: необходимо установить, не устраняется ли он другими положениями испытательной документации либо иной допустимой интерпретацией исходного требования. Само участие второго проверяющего еще не доказывает



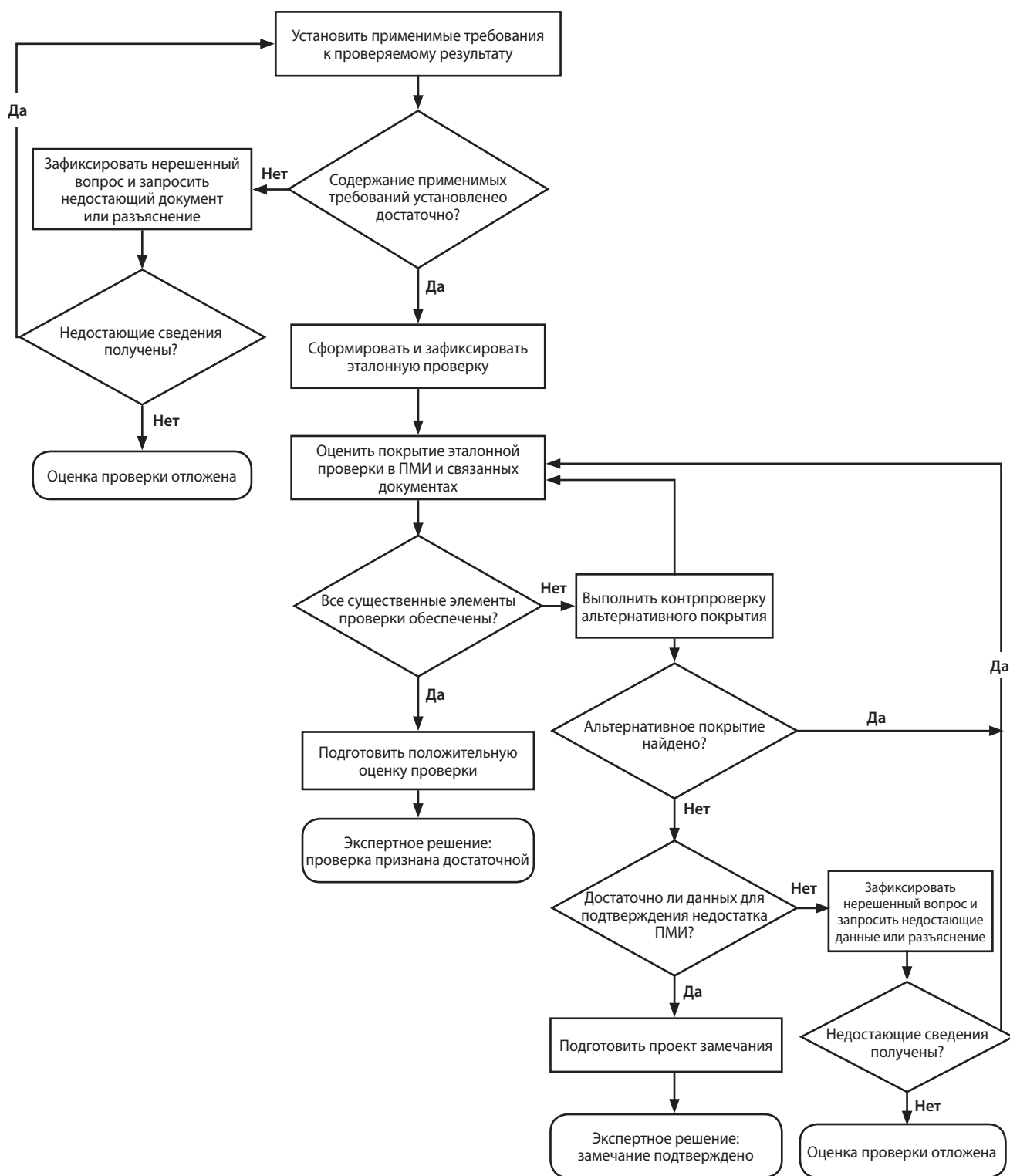


Рис. 1. Условия перехода от основания проверки к экспертному решению

Условия и границы трех исходов оценки

| Исход                          | Необходимые основания                                                                                                           | Допустимое действие                                                            | Недопустимая подмена                                                                                    |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Достаточность                  | Обоснованная проверка; согласованное обязательное покрытие всех существенных элементов; разрешенные основания вывода            | Подготовить положительную оценку данной проверки для экспертного подтверждения | Признать достаточность по тематическому совпадению или заполнению граф                                  |
| Подтвержденная недостаточность | Существенный дефицит; его связь с обязательным результатом; рассмотренные альтернативы; отсутствие блокирующей неопределенности | Сформулировать предметный проект замечания                                     | Приравнять ненайденный фрагмент к отсутствующей проверке без поиска возможного альтернативного покрытия |
| Неразрешенность                | Указанная неопределенность, препятствующая содержательному решению                                                              | Зафиксировать зависимую область и запросить недостающее основание либо решение | Выдать недостаток данных за недостаток ПМИ или за подтвержденную достаточность                          |

независимости ошибок. Рассматриваются другие сценарии, общие процедуры, приложения, формы фиксации и распределенные связи. Одновременно проверяется, не добавил ли эксперт отсутствующее в основании требование. Повторения того же поискового запроса недостаточно: проверка предполагаемого недостатка должна завершаться обоснованием того, почему рассмотренное альтернативное покрытие его не устраняет.

Неразрешенность означает, что недостаток основания, противоречие или отсутствие данных мешают обосновать содержательный вывод. Она требует получения документа, уточнения применимости или разрешения спорной интерпретации. Зависимая область остается открытой, даже если независимые проверки завершены. Доказанная неприменимость требования отличается от неизвестной применимости; в приведенных формулах и схеме это различие отдельно не формализовано.

Общая логика переходов представлена на схеме (рис. 1).

Если не предусмотрена проверка одного обязательного пользовательского результата, отсутствие действия наблюдения, критерия и фиксации может описываться одним замечанием. Это не исключает разделения независимых дефицитов. Основанием группировки служит содержание необходимого исправления, а не число отсутствующих граф.

Состав обоснования систематизирован в таблице 2.

Эксперт проверяет основание, существенность дефицита, альтернативное покрытие и формулировку. Его аналитический вывод оформляется и утверждается в порядке, установленном для конкретной экспертизы. Метод сам по себе не определяет полномочий на направление замечания или приемку результата работ.

Для поиска и подготовки вариантов толкования могут использоваться программные средства, в том числе языковые модели. Содержательная оценка их предложений остается необходимой: правильность структуры записи не подтверждает правильности толкования.

Исследования самокоррекции языковых моделей показывают существенную зависимость результата от типа и надежности обратной связи [10]. Поэтому повторная генерация не заменяет проверку исходного источника и независимую содержательную оценку.

### Сквозная учебная демонстрация

Рассмотрим учебный пример. Применимое требование устанавливает: «После успешной загрузки набора данных система должна отображать пользователю статус успешного завершения операции». Задача экспертизы состоит в том, чтобы установить, позволяет ли предусмотренная в ПМИ проверка подтвердить именно этот результат, а не только факт успешной загрузки. Поэтому эталонная проверка должна предусматривать успешное выполнение загрузки, наблюдение пользователем соответствующего статуса, однозначный критерий его связи с завершенной операцией и фиксацию результата наблюдения.

**Первый вариант: проверка результата не предусмотрена.** В ПМИ предусмотрены загрузка файла и подтверждение ее успешности путем сопоставления загруженных данных с исходным набором. Форма протокола позволяет зафиксировать выполнение загрузки и результат сопоставления. Однако ни в сценарии, ни в общей процедуре, ни в форме протокола не предусмотрены наблюдение пользовательского статуса, критерий его отображения и фиксация этого результата. Таким образом, документация позволяет подтвердить успешность загрузки, но не обеспечивает проверку предусмотренного требованием пользовательского результата.

Проверка связанных документов не выявляет положения, которое устраняло бы этот недостаток. Поэтому может быть подготовлен следующий проект замечания:

В ПМИ предусмотрены выполнение загрузки и подтверждение ее успешности сопоставлением данных,

однако не предусмотрена проверка отображения пользователю статуса успешного завершения операции. Необходимо предусмотреть проверку указанного результата, однозначный критерий его оценки и фиксацию результата проверки.

Такое замечание относится к испытательной документации. Оно не означает, что соответствующая функция отсутствует в системе, и не предписывает конкретный способ ее реализации.

**Второй вариант: проверка описана в нескольких связанных документах.** В сценарии установлена обязательность общей процедуры, которая наряду с подтверждением успешности загрузки требует проверить отображение пользователю статуса этой операции. Форма протокола предусматривает фиксацию наблюдаемого статуса и результата проверки. В этом случае отсутствие полного описания непосредственно в сценарии не является недостатком: необходимые элементы проверки распределены между связанными документами и должны оцениваться совместно.

Однако наличие всех необходимых элементов еще не означает, что процедура достаточна. Если наблюдение статуса начинается только после сопоставления загруженных данных, кратковременно отображаемый статус может быть пропущен. Исходное требование не устанавливает обязанность сохранять его до окончания сопоставления, поэтому такое свойство нельзя добавлять к требованию при экспертизе. До уточнения порядка наблюдения положительная оценка этой проверки преждевременна.

**Третий вариант: содержание требования установлено не полностью.** Предположим, что исходный документ требует предоставлять результат загрузки «в порядке и составе, установленных приложением», однако само приложение отсутствует. В такой ситуации нельзя заранее считать обязательным именно отображение пользовательского статуса: содержание требования еще не восстановлено полностью. Детально описанная процедура загрузки в ПМИ этого пробела не устраняет. Сначала необходимо получить и проверить отсутствующий документ, установить полное содержание требования и лишь затем формировать соответствующую эталонную проверку и оценивать ее наличие в ПМИ.

Три варианта показывают разные основания экспертного решения. В первом случае после проверки возможного альтернативного покрытия подтверждается конкретный недостаток ПМИ. Во втором необходимое содержание найдено в совокупности документов, но остается вопрос о достаточности предусмотренной процедуры. В третьем имеющихся исходных документов недостаточно даже для установления того, что именно должна подтверждать проверка. Следовательно, отсутствие текста в одном месте документации само по себе не доказывает недостатка, а подробность ПМИ не компенсирует неполноту требования, с которым она сопоставляется.

### Ограничения обоснования и дальнейшая проверка

Предложенный подход позволяет проследить экспертную оценку ПМИ от применимого требования до конкретной проверки и сформированного замечания. Однако обоснованность такого вывода зависит от того, насколько корректно определен исходный корпус требований. Прослеживаемость найденных положений подтверждает происхождение использованных требований, но сама по себе не доказывает, что выявлены все документы, способные повлиять на содержание проверки. Поэтому границы рассмотренного корпуса, недоступные документы и неразрешенные отсылки должны сохраняться в материалах экспертизы, а выводы — относиться к той области, для которой применимость и содержание требований действительно установлены.

Вторая группа ограничений связана с содержательной интерпретацией. Не все решения могут быть получены из формальных связей между документами. В частности, эксперт должен определить, образует ли положение самостоятельный проверяемый результат, какие элементы необходимы для его подтверждения и обеспечивает ли совокупность фрагментов ПМИ достаточную проверку. Формализация делает основания таких решений явными и позволяет локализовать разногласия, но не подменяет профессионального анализа содержания требований и испытательной документации.

Отдельное ограничение связано с независимостью стадий анализа. Формирование эталонной проверки до изучения соответствующего содержания ПМИ снижает риск подгонки необходимой проверки под представленную документацию. Аналогично, отрицательная или частичная оценка требует дополнительной проверки: поиска возможного альтернативного покрытия и проверки исходного толкования требования. Вместе с тем организационное разделение стадий еще не гарантирует независимости ошибок: одинаковые исходные предпосылки или одна и та же ошибочная интерпретация могут воспроизводиться на нескольких этапах анализа. В самой статье поэтому различается разделение процедур и доказанная независимость их результатов.

Технологии искусственного интеллекта в этой схеме целесообразно рассматривать как средство поддержки отдельных аналитических операций: выявления ссылок и потенциально применимых источников, поиска относящихся к эталонной проверке фрагментов ПМИ, подготовки вариантов интерпретации и поиска возможного альтернативного покрытия. Их использование особенно полезно при работе с объемным и распределенным документарным корпусом. При этом машинно найденное соответствие не является доказательством достаточности проверки, а предложенная интерпретация — установленным содержанием требования. Содержательная оценка применимости

источника, достаточности предусмотренной проверки и обоснованности замечания остается предметом экспертного решения. В предлагаемом подходе технологии искусственного интеллекта рассматриваются как средство поддержки отдельных аналитических операций; оценка применимости требований, достаточности проверки и обоснованности замечания остается предметом экспертного решения.

Дальнейшая проверка подхода может быть направлена не только на итоговые замечания, но и на устойчивость отдельных стадий: полноту формирования корпуса требований, согласованность выделения самостоятельных результатов, воспроизводимость оценки распределенного покрытия и результативность проверки предполагаемых недостатков. На реальных обезличенных комплексах ПМИ с независимой экспертной разметкой можно также отдельно исследовать, как применение ИИ влияет на поиск релевантных фрагментов, выявление альтернативного покрытия, число требующих ручного разрешения случаев и общую трудоемкость экспертизы.

### Результаты и выводы

В работе сформулированы условия обоснованной документарной оценки программ и методик испытаний. Исходной точкой такой оценки являются требования контракта и применимые положения иных источников, определяющие обязательные результаты и условия их проверки. На их основе до сопоставления с документацией Исполнителя формируется эталонная проверка, после чего устанавливается, предусмотрена ли соответствующая проверка в ПМИ и позволяет ли она однозначно подтвердить требуемый результат. Тем самым содержание представленной ПМИ не используется для определения того, что именно должно быть проверено.

Основным объектом оценки выступает не отдельная ссылка или фрагмент текста, а предусмотренная проверка самостоятельного результата. Наличие относящегося к требованию текста еще не означает достаточности проверки. Необходимые действия, критерии и способы фиксации могут быть распределены между сценарием, общей процедурой, приложением и формой протокола; поэтому их следует оценивать в совокупности с учетом обязательности совместного применения и согласованности содержания. Положительная оценка допустима, когда эта совокупность позволяет выполнить необходимую проверку и однозначно оценить ее результат. При этом такая оценка относится к испытательной документации и сама по себе не подтверждает фактическое выполнение требования информационной системой.

Отрицательная оценка требует дополнительно обоснования. Если часть необходимой проверки первоначально не найдена, прежде чем формировать замечание, рассматриваются другие связанные документы, возможное распределенное описание и правильность исходного толкования требования. Только

после исключения альтернативного покрытия установленный недостаток может служить основанием для проекта замечания. Если же содержание требования не может быть достоверно определено из-за отсутствующего документа, неясной применимости источника или неразрешенного противоречия, формируется нерешенный вопрос, а зависимая оценка откладывается. Поэтому в методе различаются три результата: достаточность предусмотренной проверки, подтвержденная недостаточность и невозможность обоснованной оценки до получения недостающих сведений.

Учебная демонстрация показывает различие этих ситуаций на одном проверяемом результате. Подтверждение успешной загрузки данных не заменяет проверки отображения пользователю статуса завершения операции. Вместе с тем отсутствие такого действия непосредственно в сценарии не является недостатком, если оно предусмотрено обязательной общей процедурой и надлежащим образом фиксируется. Даже при наличии распределенного описания необходимо оценивать выполнимость всей процедуры: порядок действий может не позволять наблюдать требуемый результат. Если же обязательное содержание требования определяется отсутствующим приложением, сопоставление ПМИ с предполагаемой проверкой до получения этого документа было бы необоснованным.

Формальная запись используется в работе для фиксации условий, при которых допустим переход к положительной оценке или проекту замечания. Она не заменяет содержательной оценки применимости требования, самостоятельности проверяемого результата, достаточности предусмотренной процедуры и согласованности связанных документов. Такой способ представления делает явными основания экспертного решения и позволяет отделить установленный недостаток ПМИ от неполноты исходных данных или поисковой процедуры.

Технологии искусственного интеллекта могут поддерживать отдельные операции этого процесса: поиск ссылок и потенциально применимых источников, выявление относящихся к эталонной проверке фрагментов документации, подготовку вариантов интерпретации и поиск возможного альтернативного покрытия. Полученный машиной результат рассматривается как аналитический материал, а не как самостоятельное экспертное решение. Оценка применимости требований, достаточности проверки и обоснованности замечания сохраняется за экспертом.

Предложенный подход обеспечивает прослеживаемую связь между применимым требованием, проверяемым результатом, необходимой проверкой, содержанием ПМИ и экспертным решением. Такая связь позволяет установить не только результат оценки, но и основания, по которым предусмотренная проверка признана достаточной, выявленный недостаток подтвержден либо принятие решения отложено до получения недостающих сведений.



**Информация о финансировании.**

Исследование выполнено в инициативном порядке.

**Литература**

1. Шелестович О.А. Метод идентификации процессов деятельности при создании информационных систем // Правовая информатика. 2026. № 2. С. 114—126. DOI: 10.24412/1994-1404-2026-2-114-126.
2. Свистунов А.В., Митавский Д.В. Нормативно-ориентированная архитектура сквозной прослеживаемости требований к информационным системам // Правовая информатика. 2026. № 2. С. 346—369. DOI: 10.24412/1994-1404-2026-2-346-369.
3. Грибова В.В., Жданов Д.В., Помников Е.Е. Онтологическое моделирование нормативных знаний в строительной отрасли // Онтология проектирования. 2026. Т. 16. № 2 (60). С. 226—239. DOI: 10.18287/2223-9537-2026-16-2-226-239.
4. Малиновский И.М., Стародумов А.В., Мягков К.А., Юсипов Б.Х. Актуальность внедрения системы управления требованиями в производственный процесс авиадвигателестроительной отрасли // Вестник Самарского университета. Аэрокосмическая техника, технологии и машиностроение. 2024. Т. 23. № 2. С. 167—177. DOI: 10.18287/2541-7533-2024-23-2-167-177.
5. Герлиц Е.А., Кильдишев Д.С., Хорошилов А.В. Выявление функциональных требований в документации программного интерфейса приложения для функционального тестирования // Труды Института системного программирования РАН. 2022. Т. 34. Вып. 1. С. 7—22. DOI: 10.15514/ISPRAS-2022-34(1)-1.
6. Позин Б.А., Циперман Г.Н. Прослеживаемость требований как основа проектирования функционально-логической архитектуры программной системы // Труды Института системного программирования РАН. 2022. Т. 34. Вып. 1. С. 23—34. DOI: 10.15514/ISPRAS-2022-34(1)-2.
7. Шишин К.А., Муравьев И.В., Куликов Е.К. Об автоматической генерации модульных тестов для Java-приложений, использующих фреймворк Spring // Труды Института системного программирования РАН. 2024. Т. 36. Вып. 2. С. 59—72. DOI: 10.15514/ISPRAS-2024-36(2)-5.
8. Kosenkov O., Elahidoost P., Gorschek T., Fischbach J., Mendez D., Unterkalmsteiner M., Fucci D., Mohanani R. Systematic Mapping Study on Requirements Engineering for Regulatory Compliance of Software Systems // Information and Software Technology. 2025. Vol. 178. Art. 107622. DOI: 10.1016/j.infsof.2024.107622.
9. Murugesan A., Wong I., Arias J., Stroud R., Varadarajan S., Salazar E., Gupta G., Bloomfield R., Rushby J. Automating Semantic Analysis of System Assurance Cases Using Goal-Directed ASP // Theory and Practice of Logic Programming. 2024. Vol. 24. No. 4. P. 805—824. DOI: 10.1017/S1471068424000425.
10. Kamoi R., Zhang Y., Zhang N., Han J., Zhang R. When Can LLMs Actually Correct Their Own Mistakes? A Critical Survey of Self-Correction of LLMs // Transactions of the Association for Computational Linguistics. 2024. Vol. 12. P. 1417—1440. DOI: 10.1162/tacl\_a\_00713.

**SECTION:**  
REGULATORY INFORMATICS

## VALIDITY OF EXPERT ASSESSMENT OF TEST PROGRAMS AND PROCEDURES

*Shelestovich O.A.<sup>3</sup>, Svistunov A.V.<sup>4</sup>*

**Keywords:** *test documentation, information system requirements, requirements traceability, regulatory requirements, reference test, test sufficiency, verification of expert conclusions, artificial intelligence, large language models.*

<sup>3</sup> **Olesya A. Shelestovich**, Lead Systems Analyst, Information Systems Design and Development Department, Roskadastr-Infotech Information Technology Center, branch of the Public Law Company Roskadastr, Moscow, Russia.

E-mail: [ShelestovichOA@kadastr.ru](mailto:ShelestovichOA@kadastr.ru)

<sup>4</sup> **Andrey V. Svistunov**, Ph.D. (Technology), Senior Researcher, Project Manager, Information Systems Design and Development Department, Roskadastr-Infotech Information Technology Center, branch of the Public Law Company Roskadastr, Moscow, Russia.

E-mail: [SvistunovAV@kadastr.ru](mailto:SvistunovAV@kadastr.ru)

### Abstract

**Purpose.** To define the rules for a well-founded assessment of test programs and procedures (TPPs): when a specified test can be considered sufficient, when an identified deficiency provides grounds for an expert comment, and when the assessment should be deferred because the source documentation is incomplete, including cases where the description of a test is distributed across several documents.

**Research method.** The study is based on decomposing the expert assessment of TPPs and formalizing the conditions linking an applicable requirement, a verifiable result, a reference test, documentary coverage, and an expert decision. The proposed conditions are examined using contrasting instructional cases that model complete, distributed, and insufficient descriptions of a test, as well as incomplete source documentation.

**Results.** The conditions for a well-founded assessment of test documentation have been formulated by linking an applicable requirement, a distinct verifiable result, a reference test, the content of the submitted documents, and the expert decision. A distinction is made between the presence of relevant text in the documentation and the sufficiency of the specified test for confirming the required result. Conditions are defined for assessing a test whose description is distributed across several related documents and for verifying a presumed deficiency before an expert comment is formulated, including the search for possible alternative coverage and reconsideration of the initial interpretation of the requirement. It is shown that incomplete source documentation, uncertain applicability of a requirement, or an unresolved contradiction should remain sources of uncertainty rather than be treated as deficiencies in the test documentation. The formalized relations are used as conditions governing the admissibility of a positive assessment and a draft expert comment, but they do not replace substantive analysis of requirement applicability, procedural sufficiency, or the materiality of an identified deficiency. The proposed provisions are methodological in nature and are illustrated through instructional cases; their practical effectiveness, inter-expert agreement, and the completeness of identifying applicable sources require separate empirical evaluation.

### References

1. Shelestovich O.A. Metod identifikatsii protsessov deiatel'nosti pri sozdanii informatsionnykh sistem // Pravovaia informatika. 2026. No. 2. S. 114—126. DOI: 10.24412/1994-1404-2026-2-114-126.
2. Svistunov A.V., Mitavskii D.V. Normativno-orientirovannaia arkhitektura skvoznoi proslezhivaemosti trebovani k informatsionnym sistemam // Pravovaia informatika. 2026. No. 2. S. 346—369. DOI: 10.24412/1994-1404-2026-2-346-369.
3. Gribova V.V., Zhdanov D.V., Pomnikov E.E. Ontologicheskoe modelirovanie normativnykh znani v stroitel'noi otrasli // Ontologiya proektirovaniia. 2026. T. 16. No. 2 (60). S. 226—239. DOI: 10.18287/2223-9537-2026-16-2-226-239.
4. Malinovskii I.M., Starodumov A.V., Miagkov K.A., Iusipov B.Kh. Aktual'nost' vnedreniia sistemy upravleniia trebovaniiami v proizvodstvennyi protsess aviadvigatelistroitel'noi otrasli // Vestnik Samarskogo universiteta. Aerokosmicheskaiia tekhnika, tekhnologii i mashinostroenie. 2024. T. 23. No. 2. S. 167—177. DOI: 10.18287/2541-7533-2024-23-2-167-177.
5. Gerlits E.A., Kil'dishev D.S., Khoroshilov A.V. Vyavlenie funktsional'nykh trebovani v dokumentatsii programmnogo interfeisa prilozheniia dlia funktsional'nogo testirovaniia // Trudy Instituta sistemnogo programmirovaniia RAN. 2022. T. 34. Vyp. 1. S. 7—22. DOI: 10.15514/ISPRAS-2022-34(1)-1.
6. Pozin B.A., Tsiperman G.N. Proslezhivaemost' trebovani kak osnova proektirovaniia funktsional'no-logicheskoi arkhitektury programnoi sistemy // Trudy Instituta sistemnogo programmirovaniia RAN. 2022. T. 34. Vyp. 1. S. 23—34. DOI: 10.15514/ISPRAS-2022-34(1)-2.
7. Shishin K.A., Murav'ev I.V., Kulikov E.K. Ob avtomaticheskoi generatsii modul'nykh testov dlia Java-prilozhenii, ispol'zuiushchikh freimvork Spring // Trudy Instituta sistemnogo programmirovaniia RAN. 2024. T. 36. Vyp. 2. S. 59—72. DOI: 10.15514/ISPRAS-2024-36(2)-5.
8. Kosenkov O., Elahidoost P., Gorschek T., Fischbach J., Mendez D., Unterkalmsteiner M., Fucci D., Mohanani R. Systematic Mapping Study on Requirements Engineering for Regulatory Compliance of Software Systems // Information and Software Technology. 2025. Vol. 178. Art. 107622. DOI: 10.1016/j.infsof.2024.107622.
9. Murugesan A., Wong I., Arias J., Stroud R., Varadarajan S., Salazar E., Gupta G., Bloomfield R., Rushby J. Automating Semantic Analysis of System Assurance Cases Using Goal-Directed ASP // Theory and Practice of Logic Programming. 2024. Vol. 24. No. 4. P. 805—824. DOI: 10.1017/S1471068424000425.
10. Kamoi R., Zhang Y., Zhang N., Han J., Zhang R. When Can LLMs Actually Correct Their Own Mistakes? A Critical Survey of Self-Correction of LLMs // Transactions of the Association for Computational Linguistics. 2024. Vol. 12. P. 1417—1440. DOI: 10.1162/tacl\_a\_00713.



# ЦИФРОВОЙ АВАТАР ПРЕПОДАВАТЕЛЯ КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Зуева А.С.<sup>1</sup>

**Ключевые слова:** высшее образование, генеративные нейронные сети, запись голоса человека, интеллектуальная собственность, изображение лица человека, искусственный интеллект, образовательные технологии, персональные данные, правовой режим.

## Аннотация

**Цель работы:** определение правовой природы цифрового аватара преподавателя и выявление особенностей его использования в образовательной деятельности.

**Метод исследования.** Исследование выполнено с использованием формально-юридического, системного и структурно-функционального методов. Проведен анализ российского законодательства в сфере интеллектуальной собственности, персональных данных, информации и образования, а также научных публикаций, посвященных применению технологий искусственного интеллекта в образовательной деятельности. Применен комплексный подход, позволяющий рассматривать цифровой аватар преподавателя как совокупность взаимосвязанных объектов правовой охраны и цифровых технологий. Практические выводы проверены в ходе апробации авторской образовательной технологии «Лекторий-фест искусственного интеллекта».

**Результаты:** предложено авторское определение цифрового аватара преподавателя как комплексного цифрового объекта, объединяющего результаты интеллектуальной деятельности, технологии искусственного интеллекта, изображение лица человека, запись голоса и образовательный контент преподавателя. Разработана авторская модель структуры цифрового аватара преподавателя, определены основные элементы его правового режима и основания применения норм гражданского, информационного и образовательного законодательства. Апробация разработанной технологии «Лекторий-фест искусственного интеллекта» показала возможность использования цифрового аватара при организации образовательного процесса в юридическом вузе с соблюдением требований законодательства об интеллектуальной собственности и персональных данных. Полученные результаты могут быть использованы при совершенствовании законодательства Российской Федерации, разработке локальных нормативных актов образовательных организаций и формировании правовых механизмов ответственного применения технологий искусственного интеллекта в системе высшего образования.

DOI: 10.24412/1994-1404-2026-3-219-227

## Введение

Развитие технологий искусственного интеллекта оказывает существенное влияние на образовательную деятельность, формируя новые модели взаимодействия участников образовательного процесса и создавая ранее неизвестные объекты цифровой среды. Одним из таких объектов становятся цифровые аватары, представляющие собой созданные с использованием технологий искусственного интеллекта цифровые образы человека, способные воспроизводить его внешний облик, голос, манеру речи и профессиональные знания.

Особое распространение данное явление получает в сфере высшего образования, где цифровые аватары начинают использоваться в качестве инструмента создания образовательного контента, проведения занятий, консультирования обучающихся и популяризации научных знаний. Современные технологии позволяют создавать цифровые аватары преподавателей на основе видеозаписей, голосовых образцов и научных публикаций, что открывает новые возможности для персонализации обучения и масштабирования образовательных ресурсов.

<sup>1</sup> Зуева Анна Сергеевна, кандидат экономических наук, доцент, доцент кафедры компьютерного права и информационной безопасности Высшей школы государственного аудита МГУ им. М.В. Ломоносова, г. Москва, Россия. ORCID: 0000-0003-4703-6679.

E-mail: zueva@audit.msu.ru

Вместе с тем использование цифровых аватаров преподавателей в образовательной деятельности формирует общественные отношения, правовая квалификация которых вызывает ряд вопросов. Они связаны с определением правовой природы цифрового аватара, использованием изображения и голоса преподавателя, обработкой его персональных данных, использованием результатов интеллектуальной деятельности при создании аватара, а также определением правового режима генерируемого образовательного контента.

Следует отметить, что российское законодательство не содержит специального правового режима цифрового аватара как самостоятельного объекта правового регулирования. В связи с этим при определении правового режима цифровых аватаров возникает необходимость применения совокупности норм гражданского законодательства, законодательства о персональных данных, законодательства об информации, информационных технологиях и защите информации, а также законодательства в сфере образования.

В настоящем исследовании понятия «цифровой аватар» и «цифровой двойник» разграничиваются. Цифровой двойник предполагает создание цифрового аватара объекта, воспроизводящей его характеристики, состояние или поведение и используемой для моделирования соответствующих свойств оригинала. Цифровой аватар человека имеет иную функциональную направленность и представляет собой цифровую репрезентацию отдельных индивидуализирующих признаков конкретного лица. Такой аватар может воспроизводить внешность, голос, особенности коммуникации и профессиональный контент человека, не являясь при этом его исчерпывающей цифровой копией. В рассматриваемой образовательной технологии воспроизводятся отдельные индивидуализирующие и профессиональные характеристики преподавателя, поэтому для обозначения исследуемого объекта используется понятие «цифровой аватар преподавателя».

Цель исследования состоит в разработке авторского подхода к определению понятия цифрового аватара преподавателя, выявлении его структурных элементов, определении особенностей правового режима и оценке возможностей применения в системе юридического образования.

Для достижения поставленной цели решаются следующие задачи:

- определить место цифрового аватара преподавателя в системе объектов правового регулирования;
- исследовать соотношение прав на изображение лица, запись голоса, научные публикации преподавателя и результаты работы систем искусственного интеллекта;
- проанализировать практический опыт применения цифровых аватаров преподавателей в рамках авторской образовательной технологии «Лекторий-фест искусственного интеллекта»;

– сформулировать предложения по совершенствованию правового регулирования использования цифровых аватаров в образовательной деятельности.

Объектом исследования являются общественные отношения, возникающие при использовании технологий искусственного интеллекта в образовательной деятельности.

Предмет исследования включает правовое регулирование создания и использования цифровых аватаров преподавателей в образовательном процессе.

Научный интерес к вопросам правового регулирования искусственного интеллекта, цифровых аватаров и генеративных технологий в последние годы существенно возрос.

В современной юридической литературе активно исследуются вопросы правового регулирования искусственного интеллекта, цифровой трансформации общественных отношений, обработки персональных данных и охраны результатов интеллектуальной деятельности. Т.Я. Хабриева в своих публикациях затрагивает вопросы правовой идентификации искусственного интеллекта и формирования новых правовых режимов цифровых технологий [1]. Ю.М. Батурин поднимает дискуссионный вопрос: является ли искусственный интеллект объектом или субъектом права [2]. А.В. Морозов раскрывает Кибернетические и организационно-правовые аспекты создания систем искусственного интеллекта [3]. В.В. Белозеров изучает проблемы правового регулирования ИИ и пробелы законодательства [4]. А.Б. Сливицкий, Б.А. Сливицкий описали системный анализ правового регулирования технологий искусственного интеллекта [5]. Иванов В.В., Нестеров А.Ю., Янченко И.П. исследуют использование генеративного ИИ в высшем образовании и поднимают вопросы авторского права, академической этики и правового регулирования [6]. Атабеков А.Р. провел сравнительно-правовой анализ применения цифрового аватара в образовательной деятельности [7].

В мировой научной литературе цифровые образовательные аватары рассматриваются как перспективный инструмент персонализации обучения, однако вопросы их правового регулирования исследованы значительно меньше, чем педагогические возможности их использования [8–10]. Немецкие ученые из Мюнхенского университета М. Финк, С. Робинсон, Б. Эртль [11] рассматривают образовательные аватары как новый инструмент обучения и анализируют преимущества и риски их использования.

В целом большинство исследований посвящено правовому регулированию искусственного интеллекта в целом, вопросам обработки персональных данных и использования генеративных технологий. При этом правовой режим цифрового аватара преподавателя как комплексного цифрового объекта образовательной среды практически не исследован, что обуславливает научную новизну настоящей работы.



В научной литературе обращается внимание и на отсутствие сформировавшейся практики использования цифровых аватаров в образовательной деятельности. Так, А.Р. Атабеков, анализируя правовое регулирование цифровых аватаров в Российской Федерации, США и КНР, со ссылкой на данные Аналитического центра при Правительстве Российской Федерации отмечает, что на момент проведения исследования (август 2025 года) технологии цифровых аватаров фактически не применялись в образовательном процессе [7].

С учетом вышеизложенного научная новизна характеризуется следующими положениями:

1) Впервые описан правовой режим цифрового аватара преподавателя, основанный на практическом применении данной технологии в образовательной деятельности;

2) Предложена трехэлементная структура цифрового аватара преподавателя, включающая: персональные данные и иные сведения, используемые для воспроизведения индивидуализирующих признаков преподавателя; научно-образовательный контент; алгоритмический компонент искусственного интеллекта. Обоснована необходимость дифференцированной правовой квалификации этих элементов в зависимости от характера и цели их использования.

3) На основании апробации авторской образовательной технологии «Лекторий-фест искусственного интеллекта» выявлены практические правовые риски использования цифровых аватаров в образовательном процессе.

4) Сформулированы рекомендации по правовому оформлению создания цифровых аватаров преподавателей в вузах.

Эмпирическую основу настоящего исследования составили результаты апробации авторской образовательной технологии «Лекторий-фест искусственного интеллекта», разработанной и внедренной в образовательный процесс кафедры компьютерного права и информационной безопасности Высшей школы государственного аудита МГУ имени М.В. Ломоносова в октябре 2025 года. Технология предусматривает создание обучающимися цифровых аватаров преподавателей с использованием генеративного искусственного интеллекта на основе его научных публикаций. Реализация проекта позволила смоделировать полный цикл создания и использования цифрового аватара преподавателя, начиная от получения исходных данных и заканчивая его генерацией. Это создало условия для выявления особенностей правового режима цифрового аватара преподавателя, определения состава возникающих правоотношений.

### Понятие и содержание цифрового аватара преподавателя

Практическая апробация цифрового аватара преподавателя показала, что в образовательной деятельности он воспринимается участниками образователь-

ного процесса как единый цифровой объект. Вместе с тем его создание требует последовательного использования различных объектов правовой охраны, обладающих самостоятельным правовым режимом. Именно это обстоятельство обуславливает необходимость дальнейшего анализа структуры цифрового аватара как комплексного объекта электронной образовательной среды.

В настоящем исследовании под цифровым аватаром преподавателя предлагается понимать созданный с использованием технологий искусственного интеллекта комплексный цифровой объект, воспроизводящий индивидуализирующие признаки преподавателя (внешность, голос, манеру речи, профессиональные знания и особенности педагогического взаимодействия) на основе обработки персональных данных, результатов интеллектуальной деятельности преподавателя и иных информационных технологий, предназначенный для использования в образовательной, научной и иной профессиональной деятельности.

Исследование правовой природы цифрового аватара преподавателя целесообразно осуществлять посредством структурного анализа составляющих его элементов, для чего следует определить состав возникающих правоотношений, установить пределы применения различных отраслей законодательства и выявить правовые риски использования технологий искусственного интеллекта в образовательной деятельности.

Для выявления отличительных признаков цифрового аватара преподавателя следует сопоставить его с наиболее распространенными электронными образовательными продуктами, используемыми в образовательной деятельности (табл. 1).

В отличие от традиционных электронных образовательных продуктов цифровой аватар преподавателя сочетает признаки объекта интеллектуальной собственности, средства индивидуализации личности и инструмента генеративного искусственного интеллекта (рис. 1).

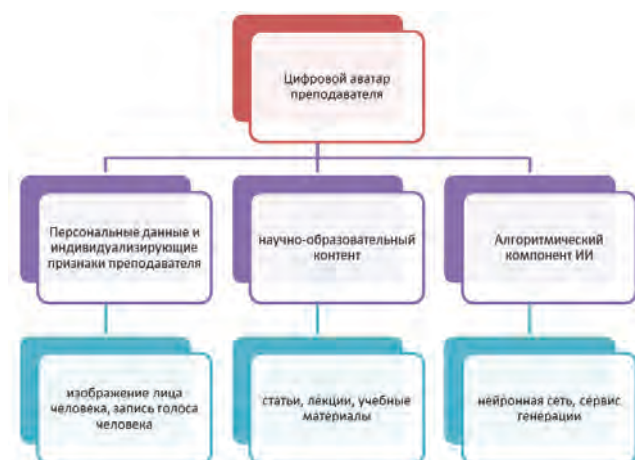


Рис. 1. Структура цифрового аватара преподавателя (авторская модель)

Соотношение цифрового аватара преподавателя с иными цифровыми объектами

| № | КРИТЕРИЙ                           | ВИДЕО ЛЕКЦИИ | ОНЛАЙН-КУРС | ЧАТ-БОТ  | ЦИФРОВОЙ АВАТАР ПРЕПОДАВАТЕЛЯ |
|---|------------------------------------|--------------|-------------|----------|-------------------------------|
| 1 | Изображение преподавателя          | +            | +           | -        | +                             |
| 2 | Голос преподавателя                | +            | +           | -        | +                             |
| 3 | Возможна генерация нового контента | -            | -           | +        | +                             |
| 4 | Используется ИИ                    | -            | -           | +        | +                             |
| 5 | Имитация личности преподавателя    | -            | -           | частично | +                             |

Модель включает три взаимосвязанных элемента: персональные данные и иные сведения, используемые для воспроизведения индивидуализирующих признаков преподавателя; научно-образовательный контент, алгоритмический компонент искусственного интеллекта. Каждый из них обладает самостоятельным правовым режимом, что свидетельствует о комплексном характере цифрового аватара и невозможности его регулирования в рамках одного правового института. Данная структура положена в основу дальнейшего анализа правового режима каждого из элементов цифрового аватара преподавателя.

#### **«Лекторий-фест искусственного интеллекта» как пример использования цифровых аватаров преподавателей в образовательной деятельности**

Практическое значение для внедрения цифрового аватара преподавателя в процесс обучения студентов-юристов имеет модель образовательной технологии «Лекторий-фест искусственного интеллекта». Суть данной технологии сводится к созданию обучающимися цифровых аватаров преподавателей с использованием технологий генеративного искусственного интеллекта. В процессе выполнения практического задания студенты не только осваивают современные ИИ-инструменты, но и анализируют правовые аспекты создания и использования цифровых аватаров, включая вопросы защиты персональных данных, интеллектуальной собственности и соблюдения требований законодательства при применении технологий искусственного интеллекта. Такой формат обучения сочетает проектную деятельность, практическое применение цифровых технологий и решение профессиональных юридических задач, обеспечивая формирование как цифровых, так и профильных компетенций будущих специалистов.

Особенность данной технологии заключается в том, что цифровой аватар преподавателя выступает одновременно объектом изучения, инструментом обучения и предметом правового анализа.

В рамках реализации технологии обучающиеся создают цифровые аватары преподавателей кафедры

на основе его видеозаписи и научных публикаций. Работа организуется в несколько этапов и предполагает не только освоение технологий искусственного интеллекта, но и проведение правовой оценки всех действий, связанных с созданием и использованием цифрового аватара.

На подготовительном этапе особое внимание уделяется вопросам правового регулирования обработки персональных данных, использования изображений граждан и соблюдения законодательства об интеллектуальной собственности. Студенты изучают правовые требования, предъявляемые к использованию фото-, видео- и аудио, а также анализируют возможные риски, возникающие при создании цифровых аватаров человека.

На основном этапе обучающиеся делают видеозапись преподавателя, создают цифровой образ преподавателя, формируют голосовую модель и генерируют образовательный контент на основе научных публикаций преподавателя. При этом обязательным элементом работы является анализ правомерности использования каждого вида данных и определение круга субъектов, обладающих правами на создаваемый цифровой продукт.

Реализация проекта показала, что наибольшие дискуссии вызывают следующие вопросы.

1. Пределы использования изображения и голоса преподавателя для последующего создания цифровой модели. Формально согласие на видеосъемку не всегда означает согласие на создание цифрового аватара, способного самостоятельно воспроизводить внешний облик и голос человека.

2. Использование научных публикаций преподавателя в качестве источника данных для генерации образовательного контента. В зависимости от условий опубликования произведений и характера предоставленных прав возникает необходимость оценки допустимости их использования для обучения систем искусственного интеллекта и создания производного контента.

3. Определение правового режима образовательного продукта, созданного с использованием технологий искусственного интеллекта. В рассматриваемом

Элементы цифрового аватара преподавателя и их правовой режим

| № | ЭЛЕМЕНТ                                                                                               | ОБЪЕКТ РЕГУЛИРОВАНИЯ                    | НОРМАТИВНАЯ ОСНОВА          |
|---|-------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------|
| 1 | Персональные данные и индивидуализирующие признаки: изображение лица человека, запись голоса человека | нематериальное благо                    | ст. 152.1 ГК РФ             |
|   |                                                                                                       | идентифицирующий признак личности       | ГК РФ, судебная практика    |
|   |                                                                                                       | персональные данные                     | Федеральные законы № 152-ФЗ |
| 2 | Научно-образовательный контент преподавателя: научные статьи, учебные пособия и др.                   | объекты авторских и исключительных прав | часть IV ГК РФ              |
| 3 | Алгоритмический компонент ИИ                                                                          | программа для ЭВМ                       | часть IV ГК РФ              |

случае результат является следствием совместного участия нескольких субъектов: преподавателя как автора научного контента, обучающихся как инициаторов и организаторов процесса создания цифрового аватара, а также разработчиков программного обеспечения, используемого для генерации контента.

Таким образом, образовательная деятельность может выступать эффективной средой для формирования правовой культуры использования технологий искусственного интеллекта. В отличие от абстрактного изучения законодательства обучающиеся сталкиваются с необходимостью практического решения вопросов, связанных с обработкой персональных данных, использованием результатов интеллектуальной деятельности и соблюдением требований информационной безопасности.

Полученный опыт свидетельствует о том, что технологии создания цифровых аватаров обладают значительным образовательным потенциалом, однако их внедрение должно сопровождаться разработкой локальных нормативных механизмов, определяющих порядок получения согласия преподавателей, использования образовательного контента и распределения прав на результаты деятельности, создаваемые с применением искусственного интеллекта. Технология «Лекторий-фест искусственного интеллекта» позволяет рассматривать цифровой аватар преподавателя не только как образовательный инструмент, но и как практическую модель правоотношений, возникающих в условиях цифровой трансформации образовательной среды.

### Правовой режим цифрового аватара преподавателя как комплексного объекта электронной образовательной среды

Предложенная трехэлементная структура цифрового аватара преподавателя предполагает самостоятельное определение правового режима каждого из входящих в нее элементов. Соотношение элементов цифрового аватара и применимых к ним правовых режимов представлено в таблице 2.

Первую группу элементов цифрового аватара преподавателя образуют персональные данные и иные сведения, используемые для воспроизведения его индивидуализирующих признаков. К ним могут относиться изображение, видео- и аудиозаписи, голос и иные сведения, относящиеся к конкретному преподавателю.

При этом необходимо разграничивать персональные данные и биометрические персональные данные. В соответствии со статьей 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»<sup>2</sup> к биометрическим персональным данным относятся сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных. Следовательно, изображение лица или запись голоса не приобретают специальный правовой режим биометрических персональных данных исключительно в силу характера содержащейся в них информации. Для такой квалификации имеет значение цель их обработки и использование соответствующих сведений для установления личности.

В рассматриваемой образовательной технологии изображение и голос преподавателя используются прежде всего для воспроизведения его внешности и голосовых характеристик при создании цифрового аватара, а не для идентификации или аутентификации преподавателя. Поэтому автоматическая квалификация всех используемых фото-, видео- и аудиоматериалов как биометрических персональных данных была бы необоснованной. Вместе с тем при изменении цели и способа обработки, в частности при использовании соответствующих характеристик для установления личности, может возникнуть специальный правовой режим биометрических персональных данных.

Согласно статье 152.1 Гражданского кодекса Российской Федерации обнародование и дальнейшее использование изображения гражданина допускается только с его согласия, за исключением случаев, прямо

<sup>2</sup> Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451.

предусмотренных законом<sup>3</sup>. При создании цифрового аватара происходит не только использование изображения преподавателя, но и его цифровая реконструкция посредством технологий искусственного интеллекта. В результате возникает вопрос о пределах действия согласия на использование изображения и возможности последующего создания производных цифровых образов.

Голос также способен выполнять индивидуализирующую функцию и приобретает особое значение в условиях развития технологий синтеза речи и голосового клонирования. Однако запись голоса, как и изображение человека, не во всех случаях должна квалифицироваться как биометрические персональные данные. Такая квалификация зависит от характера и цели обработки соответствующих сведений. Специальные требования законодательства об использовании биометрических персональных данных подлежат применению в тех случаях, когда голосовые или иные биометрические характеристики используются в предусмотренных законом целях идентификации или аутентификации физического лица.

В ходе реализации образовательной технологии «Лекторий-фест искусственного интеллекта» первоначально предполагалось, что согласия преподавателя на использование фото- и видеоматериалов достаточно для создания цифрового аватара. Проведенный правовой анализ показал необходимость разграничения нескольких юридически значимых действий: осуществления фото-, видео- и аудиозаписи преподавателя, использования его изображения, обработки персональных данных и применения полученных материалов для генерации цифрового образа и синтеза голоса. При этом сам факт использования изображения или записи голоса при создании цифрового аватара не является достаточным основанием для квалификации соответствующих сведений как биометрических персональных данных; такая квалификация определяется целью и способом их обработки.

Вторым элементом цифрового аватара преподавателя является научно-образовательный контент, используемый при обучении искусственной интеллектуальной модели. К нему относятся научные статьи, монографии, учебники, учебные пособия, презентации, видеолекции, методические материалы, тестовые задания, практические кейсы, авторские методики преподавания и иные результаты интеллектуальной деятельности преподавателя.

С правовой точки зрения указанные материалы являются объектами авторского права, правовой режим которых определяется частью четвертой Гражданского кодекса Российской Федерации. В соответствии со статьей 1259 ГК РФ произведения науки, литературы и искусства являются объектами авторских прав независи-

мо от достоинств, назначения и способа их выражения. Исключительное право на такие произведения принадлежит автору либо иному правообладателю в случаях, предусмотренных законом или договором.

Особенностью использования научно-образовательного контента при создании цифрового аватара является то обстоятельство, что соответствующие материалы применяются не только для непосредственного доведения до обучающихся, но и для обучения искусственной интеллектуальной модели, формирования индивидуального стиля объяснения учебного материала, воспроизведения научной терминологии, структуры изложения, логики аргументации и особенностей педагогического взаимодействия конкретного преподавателя. Иными словами, произведения применяются в качестве обучающего массива данных, что выходит за рамки традиционного использования объектов авторского права в образовательном процессе.

В связи с этим возникает вопрос о правовых основаниях использования произведений преподавателя для обучения моделей искусственного интеллекта. Действующее российское законодательство не содержит специальных норм, регулирующих использование объектов авторского права в целях машинного обучения. Следовательно, правомерность включения научно-образовательных материалов в обучающие выборки должна определяться общими положениями гражданского законодательства об использовании результатов интеллектуальной деятельности, а также условиями трудового договора, локальных нормативных актов образовательной организации и соглашений между преподавателем и образовательной организацией.

Дополнительную специфику приобретает ситуация, когда учебные материалы создаются преподавателем в рамках исполнения трудовых обязанностей. В этом случае возникает необходимость разграничения личных неимущественных прав автора и исключительных прав на служебные произведения, принадлежащих работодателю в случаях, предусмотренных статьей 1295 ГК РФ. Однако даже переход исключительных прав к образовательной организации не означает автоматического возникновения права использовать произведения для обучения искусственного интеллекта, поскольку подобный способ использования может требовать специального договорного регулирования с учетом целей обработки произведений и характера создаваемого цифрового аватара.

При создании цифровых аватаров использовались тексты лекций, презентации, научные статьи, методические материалы и иные произведения преподавателей. Практическая апробация показала, что уже на данном этапе возникает необходимость разграничения объектов авторского права, определения объема предоставляемых прав и оценки допустимости использования произведений при обучении модели искусственного интеллекта.

<sup>3</sup> Гражданский кодекс Российской Федерации (часть IV) от 18 декабря 2006 г. № 230-ФЗ // Собрание законодательства РФ. 2006. № 52 (ч. I). Ст. 5496.



Третьим элементом цифрового аватара выступает искусственная интеллектуальная модель, обеспечивающая функционирование цифрового аватара и его взаимодействие с пользователями электронной образовательной среды. Этот элемент объединяет два предыдущих в единую цифровую систему, способную воспроизводить ответы, объяснения, рекомендации и иные формы педагогической коммуникации.

С позиции действующего российского законодательства искусственная интеллектуальная модель не относится к самостоятельным объектам гражданских прав. В зависимости от способа реализации она может рассматриваться как программа для ЭВМ, совокупность программных компонентов либо программно-аппаратный комплекс, правовой режим которых определяется положениями части четвертой Гражданского кодекса Российской Федерации. При этом алгоритмы машинного обучения и параметры нейронной сети сами по себе не изменяют установленного законодательством режима охраны программ для ЭВМ как объектов авторского права.

Вместе с тем правовой режим модели искусственного интеллекта не исчерпывается регулированием интеллектуальной собственности. В образовательной сфере такая модель одновременно выступает элементом информационной системы образовательной организации, осуществляет обработку персональных данных обучающихся, принимает участие в реализации образовательных программ и оказывает влияние на процесс формирования результатов обучения. Следовательно, на ее функционирование распространяются также требования законодательства об информации, персональных данных, образовании, а также законодательства о применении технологий искусственного интеллекта в части обеспечения безопасности, прозрачности и ответственности при эксплуатации соответствующих цифровых решений.

После интеграции подготовленных материалов в генеративную систему искусственного интеллекта возникли вопросы, связанные с определением правового режима создаваемого образовательного контента, распределением ответственности за его содержание, а также допустимыми пределами использования цифрового аватара преподавателя в образовательном процессе.

Таким образом, отсутствие специального регулирования цифровых аватаров обуславливает необходимость применения норм нескольких отраслей права. Межотраслевой подход может обеспечить баланс интересов преподавателя, образовательной организации, обучающихся и разработчиков технологий искусственного интеллекта. Лишь совокупность правовых режимов всех трех элементов предоставляет возможность сформировать целостную правовую конструкцию цифрового аватара преподавателя как комплексного объекта электронной образовательной среды.

## **Выводы**

Апробация трехэлементной структуры цифрового аватара преподавателя в рамках «Лекторий-феста искусственного интеллекта» подтвердила ее применимость к отношениям, возникающим в образовательной деятельности. Именно результаты апробации позволили выявить ряд правовых вопросов, которые ранее практически не анализировались в отечественной юридической литературе ввиду отсутствия соответствующей практики.

Проблема правового режима цифрового аватара преподавателя как элемента электронной образовательной среды недостаточно исследован и требует дальнейшего комплексного анализа научного юридического сообщества ввиду инновационности объекта исследования. Цифровизация образования и развитие технологий искусственного интеллекта приводят к появлению новых объектов цифровой образовательной среды, одним из которых является цифровой аватар преподавателя. Проведенное исследование показало, что данный объект обладает сложной правовой природой и не может быть отнесен исключительно к сфере интеллектуальной собственности, персональных данных или образовательного права.

На примере реализации образовательной технологии «Лекторий-фест искусственного интеллекта» показано, что образовательная деятельность выступает не только сферой применения цифровых аватаров, но и эффективной площадкой для формирования правовой культуры использования технологий искусственного интеллекта. Практика создания цифровых аватаров преподавателей дает возможность обучающимся изучать актуальные вопросы защиты персональных данных, охраны результатов интеллектуальной деятельности и обеспечения информационной безопасности.

Полученные результаты могут быть использованы при совершенствовании локального регулирования в образовательных организациях, разработке методических рекомендаций по применению технологий искусственного интеллекта в образовании и дальнейшем развитии научных исследований в области правовой информатики.

## Литература

1. Хабриева Т.Я. Правовые проблемы идентификации искусственного интеллекта // Вестник Российской академии наук. 2024. Т. 94. № 7. С. 609—622.
2. Батурин Ю.М., Полубинская С.В. Искусственный интеллект: правовой статус или правовой режим? // Государство и право. 2022. № 10. С. 141—154.
3. Морозов А.В. Кибернетические и организационно-правовые аспекты создания систем искусственного интеллекта // Вестник Московского университета. Серия 26. Государственный аудит. 2024. № 3. С. 107—124.
4. Белозерцева В.В. Правовое регулирование искусственного интеллекта // Проблемы в российском законодательстве. 2024. Т. 17. № 6. С. 78—86.
5. Сливицкий А.Б., Сливицкий Б.А. Анализ системы правового регулирования бытия технологий искусственного интеллекта // Управление наукой: теория и практика. 2024. Т. 6. № 2. С. 53—61.
6. Иванов В.В., Нестеров А.Ю., Янченко И.П. Этические и правовые аспекты применения технологий генеративного искусственного интеллекта при подготовке квалификационных и научных работ // Вестник Самарского университета. История, педагогика, филология. 2024. Т. 30. № 4. С. 23—32. DOI: 10.18287/2542-0445-2024-30-4-23-32.
7. Атабеков А.Р. Правовое регулирование цифровых аватаров в публичной и образовательной деятельности: сравнительно-правовое исследование регулирования в РФ, США и КНР // Вестник Московской академии Следственного комитета Российской Федерации. 2025. № 3 (45). С. 130—139. DOI: 10.54217/2588-0136.2025.45.3.017.
8. Ehsan Latifa, Gengchen Maie, Matthew Nyaabaa, Xuansheng Wub, Ninghao Liub, Guoyu Lua, Sheng Lid, Tianming Liua, Xiaoming Zhaia. AGI: Artificial General Intelligence for Education // arXiv:2304.12479v5 [cs.AI] 13 Mar 2024. URL: <https://arxiv.org/abs/2304.12479>
9. Chan C.K.Y., Tsi L.H.Y. The AI Revolution in Education: Will AI Replace or Assist Teachers in Higher Education? arXiv:2305.01185 (cs) [Submitted on 2 May 2023] URL: <https://arxiv.org/abs/2305.01185>
10. Porayska-Pomsta K., Holmes W., Nemorin S. The Ethics of AI in Education // arXiv:2406.11842 (cs) [Submitted on 22 Mar 2024] URL: <https://arxiv.org/abs/2406.11842>
11. Fink M., Robinson S., Ertl B. AI-based avatars are changing the way we learn and teach: benefits and challenges // Front. Educ., 16 July 2024. Sec. Digital Learning Innovations. Volume 9 — 2024. DOI: 10.3389/feduc.2024.1416307.

SECTION:  
REGULATORY INFORMATICS

# DIGITAL AVATAR OF A TEACHER AS AN OBJECT OF LEGAL REGULATION

Zueva A.S.<sup>4</sup>

**Keywords:** higher education, generative neural networks, human voice recording, intellectual property, human face image, artificial intelligence, educational technologies, personal data, legal regime.

## Abstract

**Purpose.** The purpose of the work is to develop the author's approach to defining the concept of a teacher's digital avatar, identify its structural elements, determine the specific features of its legal framework, and substantiate the possibilities of its application in legal education.

**Research methods.** The study employs formal legal, systemic, and structural-functional research methods. Russian legislation governing intellectual property, personal data, information, and education, as well as academic publications on the use of artificial intelligence technologies in education, were analyzed. A comprehensive approach was applied to examine the teacher's digital avatar as an integrated set of interconnected legally protected objects and digital technologies. The practical validity of the findings was confirmed through the implementation of the author's educational technology "AI Lecture Fest".

---

<sup>4</sup> Anna S. Zueva, Ph.D. (Law), Associate Professor at the Department of Computer Law and Information Security, Graduate School of Public Audit, Lomonosov Moscow State University, Moscow, Russia. ORCID: 0000-0003-4703-6679.  
E-mail: [zueva@audit.msu.ru](mailto:zueva@audit.msu.ru)

**Results of the study:** The author's definition of the teacher's digital avatar is proposed as a complex digital object combining the results of intellectual activity, artificial intelligence technologies, an image of a person's face, voice recording and the teacher's educational content. The author's model of the structure of the teacher's digital avatar has been developed, the main elements of his legal regime and the grounds for applying the norms of civil, information and educational legislation have been identified. The testing of the developed technology "Lecture Hall-fest of artificial intelligence" has shown the possibility of using a digital avatar in the organization of the educational process at a law school in compliance with the requirements of legislation on intellectual property and personal data. The results obtained can be used in improving the legislation of the Russian Federation, developing local regulations of educational organizations and forming legal mechanisms for the responsible use of artificial intelligence technologies in the higher education system.

## References

1. Khabrieva T.Ia. Pravovye problemy identifikatsii iskusstvennogo intellekta // Vestnik Rossiiskoi akademii nauk. 2024. T. 94. No. 7. S. 609—622.
2. Baturin Iu.M., Polubinskaia S.V. Iskusstvennyi intellekt: pravovoi status ili pravovoi rezhim? // Gosudarstvo i pravo. 2022. No. 10. S. 141—154.
3. Morozov A.V. Kiberneticheskie i organizatsionno-pravovye aspekty sozdaniia sistem iskusstvennogo intellekta // Vestnik Moskovskogo universiteta. Seriya 26. Gosudarstvennyi audit. 2024. No. 3. S. 107—124.
4. Belozertseva V.V. Pravovoe regulirovanie iskusstvennogo intellekta // Problemy v rossiiskom zakonodatel'stve. 2024. T. 17. No. 6. S. 78—86.
5. Slivitskii A.B., Slivitskii B.A. Analiz sistemy pravovogo regulirovaniia bytiia tekhnologii iskusstvennogo intellekta // Upravlenie nauko: teoriia i praktika. 2024. T. 6. No. 2. S. 53—61.
6. Ivanov V.V., Nesterov A.Iu., Ianchenko I.P. Eticheskie i pravovye aspekty primeneniia tekhnologii generativnogo iskusstvennogo intellekta pri podgotovke kvalifikatsionnykh i nauchnykh rabot // Vestnik Samarskogo universiteta. Istorii, pedagogika, filologiya. 2024. T. 30. No. 4. C. 23—32. DOI: 10.18287/2542-0445-2024-30-4-23-32.
7. Atabekov A.R. Pravovoe regulirovanie tsifrovyykh avatarov v publichnoi i obrazovatel'noi deiatel'nosti: sravnitel'no-pravovoe issledovanie regulirovaniia v RF, SShA i KNR // Vestnik Moskovskoi akademii Sledstvennogo komiteta Rossiiskoi Federatsii. 2025. No. 3 (45). S. 130—139. DOI: 10.54217/2588-0136.2025.45.3.017.
8. Ehsan Latifa, Gengchen Maie, Matthew Nyaabaa, Xuansheng Wub, Ninghao Liub, Guoyu Lua, Sheng Lid, Tianming Liua, Xiaoming Zhaia. AGI: Artificial General Intelligence for Education // arXiv:2304.12479v5 [cs.AI] 13 Mar 2024. URL: <https://arxiv.org/abs/2304.12479>
9. Chan C.K.Y., Tsi L.H.Y. The AI Revolution in Education: Will AI Replace or Assist Teachers in Higher Education? arXiv:2305.01185 (cs) [Submitted on 2 May 2023] URL: <https://arxiv.org/abs/2305.01185>
10. Porayska-Pomsta K., Holmes W., Nemorin S. The Ethics of AI in Education // arXiv:2406.11842 (cs) [Submitted on 22 Mar 2024] URL: <https://arxiv.org/abs/2406.11842>
11. Fink M., Robinson S., Ertl B. AI-based avatars are changing the way we learn and teach: benefits and challenges // Front. Educ., 16 July 2024. Sec. Digital Learning Innovations. Volume 9 — 2024. DOI: 10.3389/feduc.2024.1416307.



# НЕКОММЕРЧЕСКИЕ ОРГАНИЗАЦИИ В ЦИФРОВОЙ МОДЕЛИ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ И ИСПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ

Дубровина М.О.<sup>1</sup>

**Ключевые слова:** цифровизация, модель управления, обязательные требования, договорные обязательства, риски, классификация рисков, внутренний контроль, отчётность, государственный контроль, надзор, НКО.

## Аннотация

**Цель исследования** заключается в разработке цифровой модели управления соблюдением обязательных требований и исполнением договорных обязательств некоммерческой организации. Модель должна обеспечивать систематизацию требований, распределение ответственности, контроль сроков, документальное подтверждение исполнения и риск-ориентированное управление законодательными, договорными, грантовыми, финансовыми, организационными и техническими рисками.

**Методы исследования** включают формально-юридический метод, применённый для анализа нормативных актов, устанавливающих обязанности некоммерческой организации; системный метод — для выявления взаимосвязи правовых, договорных, организационных и цифровых элементов управления соблюдением обязательств; функциональный метод — для разграничения задач ответственных лиц, проверяющих и руководства некоммерческой организации. Риск-ориентированный подход использован для классификации рисков неисполнения требований и обязательств по их содержанию и этапам исполнения.

**Результаты исследования:** предложена цифровая модель управления соблюдением обязательных требований и исполнением договорных обязательств некоммерческой организации. Модель учитывает требования законодательства, условия предоставления грантов и субсидий, а также положения заключённых договоров. В её состав входят реестр требований и обязательств, календарь юридически значимых сроков, перечень ответственных лиц, процедуры подготовки, согласования и проверки документов, фиксация их направления и получения, архив подтверждений исполнения, а также порядок мониторинга и устранения выявленных нарушений.

Разработана двухуровневая классификация рисков. На первом уровне риски подразделяются по содержанию на законодательные, договорные, грантовые, финансовые, организационные и технические. На втором уровне они классифицируются по этапам движения юридически значимой информации: выявлению обязательства, назначению ответственного лица, подготовке и согласованию сведений, подписанию и направлению документов, подтверждению их получения, хранению, мониторингу исполнения, а также исправлению выявленных ошибок.

**Научная новизна исследования** заключается в разработке комплексного риск-ориентированного подхода, обеспечивающего связь каждого требования или обязательства с его нормативным либо договорным основанием, сроком исполнения, ответственным лицом, контрольной процедурой и документальным подтверждением выполнения. В отличие от общего документооборота предложенная цифровая модель охватывает полный цикл исполнения обязанности — от выявления её основания до подтверждения исполнения и устранения выявленных нарушений.

DOI: 10.24412/1994-1404-2026-3-228-239

---

<sup>1</sup> Дубровина Мадина Олеговна, кандидат юридических наук, преподаватель отделения повышения квалификации ФБУ НЦПИ при Минюсте России, г. Москва, Россия.  
E-mail: [madina.dubrovina@scli.ru](mailto:madina.dubrovina@scli.ru)



## **Введение**

**Н**екоммерческие организации (НКО) осуществляют деятельность в условиях широкого применения информационных систем. В условиях цифровой экономики цифровая трансформация позволяет НКО повышать эффективность работы, экономить временные, финансовые и организационные ресурсы, расширять охват целевой аудитории и совершенствовать взаимодействие с гражданами, донорами и другими организациями [1, с. 89—90].

Одним из ключевых направлений такой трансформации становится развитие электронного взаимодействия НКО с государственными органами. Это особенно важно в связи с необходимостью предоставления отчётности, участия в грантовых конкурсах, получения государственных услуг и реализации социально значимых проектов. В этой связи цифровая трансформация государственного управления предполагает переход к комплексным электронным сервисам, основанным на межведомственном взаимодействии, автоматизированном обмене данными и снижении административной нагрузки [2, с. 312—313]. Для НКО, взаимодействующих с государственными органами, грантодателями и иными публичными субъектами, такие изменения имеют непосредственное практическое значение.

Внедрение цифровых технологий меняет порядок взаимодействия государства, организаций и граждан, одновременно повышая требования к качеству, достоверности и своевременности обработки информации [3, с. 215—216]. Цифровые инструменты используются НКО для коммуникации с гражданами, донорами, что расширяет возможности открытого взаимодействия, однако одновременно требует повышения прозрачности, подотчётности и надёжности информационных процессов [4, с. 27]. Поэтому цифровизация должна сопровождаться проверкой достоверности данных, согласованностью информационных ресурсов, а также процедурами выявления ошибок, коллизий и пробелов в правовом регулировании [5, с. 67—68]. Информационные системы становятся не только техническим средством передачи данных, но и элементом обеспечения юридически значимых действий организации.

Особое значение цифровые инструменты приобретают во взаимодействии НКО с органами государственного контроля. Электронные ресурсы обеспечивают доступ к необходимой информации, автоматизацию отдельных контрольных процедур и обмен сведениями между контролируемыми лицами и контролирующими органами [6, с. 165, 171]. Следовательно, предупреждение нарушений зависит не только от правильной правовой оценки соответствующих действий, но и от того, насколько эффективно в организации организованы учёт требований, контроль сроков, движение документов и фиксация результатов их исполнения.

Для эффективного использования цифровых технологий необходимо учитывать особый правовой статус НКО. Она одновременно выступает юриди-

ческим лицом, участником гражданского оборота, получателем имущества, пожертвований, грантов и субсидий, работодателем и субъектом взаимодействия с государственными органами. Каждая из этих ролей предполагает наличие самостоятельных прав и обязанностей, что обуславливает множественность требований к деятельности организации. При этом надлежащее исполнение обязанностей предполагает не только совершение соответствующих действий, но и возможность документально подтвердить их законность, целевое использование средств и исполнение обязательств перед государством, контрагентами и благополучателями.

Дополнительную сложность создаёт многоуровневый характер регулирования деятельности НКО. Помимо законодательных норм, организация должна учитывать подзаконные акты, локальные документы и договорные предписания [7]. Поэтому до разработки информационной системы необходимо сформировать цифровую модель, в которой требования будут соотносены с конкретными процессами, ответственными лицами, документами, сроками, контрольными процедурами и способами подтверждения исполнения. Такая модель обеспечивает прослеживаемую связь между нормативными предписаниями, организационной деятельностью и архитектурой информационной системы [8, с. 114—115, 120—121].

Вместе с тем использование цифровых технологий не устраняет правовые, договорные и организационные риски, а лишь изменяет формы их проявления. К ним относятся пропуск юридически значимого срока, представление неполного или недостоверного документа, ошибка при идентификации подписанта, нарушение порядка использования электронной подписи, отсутствие подтверждения получения документа и техническая недоступность информационной системы. Дополнительные риски связаны с непрозрачностью принимаемых решений, нарушением режима персональных данных и неопределённостью ответственности за технические ошибки [9, с. 153].

В связи с этим оценка исполнения конкретного требования или обязательства должна основываться не только на содержании соответствующего предписания. Необходимо также учитывать доступность информационной системы, корректность уведомления, наличие у подписанта необходимых полномочий, возможность своевременного исправления ошибки и наличие документально подтверждённых действий НКО. Иными словами, надлежащее исполнение в цифровой среде предполагает одновременный учёт правовых, организационных и технических условий.

Таким образом, цифровая модель управления соблюдением требований и исполнением обязательств должна объединять нормативные и договорные основания деятельности НКО, связанные с ними информационные системы и организационные процессы, распределение ответственности, контроль юридически значимых сроков и документирование результатов

исполнения. Её разработка позволит обеспечить системный, а не фрагментарный подход к предупреждению нарушений и подтверждению надлежащего исполнения обязанностей.

В рамках исследования анализируются нормативные акты, определяющие обязанности НКО и последствия их неисполнения; рассматриваются условия предоставления грантов и положения договоров; классифицируются риски нарушения требований и обязательств с учётом их содержания и этапов исполнения; исследуется значение электронных документов и иных цифровых подтверждений юридически значимых действий; разграничиваются функции ответственных лиц, а также внутреннего и внешнего контроля.

### Информационные основы соблюдения требований и исполнения обязательств НКО

Деятельность НКО регулируется нормами гражданского, бухгалтерского, налогового, трудового и административного законодательства, а также законодательством об электронной подписи, информации, персональных данных, закупках, грантовом финансировании и государственном контроле (надзоре). Основу регулирования составляет Федеральный закон № 7-ФЗ «О некоммерческих организациях»<sup>2</sup> (Закон № 7-ФЗ), однако конкретный объём требований и обязательств зависит от организационно-правовой формы НКО, целей её деятельности, источников финансирования, наличия работников и реализуемых проектов.

Помимо требований законодательства, НКО обязана исполнять обязательства, возникающие из договоров, соглашений о предоставлении грантов и субсидий, документов о целевом финансировании и пожертвованиях. В связи с этим НКО необходима цифровая модель управления соблюдением требований и обязательств. Она должна учитывать особенности правового статуса организации, порядок принятия решений, распределение полномочий между органами управления и ответственными лицами, а также положения Гражданского кодекса Российской Федерации<sup>3</sup> о юридических лицах, компетенции органов управления, представительстве и распоряжении имуществом.

В цифровой модели необходимо закрепить полномочия лиц, принимающих решения, подписывающих документы и представляющих НКО во взаимоотношениях с государственными органами, грантодателями и контрагентами. Это позволяет установить порядок подготовки, проверки, согласования, подписания и хранения документов, а также обеспечить контроль действий уполномоченных лиц.

В соответствии с Федеральным законом № 402-ФЗ «О бухгалтерском учёте»<sup>4</sup> НКО обязана документировать хозяйственные операции, оформлять первичные документы и обеспечивать достоверность отчётности. Необходимость внутреннего контроля финансово-хозяйственной деятельности, проверки бухгалтерского учёта и наличия подтверждающих документов отмечается в научной литературе [10, с. 220—221]. При использовании пожертвований, грантов, субсидий и членских взносов необходимо обеспечивать соответствие расходов источникам финансирования, утверждённому бюджету, целям проекта и условиям договора. Нарушение такого соответствия может повлечь риск признания расходов нецелевыми и невозможность выполнения проекта [10, с. 221—222].

При использовании электронной подписи в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи»<sup>5</sup> НКО должна вести перечень уполномоченных подписантов, контролировать сроки действия сертификатов и полномочия работников, обеспечивать сохранность ключей и своевременно прекращать доступ выбывших сотрудников. Несоблюдение этих требований может привести к неприятию документа, нарушению договорного обязательства или спору о юридической значимости совершённого действия.

Требования Федеральных законов № 152-ФЗ «О персональных данных»<sup>6</sup> и № 149-ФЗ «Об информации, информационных технологиях и о защите информации»<sup>7</sup> должны закрепляться в локальных актах, должностных инструкциях и правилах электронного документооборота. В НКО необходимо определить порядок доступа к сведениям, журналирования действий, резервного копирования, передачи документов и их архивирования.

Отдельное направление цифровой модели связано с взаимодействием НКО с государственными органами. Такое взаимодействие регулируется статьёй 32 Закона № 7-ФЗ и иными нормативными актами о государственном контроле (надзоре)<sup>8</sup>. В современных условиях оно преимущественно осуществляется через цифровые каналы, поэтому регистрация уведомлений, запросов, ответов и подтверждений их получения должна быть включена в единый процесс исполнения обязательств.

<sup>4</sup> Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учёте», статьи 5, 6, 7, 9, 13, 29 // СЗ РФ. 2011. № 50. Ст. 7344.

<sup>5</sup> Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», статьи 2, 5, 6, 9, 10, 17 // СЗ РФ. 2011. № 15. Ст. 2036.

<sup>6</sup> Федеральный закон от 27.07.2006 № 152-ФЗ, статьи 3, 5, 6, 7, 18.1, 19, 21 // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

<sup>7</sup> Федеральный закон от 27.07.2006 № 149-ФЗ, ст. 2, 5, 6, 7, 9, 11, 16 // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

<sup>8</sup> Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» // СЗ РФ. 2008. № 52 (ч. 1). Ст. 6249; Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» // СЗ РФ. 2001. № 33. Ст. 3418; Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // СЗ РФ. 2006. № 19. Ст. 2060 и другие.

<sup>2</sup> Федеральный закон от 12.01.1996 № 7-ФЗ «О некоммерческих организациях» // Собрание законодательства Российской Федерации. 1996. № 3. Ст. 145

<sup>3</sup> Гражданский кодекс Российской Федерации, гл. 4, статьи 48, 50, 52, 53, 65.1, 123.1—123.3 // СЗ РФ. 1994. № 32. Ст. 3301; 1996. № 5. Ст. 410.

НКО следует фиксировать содержание документов, сведения об отправителе, даты получения и ответа, приложения, ответственного сотрудника, результаты проверки и факт направления ответа. Это обеспечивает контроль сроков, прослеживаемость взаимодействия и подтверждение юридически значимых действий.

Для своевременного выявления, исполнения и документального подтверждения требований законодательства, условий грантов и договорных обязательств целесообразно вести реестр обязательных требований и договорных обязательств. В нём следует отражать нормативный или договорный источник, содержание и применимость требования, срок исполнения, ответственное и контролирующее лицо, адресата, форму документа и способ подтверждения результата.

Реестр необходимо связывать с календарём юридически значимых сроков. В него включаются даты представления отчётности, направления ответов, исполнения условий грантов и субсидий, выполнения договорных обязательств, продления документов, а также сдачи кадровой и бухгалтерской отчётности.

Исполнение требований организует руководитель НКО: он принимает управленческие решения, утверждает локальные акты, распределяет полномочия и назначает ответственных лиц. Они обеспечивают подготовку, проверку, подписание и направление документов, а также фиксируют результаты исполнения.

Подтверждением исполнения могут служить приказы, протоколы, доверенности, электронные документы, сведения из личного кабинета, уведомления о доставке, регистрационные номера и метки времени. Однако их доказательственное значение определяется в совокупности с локальными актами, договорами, перепиской, первичными документами и данными о работе информационной системы<sup>9</sup>.

При этом документальное подтверждение исполнения не исключает возможности возникновения ошибок и иных неблагоприятных обстоятельств. На каждом этапе исполнения могут возникать содержательные, процедурные, организационные и технические риски: ошибки в документах, пропуск сроков, несоответствие расходов условиям гранта или договора, отсутствие полномочий у подписанта, нарушение правил обработки персональных данных, сбой информационных систем и утрата подтверждающих материалов. Поэтому риски НКО в цифровой среде следует анализировать с учётом содержания конкретного требования или обязательства и этапа его исполнения.

### **Риски соблюдения требований и исполнения обязательств НКО в цифровой среде**

Риски НКО целесообразно классифицировать по двум взаимосвязанным основаниям: содержанию требования или обязательства и этапу движения юридически значимой информации. Содержательная классификация позволяет определить сферу возникновения риска, тогда как процессуальная — установить конкретный этап исполнения, на котором он возникает, и выбрать соответствующие меры реагирования. Такой подход соответствует риск-ориентированной модели. Риск-ориентированный подход предполагает оценку вероятности нарушения, выделение объектов повышенного риска и дифференциацию профилактических и контрольных мер [11, с. 432—434].

В настоящем исследовании под риском несоблюдения обязательных требований и неисполнения договорных обязательств понимается вероятность наступления неблагоприятных правовых, финансовых, организационных или репутационных последствий вследствие нарушения установленной обязанности, условия грантового финансирования или договорного положения, а также невозможности документально подтвердить их надлежащее исполнение.

С учётом содержания требований и обязательств выделяются законодательные, договорные, грантовые, финансовые, организационные и технические риски. Предлагаемая классификация развивает подход, согласно которому риски НКО подразделяются на операционные, финансовые, регуляторные, репутационные и коррупционные [12, с. 39].

К основным сферам возникновения рисков относятся регистрационные и уведомительные обязанности, представление отчётности, ведение бухгалтерского учёта и налогообложение, целевое использование средств, исполнение условий грантов и субсидий, выполнение договорных обязательств, применение электронной подписи, обработка персональных данных, а также подтверждение и хранение документов. Распределение рисков по указанным сферам представлено в таблице 1.

При этом содержательная классификация не позволяет определить конкретный момент формирования риска и последовательность действий по его предупреждению. Один и тот же риск может возникать на разных этапах исполнения требования или обязательства. Например, несоответствие отчётности может быть связано с ошибкой при подготовке документа, нарушением полномочий подписанта, пропуском срока направления или отсутствием подтверждения его получения.

В связи с этим риски следует оценивать с учётом последовательных этапов исполнения требования или обязательства, включая его выявление и регистрацию, назначение ответственного лица, подготовку и проверку документов, определение полномочий подписанта, подписание и направление документов, получение

<sup>9</sup> Электронная запись подтверждает исполнение обязательства только при возможности установить её содержание, источник, дату, целостность, факт направления или получения и полномочия подписанта. Поэтому электронная подпись, регистрационный номер или метка времени сами по себе не доказывают надлежащее исполнение обязательства.

**Основные риски несоблюдения обязательных требований и неисполнения  
договорных обязательств НКО в цифровой среде**

| ГРУППА РИСКА                                             | ТИПИЧНЫЕ ОШИБКИ                                                                                                                                                                                                                                                                                                                | КЛЮЧЕВЫЕ МЕРЫ ПРЕДУПРЕЖДЕНИЯ                                                                                                                                      |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Регистрационные и уведомительные обязанности НКО</b>  | Непредставление или несвоевременное представление в уполномоченный орган сведений об изменениях, подлежащих государственной регистрации либо уведомлению, в том числе о руководителе, месте нахождения, учредительных документах и иных юридически значимых обстоятельствах; представление неполных или недостоверных сведений | Реестр обязанностей, календарь юридически значимых сроков, проверка документов и хранение подтверждений                                                           |
| <b>Представление отчётности и сведений в Минюст</b>      | Пропуск установленного срока, неполные или недостоверные сведения, несоответствие отчётности фактической деятельности НКО                                                                                                                                                                                                      | Календарь юридически значимых сроков, предварительная проверка полноты и достоверности сведений, контроль приёма документов                                       |
| <b>Бухгалтерский учёт</b>                                | Отсутствие или ненадлежащее оформление первичных учётных документов, ошибки в обязательных реквизитах, несвоевременное отражение хозяйственных операций                                                                                                                                                                        | Электронный архив первичных документов с разграничением доступа, контроль обязательных реквизитов,                                                                |
| <b>Налогообложение</b>                                   | Неправильное определение налоговой базы, непредставление или несвоевременное представление налоговой отчётности, ошибки при исчислении и выплате доходов физическим лицам                                                                                                                                                      | Налоговый календарь, сверка налоговых данных с бухгалтерскими регистрами, проверка выплат работникам и подрядчикам, контроль представления отчётности             |
| <b>Целевое использование средств</b>                     | Расходование средств не в соответствии с уставными целями, условиями договора о предоставлении гранта или субсидии, утверждённой сметой либо финансовым планом; смешение средств разных проектов и источников финансирования; отсутствие документов, подтверждающих целевое использование                                      | Раздельный учёт источников финансирования и проектов; сверка расходов и хранение подтверждающих документов                                                        |
| <b>Договорные обязательства НКО</b>                      | Нарушение условий договоров с грантодателями, партнёрами и получателями благотворительной помощи; несоблюдение сроков и мероприятий благотворительных проектов; отсутствие отчётности и подтверждений передачи помощи                                                                                                          | Реестр договоров, календарь юридически значимых сроков, назначение ответственных лиц, проверка документов, фиксация передачи помощи и архивирование подтверждений |
| <b>Отчётность по грантам и субсидиям</b>                 | Непредставление, неполнота или недостоверность отчёта; несоответствие фактических расходов условиям соглашения, утверждённой смете или финансовому плану                                                                                                                                                                       | Реестр условий финансирования, календарь отчётности, раздельный учёт расходов по проектам и источникам финансирования.                                            |
| <b>Электронная подпись и полномочия</b>                  | Использование недействительного или неактуального сертификата электронной подписи; отсутствие либо прекращение полномочий подписанта; ошибки при идентификации лица                                                                                                                                                            | Реестр сертификатов и доверенностей, контроль сроков и полномочий                                                                                                 |
| <b>Персональные данные</b>                               | Неправомерный доступ, утечка или нарушение правил хранения                                                                                                                                                                                                                                                                     | Разграничение доступа, журналирование, контроль сроков хранения                                                                                                   |
| <b>Подтверждение и хранение доказательств исполнения</b> | Отсутствие подтверждения отправки, доставки или приёма документа либо архива                                                                                                                                                                                                                                                   | Архивирование электронного подтверждения приёма документа уполномоченным органом, протоколов и иных подтверждений                                                 |



**Риски на этапах исполнения обязательных требований  
и договорных обязательств НКО**

| ЭТАП ДВИЖЕНИЯ<br>ИНФОРМАЦИИ                           | ОСНОВНОЙ РИСК                                                                                                            | ВОЗМОЖНОЕ ПОСЛЕДСТВИЕ                                                                     | МЕРА ПРЕДУПРЕЖДЕНИЯ                                                                                                              |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Выявление<br/>требования или<br/>обязательства</b> | Требование, условие гранта<br>или договорное обязательство<br>не установлено в качестве объекта<br>исполнения и контроля | Пропуск срока или нарушение<br>обязательства                                              | Реестр требований, договоров<br>и обязательств; календарь<br>юридически значимых сроков                                          |
| <b>Назначение<br/>ответственного<br/>лица</b>         | Отсутствие или ненадлежащее<br>закрепление ответственности                                                               | Несвоевременное или ненадлежащее<br>исполнение требования или<br>обязательства            | Реестр ответственных лиц;<br>закрепление обязанностей                                                                            |
| <b>Подготовка<br/>документов<br/>для исполнения</b>   | Неполные или недостоверные<br>данные                                                                                     | Представление ошибочной отчётности<br>или документов                                      | Первичная проверка, единые формы<br>данных                                                                                       |
| <b>Согласование</b>                                   | Несогласованность сведений между<br>подразделениями                                                                      | Направление противоречивой<br>информации                                                  | Внутренний порядок согласования                                                                                                  |
| <b>Подписание и<br/>направление</b>                   | Подписание неуполномоченным<br>лицом; пропуск установленного<br>срока                                                    | Непринятие документа, признание<br>обязанности неисполненной,<br>применение санкций       | Проверка сертификата и срока<br>действия ЭП; календарь юридически<br>значимых сроков, автоматические<br>напоминания              |
| <b>Передача файла и<br/>приём документа</b>           | Загрузка неполного или технически<br>некорректного документа;<br>отсутствие подтверждения<br>получения или приёма        | Возврат документа или его<br>непринятие; невозможность доказать<br>исполнение обязанности | Проверка формата, состава<br>и читаемости файла; контроль<br>электронного документа о доставке<br>или приёме и статуса документа |
| <b>Хранение</b>                                       | Утрата документа или цифрового<br>подтверждения                                                                          | Невозможность представить<br>доказательства                                               | Архивирование и резервное<br>копирование                                                                                         |
| <b>Мониторинг</b>                                     | Несвоевременное выявление<br>ошибки                                                                                      | Продолжение нарушения и увеличение<br>его последствий                                     | Регулярная проверка статусов<br>и сроков                                                                                         |
| <b>Исправление</b>                                    | Отсутствие корректирующих<br>действий                                                                                    | Сохранение нарушения или повторное<br>нарушение                                           | Порядок исправления и повторной<br>отправки                                                                                      |

подтверждения их отправки или приёма, а также последующее архивирование документов и подтверждений исполнения. Распределение рисков по указанным этапам представлено в таблице 2.

Данные таблицы 2 показывают, что возникновение риска определяется не только содержанием регулируемой сферы, но и организацией процесса исполнения. Поэтому одно требование или обязательство может быть связано с несколькими рисками, возникающими на разных этапах его реализации. Сочетание содержательной и процессуальной классификаций позволяет соотнести каждую сферу риска с этапом его формирования и соответствующей профилактической мерой.

Однако рассмотренная классификация не отражает субъектный состав и порядок осуществления контроля. Между тем эффективность предупреждения нарушений во многом зависит от распределения контрольных функций между НКО, государственными органами

и иными уполномоченными субъектами. Контроль следует рассматривать не только как проверку уже совершённых действий, но и как информационный механизм обратной связи, обеспечивающий своевременное выявление отклонений. Контрольные процедуры включают получение, обработку и использование информации о фактическом исполнении требований и обязательств [13, с. 175—176].

В связи с этим необходимо разграничить внешний и внутренний контроль. Внешний контроль за соблюдением НКО обязательных требований осуществляют государственные органы и иные уполномоченные субъекты. Он может включать не только проверку совершённых действий, но и применение превентивных мер, направленных на предупреждение нарушений и защиту публичных интересов [14].

Основные направления внешнего контроля, его субъекты и объекты, а также применяемые цифровые инструменты представлены в таблице 3.

## Внешний контроль (надзор) за деятельностью НКО

| НАПРАВЛЕНИЕ КОНТРОЛЯ                                                                   | СУБЪЕКТ КОНТРОЛЯ                                                                                                                                                                | ОБЪЕКТ И СОДЕРЖАНИЕ ПРОВЕРКИ                                                                                                                                                                | ЦИФРОВЫЕ ИНСТРУМЕНТЫ И ПОДТВЕРЖДЕНИЕ                                                                                                                                                               |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Государственная регистрация и уведомительные обязанности</b>                        | Минюст России и его территориальные органы; ФНС России — в части ведения ЕГРЮЛ.                                                                                                 | Достоверность сведений об НКО, её руководителе, месте нахождения и учредительных документах; соблюдение порядка и сроков представления уведомлений и отчётности                             | ЕГРЮЛ; государственные информационные системы; электронная подача документов; электронная подпись; протокол приёма и уведомление о результате рассмотрения                                         |
| <b>Налоговый контроль</b>                                                              | ФНС России и территориальные налоговые органы                                                                                                                                   | Исчисление и уплата налогов и страховых взносов; представление деклараций, расчётов и сведений; выплаты физическим лицам; применение налоговых льгот                                        | Личный кабинет налогоплательщика; системы электронной отчётности; электронные требования налогового органа; квитанции о приёме и извещения                                                         |
| <b>Контроль бухгалтерского учёта и отчётности</b>                                      | ФНС России — в пределах установленной компетенции; органы государственного финансового контроля; аудиторская организация или аудитор — при обязательном или инициативном аудите | Ведение бухгалтерского учёта; наличие и оформление первичных документов; достоверность отчётности; соответствие учётных данных совершённым операциям                                        | Электронная бухгалтерская база; система представления отчётности; электронный архив документов; разграничение доступа; резервное копирование; протоколы сверки                                     |
| <b>Контроль целевого использования грантов и субсидий</b>                              | Грантодатель или организация, предоставившая субсидию; главный распорядитель бюджетных средств; органы государственного финансового контроля — в пределах компетенции           | Соблюдение условий соглашения; соответствие расходов целям, смете и финансовому плану; достижение установленных показателей; своевременность и достоверность отчётности                     | Реестр соглашений и условий финансирования; раздельный аналитический учёт; электронные отчёты; первичные документы; подтверждения направления и приёма отчётности                                  |
| <b>Контроль в сфере персональных данных</b>                                            | Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)                                                                   | Наличие правовых оснований обработки персональных данных; соответствие обработки заявленным целям; соблюдение требований к уведомлению оператора, защите данных и реагированию на инциденты | Реестр операторов персональных данных; электронные уведомления; журналирование доступа; реестр согласий; система управления правами доступа; документы об устранении нарушений                     |
| <b>Контроль исполнения требований, предписаний, запросов и договорных обязательств</b> | Государственный орган, вынесший требование или предписание; грантодатель, благотворитель или иной контрагент — в части договорных обязательств                                  | Соблюдение установленных сроков; полнота представленных документов и пояснений; целевое использование средств; исполнение условий договора; устранение выявленных нарушений                 | Реестр требований, предписаний и договорных обязательств; календарь юридически значимых сроков; личные кабинеты; электронный документооборот; подтверждения отправки, доставки и приёма документов |

Внешний контроль, как правило, реализуется в рамках проводимых контрольных мероприятий и может выявить нарушение уже после истечения срока исполнения обязанности или неисполнения договорного обязательства. Поэтому особое значение имеет предварительный внутренний контроль, направленный на своевременное распределение ответственности, проверку документов и фиксацию исполнения.

Внутренний контроль в НКО включает организационные, финансовые, бухгалтерские, налоговые и информационные процедуры. К ним относятся распределение обязанностей и полномочий, проверка документов и расходов, контроль юридически значимых сроков, соблюдение условий грантовых соглашений и договоров, разграничение доступа к информационным ресурсам, обеспечение сохранности документов и подтверждений их исполнения, а также принятие

Таблица 4

**Внутренний контроль в деятельности НКО**

| НАПРАВЛЕНИЕ КОНТРОЛЯ                                | СУБЪЕКТ КОНТРОЛЯ                                                                    | ОБЪЕКТ И СОДЕРЖАНИЕ ПРОВЕРКИ                                                                                                                                                               | ЦИФРОВЫЕ ИНСТРУМЕНТЫ И ПОДТВЕРЖДЕНИЕ                                                                                                                                   |
|-----------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Организационный контроль</b>                     | Руководитель, уполномоченные работники, коллегиальные органы                        | Распределение обязанностей и полномочий; соблюдение устава и локальных актов; исполнение поручений и решений                                                                               | Электронные поручения; реестр решений; протоколы; подтверждение ознакомления                                                                                           |
| <b>Финансовый контроль</b>                          | Руководитель, бухгалтер, материально ответственное лицо                             | Соответствие расходов уставным целям, смете, финансовому плану и условиям финансирования; наличие подтверждающих документов                                                                | Первичные документы; электронные регистры; реестр платежей; отчёты; результаты сверки                                                                                  |
| <b>Бухгалтерский и налоговый контроль</b>           | Руководитель, бухгалтер, ответственные исполнители                                  | Полнота, достоверность и своевременность бухгалтерского и налогового учёта, отчётности и расчётов                                                                                          | Электронная бухгалтерская база; журналы согласования, версии документов, документы о приёме отчётности                                                                 |
| <b>Контроль грантов, субсидий и пожертвований</b>   | Руководитель, ответственный исполнитель, бухгалтер                                  | Соблюдение условий финансирования; целевое использование средств; своевременность и достоверность отчётности, уведомлений и                                                                | Реестр соглашений и пожертвований; календарь юридически значимых сроков; автоматические напоминания; электронные отчёты; подтверждения направления и приёма документов |
| <b>Информационный и цифровой контроль</b>           | Руководитель, администратор информационных ресурсов, ответственный за защиту данных | Разграничение доступа; сохранность документов и подтверждений исполнения; защита персональных данных; контроль электронных операций                                                        | Журналы операций и доступа; резервное копирование; электронный архив; реестр предоставленных полномочий; документы о согласиях и доступе                               |
| <b>Контроль исполнения договоров и обязательств</b> | Руководитель, ответственный исполнитель, внутренний проверяющий                     | Соблюдение сроков и условий договоров; исполнение обязательств перед грантодателями, партнёрами и получателями благотворительной помощи; выявление нарушений и принятие корректирующих мер | Реестр договоров и обязательств; календарь юридически значимых сроков; акты проверки; план корректирующих мер; документы, подтверждающие устранение нарушения          |

корректирующих мер. Основные направления внутреннего контроля, его субъекты и объекты, а также используемые цифровые инструменты представлены в таблице 4.

Взаимодействие внутреннего и внешнего контроля образует последовательный механизм управления соблюдением требований и исполнением обязательств. Механизм можно определить следующим образом: *выявление требования или обязательства → назначение ответственного лица → подготовка и проверка документов → их подписание и направление → получение подтверждения → внешний контроль или запрос → корректирующие меры → повторная проверка → архивирование и актуализация процедур.*

На каждом из указанных этапов могут возникать риски, связанные с пропуском установленных сроков,

неполнотой или ненадлежащим оформлением документов, отсутствием полномочий у подписанта, неполучением подтверждения доставки или утратой доказательств исполнения.

Выделенные виды рисков, этапы их возникновения, контрольные процедуры и результаты внутреннего и внешнего контроля образуют взаимосвязанную основу цифровой модели управления соблюдением обязательных требований и исполнением договорных обязательств НКО. Такая модель должна обеспечивать не только предупреждение нарушений, но и своевременную фиксацию действий, документов и подтверждений, необходимых для подтверждения надлежащего исполнения требований законодательства, условий грантового финансирования и договорных обязательств.

### Цифровая модель управления соблюдением требований и исполнением обязательств НКО

Цифровая модель управления соблюдением требований и исполнением обязательств НКО должна формироваться с учётом не только возможностей информационной системы, но и нормативно установленных и договорных процессов, ролей, действий, документов, сроков и условий их исполнения. Такой подход обеспечивает связь между нормативными источниками, деятельностью НКО и проектированием информационной системы [8, с. 114—115, 120—121].

Под цифровой моделью понимается организационно-управленческая конструкция, реализуемая с помощью информационной системы. Она применима к требованиям законодательства, условиям соглашений о предоставлении грантов и субсидий, а также обязательствам по договорам с партнёрами, благотворителями и получателями помощи. Модель связывает каждое требование или обязательство с его основанием, содержанием, сроком исполнения, ответственным и замещающим лицами, адресатом, контрольной процедурой и подтверждением исполнения.

Практическую основу модели составляют реестр требований и обязательств, календарь юридически значимых сроков, перечень ответственных лиц, процедура внутренней проверки документов, журнал их направления и получения, электронный архив и порядок принятия корректирующих мер. В реестре также фиксируются запросы, уведомления, требования и предписания государственных органов, грантодателей, аудиторов и иных уполномоченных субъектов. Это позволяет учитывать результаты внешнего контроля при оценке рисков и совершенствовании внутренних процедур.

Внутренний контроль включает проверку содержания и полноты документов, соответствия расходов условиям гранта или договора, соблюдения сроков, наличия необходимых согласований и полномочий у подписанта. Внешний контроль может осуществляться государственными органами, грантодателями, аудиторами и иными уполномоченными лицами в форме проверки документов, направления запросов, мониторинга отчётности, выдачи требований или предписаний. Его результаты подлежат регистрации в информационной системе и используются для оценки рисков, принятия корректирующих мер и актуализации внутренних процедур.

Последовательность взаимодействия элементов модели представлена на рисунке 1. Процесс начинается с выявления и систематизации требования или обязательства, определения срока исполнения, ответственного и замещающего лица, необходимых документов и контрольных процедур. Подготовленные документы проходят внутреннюю проверку на полноту, соответствие установленным условиям и наличие полномочий у подписанта.

При выявлении ошибок или неполноты документы дорабатываются и проверяются повторно. После подписания уполномоченным лицом они направляются адресату — государственному органу, грантодателю, контрагенту или иному получателю. Сведения об отправке, доставке или получении фиксируются в информационной системе.

Если подтверждение исполнения отсутствует либо внутренний или внешний контроль выявляет нарушение, принимаются корректирующие меры: документы дорабатываются, утраченные материалы восстанавливаются, ошибки устраняются, а документы при необходимости направляются повторно. Результаты этих действий также подлежат регистрации.

При подтверждении надлежащего исполнения документы и связанные с ними доказательства помещаются в электронный архив. Затем актуализируются реестр требований и обязательств, календарь юридически значимых сроков и оценка рисков. Подтверждение исполнения должно позволять установить содержание документа, его источник, дату, адресата, факт направления или получения, целостность документа и полномочия подписанта.

Таким образом, цифровая модель имеет циклический характер и обеспечивает не только предупреждение нарушений, но и прослеживаемость действий, документов и решений, включая результаты внешнего контроля и устранение выявленных нарушений. Надёжность модели поддерживается актуализацией нормативных и договорных источников, разграничением доступа, проверкой контрольных данных, резервным копированием и сохранением электронных документов.

### Заключение

Результаты исследования показывают, что соблюдение требований и исполнение обязательств НКО зависят не только от содержания правовых норм, но и от организации движения информации. Нарушение может возникнуть при любом переходе от требования к его документированному исполнению.

Установлено, что классификация рисков по содержанию обязанности должна дополняться их классификацией по этапам движения информации. Это позволяет связать каждый риск с конкретной профилактической мерой, включая проверку сведений, контроль полномочий, согласование документов, фиксацию их направления и резервное хранение.

Показано, что внутренний и внешний контроль имеют разные задачи. Внутренний контроль предупреждает нарушения и обеспечивает исправление недостатков, внешний — оценивает соблюдение требований и исполнение обязательств. Их разграничение позволяет определить ответственность НКО и пределы проверки со стороны уполномоченных субъектов.

Обосновано значение подтверждений отправки, доставки, получения и приёма документов. Они



**АЛГОРИТМ ДОКУМЕНТАЛЬНОГО СОПРОВОЖДЕНИЯ И КОНТРОЛЯ ИСПОЛНЕНИЯ  
ТРЕБОВАНИЙ И ОБЯЗАТЕЛЬСТВ НКО**

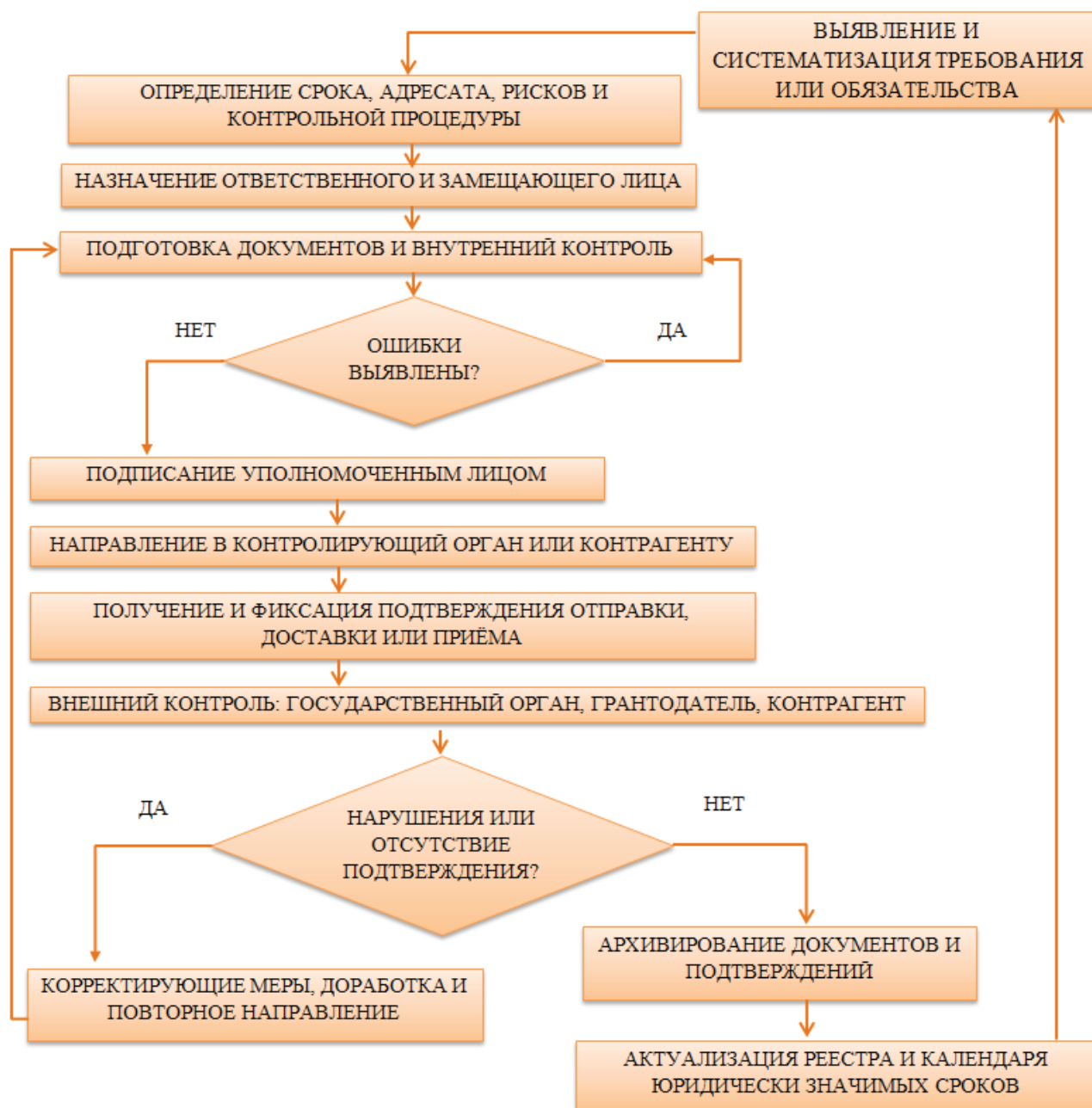


**Рис. 1. Алгоритм документального сопровождения и контроля исполнения требований и обязательств НКО**

являются не только элементами документооборота, но и частью доказательственной базы исполнения требований и обязательств. Поэтому электронный архив должен включать как сами документы, так и сведения об их подписании, направлении, получении и изменении статуса.

Предложенная модель дополняет существующие процедуры внутреннего контроля информационными связями между требованием, ответственным лицом, сроком, документом и подтверждением исполнения.

Её применение может повысить управляемость обязательств и снизить вероятность ошибок, связанных с пропуском сроков, неполнотой сведений и ненадлежащим документированием.

Значение предлагаемой модели состоит в создании организационной и информационной основы для своевременного исполнения требований, выявления недостатков и подтверждения добросовестности действий НКО.

## Литература

1. Дуброва М.В. Трансформация внутренней среды некоммерческих организаций в условиях цифровой экономики // Экономика и управление: проблемы, решения. 2020. Т. 1. № 1. С. 81—90.
2. Матвиенко И.Ю. Преимущества разработки комплексных услуг для Единого портала государственных и муниципальных услуг: технологические и правовые аспекты // Правовая информатика. 2026. № 1. С. 312—320. DOI: 10.24412/1994-1404-2026-1-00-35.
3. Полякова Т.А., Троян Н.А. Трансформация государственного управления в Российской Федерации: от кибернетики, информатики к цифровизации // Правовая информатика. 2025. № 4. С. 215—226. DOI: 10.24412/1994-1404-2025-4-215-226
4. Морозова О.С., Постникова О.Ю. Некоммерческие организации и цифровая трансформация: формирование новых форм гражданского участия // Социально-политические исследования. 2026. № 1 (30). С. 26—39. DOI: 10.20323/2658-428X-2026-1-30-26
5. Токолов А.В. Применение технологий искусственного интеллекта в деятельности Минюста России // Правовая информатика. 2025. № 2. С. 66—71. DOI: 10.24412/1994-1404-2025-2-66-71.
6. Дубровина М.О. Информатизация контрольно-надзорной деятельности в России: оценка информационных систем на прозрачность и доступность информации // Правовая информатика. 2025. № 3. С. 164—173. DOI: 10.24412/1994-1404-2025-3-00-17
7. Кашанина Т.В. Система права: вертикальный срез // Правовая информатика. 2026. № 2. С. 234—244. DOI: 10.24412/1994-1404-2026-2-234-244 .
8. Шелестович О.А. Метод идентификации процессов деятельности при создании информационных систем // Правовая информатика. 2026. № 2. С. 114—126. DOI: 10.24412/1994-1404-2026-2-114-126.
9. Багинский В.Д. Правовая природа и специфика реализации искусственного интеллекта в российской судебной системе // Правовая информатика. 2026. № 1. С. 153—160. DOI: 10.24412/1994-1404-2026-1-00-16
10. Тимофеева М.В. Планирование аудита финансовых ресурсов в некоммерческой организации // Экономика и бизнес: теория и практика. 2022. № 7 (89). С. 219—223. DOI:10.24412/2411-0450-2022-7-219-223
11. Данилова К.Н. Риск-ориентированный подход в государственном лесном надзоре: проблемы нормативного закрепления и совершенствования системы индикаторов риска // Правовая информатика. 2026. № 1. С. 432—440 DOI: 10.24412/1994-1404-2026-2-432-440
12. Климошенко М.И., Билиходзе А.К., Парушина Н.В. Развитие риск-ориентированного управления в некоммерческих организациях // Фундаментальные исследования. 2020. № 8. С. 35—39.
13. Запольский С.В. Об информационно-правовой природе контроля в экономике // Правовая информатика. 2024. № 3. С. 174—179. DOI: 10.24682/1994-1404-2024-3-174-179
14. Запольский С.В. О пределах применения и основаниях административного принуждения // Правовая информатика. 2025. № 2. С. 42—46

SECTION:  
REGULATORY INFORMATICS

# NON-PROFIT ORGANIZATIONS WITHIN A DIGITAL MODEL FOR COMPLIANCE WITH REQUIREMENTS AND THE PERFORMANCE OF OBLIGATIONS

Dubrovina M.O.<sup>10</sup>

**Keywords:** digitalization, management model, mandatory requirements, contractual obligations, risks, risk classification, internal control, reporting, state control, supervision, non-profit organizations.

## Abstract

**Purpose of work** is to develop a digital management model for ensuring compliance with mandatory requirements and the fulfilment of contractual obligations by a non-profit organization. The model is intended to systematize requirements,

<sup>10</sup> **Madina O. Dubrovina**, Ph.D. (Law), Lecturer at the Professional Development Department of the Federal Budgetary Institution "Scientific Center for Legal Information under the Ministry of Justice of Russia," Moscow, Russia.  
E-mail: [madina.dubrovina@scli.ru](mailto:madina.dubrovina@scli.ru)

*allocate responsibilities, monitor deadlines, provide documentary evidence of compliance, and support the risk-based management of legal, contractual, grant-related, financial, organizational, and technical risks.*

**Research methods** include the formal legal method, applied to the analysis of regulations establishing the obligations of non-profit organizations; the systems method, used to identify the interrelationships among the legal, contractual, organizational, and digital elements of compliance management; and the functional method, employed to distinguish the responsibilities of designated officers, reviewers, and the management of a non-profit organization. A risk-based approach was used to classify the risks associated with the non-fulfilment of requirements and obligations according to their substance and stages of implementation.

**Results of the study** include a digital management model for ensuring compliance with mandatory requirements and the fulfilment of contractual obligations by a non-profit organization. The model takes into account statutory requirements, the conditions governing the provision of grants and subsidies, and the provisions of concluded agreements. It includes a register of requirements and obligations, a calendar of legally significant deadlines, a list of responsible persons, procedures for preparing, approving, and reviewing documents, records confirming their submission and receipt, an archive of evidence of compliance, and procedures for monitoring and remedying identified violations.

A two-level risk classification has been developed. At the first level, risks are divided according to their substance into legal, contractual, grant-related, financial, organizational, and technical risks. At the second level, they are classified according to the stages of the movement of legally significant information: identifying an obligation, appointing a responsible person, preparing and approving information, signing and submitting documents, confirming their receipt, storing records, monitoring fulfilment, and correcting identified errors.

**The scientific novelty of the study** lies in the development of an integrated risk-based approach that links each requirement or obligation to its statutory or contractual basis, deadline, responsible person, control procedure, and documentary evidence of fulfilment. Unlike general document management, the proposed digital model covers the entire obligation-fulfilment cycle — from identifying the basis of an obligation to confirming its fulfilment and remedying identified violations.

## References

1. Dubrova M.V. Transformatsiya vnutrenney sredy nekommercheskikh organizatsiy v usloviyakh tsifrovoy ekonomiki // *Ekonomika i upravlenie: problemy, resheniya*. 2020. Vol. 1. № 1. P. 81—90.
2. Matvienko I.Yu. Preimushchestva razrabotki kompleksnykh uslug dlya Edinogo portala gosudarstvennykh i munitsipalnykh uslug: tekhnologicheskie i pravovye aspekty // *Pravovaya informatika*. 2026. № 1. P. 312—320. DOI: 10.24412/1994-1404-2026-1-00-35.
3. Polyakova T.A., Troyan N.A. Transformatsiya gosudarstvennogo upravleniya v Rossiyskoy Federatsii: ot kibernetiki, informatiki k tsifrovizatsii // *Pravovaya informatika*. 2025. № 4. P. 215—226. DOI: 10.24412/1994-1404-2025-4-215-226.
4. Morozova O.S., Postnikova O.Yu. Nekommercheskie organizatsii i tsifrovaya transformatsiya: formirovaniye novykh form grazhdanskogo uchastiya // *Sotsialno-politicheskie issledovaniya*. 2026. № 1 (30). P. 26—39. DOI: 10.20323/2658-428X-2026-1-30-26.
5. Tokolov A.V. Primeneniye tekhnologiy iskusstvennogo intellekta v deyatel'nosti Minyusta Rossii // *Pravovaya informatika*. 2025. № 2. P. 66—71. DOI: 10.24412/1994-1404-2025-2-66-71.
6. Dubrovina M.O. Informatizatsiya kontrol'no-nadzorno-y deyatel'nosti v Rossii: otsenka informatsionnykh sistem na prozrachnost i dostupnost informatsii // *Pravovaya informatika*. 2025. № 3. P. 164—173. DOI: 10.24412/1994-1404-2025-3-00-17.
7. Kashanina T.V. Sistema prava: vertikal'nyy srez // *Pravovaya informatika*. 2026. № 2. P. 234—244. DOI: 10.24412/1994-1404-2026-2-234-244.
8. Shelestovich O.A. Metod identifikatsii protsessov deyatel'nosti pri sozdaniy informatsionnykh sistem // *Pravovaya informatika*. 2026. № 2. P. 114—126. DOI: 10.24412/1994-1404-2026-2-114-126.
9. Baginskiy V.D. Pravovaya priroda i spetsifika realizatsii iskusstvennogo intellekta v rossiyskoy sudebnoy sisteme // *Pravovaya informatika*. 2026. № 1. P. 153—160. DOI: 10.24412/1994-1404-2026-1-00-16.
10. Timofeeva M.V. Planirovaniye audita finansovykh resursov v nekommercheskoy organizatsii // *Ekonomika i biznes: teoriya i praktika*. 2022. № 7 (89). P. 219—223. DOI: 10.24412/2411-0450-2022-7-219-223.
11. Danilova K.N. Risk-orientirovanny podkhod v gosudarstvennom lesnom nadzore: problemy normativnogo zakrepleniya i sovershenstvovaniya sistemy indikatorov riska // *Pravovaya informatika*. 2026. № 1. P. 432—440. DOI: 10.24412/1994-1404-2026-2-432-440.
12. Klimoshenko M.I., Bilikhodze A.K., Parushina N.V. Razvitiye risk-orientirovannogo upravleniya v nekommercheskikh organizatsiyakh // *Fundamentalnye issledovaniya*. 2020. № 8. P. 35—39.
13. Zapolskiy S.V. Ob informatsionno-pravovoy prirode kontrolya v ekonomike // *Pravovaya informatika*. 2024. № 3. P. 174—179. DOI: 10.24682/1994-1404-2024-3-174-179.
14. Zapolskiy S.V. O predelakh primeneniya i osnovaniyakh administrativnogo prinuzhdeniya // *Pravovaya informatika*. 2025. № 2. P. 42—46.



# ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММ ФИЗИЧЕСКОЙ ПОДГОТОВКИ КУРСАНТОВ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МЧС РОССИИ

Кокшаров Е.В.<sup>1</sup>, Гареев Д.Р.<sup>2</sup>

**Ключевые слова:** цифровой мониторинг, персональные данные, информационно-правовое обеспечение, формирование профессиональных компетенций, обработка информации, цифровые технологии, информационный контур, контрольные нормативы, информационные ресурсы.

## Аннотация

**Цель статьи:** теоретическое обоснование модели информационно-правового обеспечения программ физической подготовки курсантов вузов МЧС России, а также правовые режимы обрабатываемых сведений.

**Метод исследования:** системно-структурный анализ нормативно-правовых актов, научной литературы, связанной с образовательной деятельностью, обработкой персональных данных и применением цифровых технологий.

**Результаты исследования:** уточнено содержание информационно-правового обеспечения применительно к программам физической подготовки, а также определены риски неправомерной обработки, искажения и избыточного использования данных. Предложена модель, включающая нормативно-целевой, организационный, информационно-процессный, технологический и контрольно-аналитический уровни. В качестве основы распределения прав доступа предложено использовать функциональный подход: объем доступной информации и перечень разрешенных действий должны соответствовать обязанностям конкретного работника. При этом полномочия по внесению первичных данных, подтверждению результатов, исправлению технических ошибок и контролю соблюдения процедур необходимо закреплять отдельно, обеспечивая возможность установить участников и последовательность каждого изменения. Обоснована целесообразность разграничения педагогического и медицинского информационных контуров. Для организации занятий преподавателю необходимы прежде всего сведения о допуске курсанта, ограничениях при выполнении упражнений и допустимой нагрузке.

**Практическая ценность:** предложенная модель позволяет повысить достоверность результатов контроля, обеспечить защиту сведений о состоянии здоровья и сформировать доказуемую связь между утвержденными нормативами, электронными записями и принимаемыми образовательными решениями.

DOI: 10.24412/1994-1404-2026-3-240-247

## Введение

Цифровизация образовательной деятельности не ограничивается заменой бумажных журналов и ведомостей электронными аналогами. Она предполагает внедрение систем управления обучением, инструментов видеофиксации, мобильных приложений и носимых устройств. Использование таких решений постепенно меняет порядок планирования занятий, учета достигнутых результатов и оценки качества подготовки обучающихся. Следовательно, информационные технологии становятся полноценным элементом образо-

вательного процесса, а не только средством выполнения отдельных организационных задач [1].

В образовательных организациях МЧС России особого внимания требует информационное сопровождение физической подготовки курсантов. Получаемые в ходе занятий показатели позволяют оценивать степень освоения соответствующего раздела образовательной программы, динамику развития профессионально значимых физических качеств и готовность обучающихся действовать в условиях высоких

<sup>1</sup> Кокшаров Евгений Владимирович, доцент, доцент кафедры физической культуры и спорта Уральского института ГПС МЧС России, г. Екатеринбург, Российская Федерация.

E-mail: sheff.patriot@yandex.ru

<sup>2</sup> Гареев Дмитрий Ринатович, кандидат педагогических наук, доцент, доцент кафедры физической культуры, Уральский государственный медицинский университет, г. Екатеринбург, Российская Федерация.

E-mail: dimagario@yandex.ru



## **Основная часть**

нагрузок [2]. Вместе с тем цифровой учет результатов предполагает обработку значительного объема чувствительной информации. К ней относятся персональные данные курсантов, сведения о состоянии их здоровья и посещаемости, результаты выполнения контрольных нормативов, а также информация, на основании которой принимаются решения о допуске к отдельным видам занятий.

Правовое регулирование данной сферы имеет комплексный характер. Оно включает положения законодательства об образовании, физической культуре и спорте, информации, персональных данных и использовании электронной подписи. Общие правовые нормы конкретизируются в федеральных государственных образовательных стандартах, ведомственных документах, основных профессиональных образовательных программах и локальных нормативных актах образовательной организации. Поэтому порядок цифровой фиксации результатов физической подготовки должен определяться с учетом требований всех перечисленных уровней регулирования.

На практике развитие цифровых средств учета нередко происходит быстрее, чем формирование необходимых организационных и правовых процедур. Например, электронные таблицы, мобильные приложения или носимые устройства могут использоваться без четкого определения перечня собираемых данных, продолжительности их хранения и круга лиц, имеющих к ним доступ. Не всегда регламентируются порядок корректировки ошибочных сведений, способы подтверждения достоверности электронной записи и ответственность работников, участвующих в обработке информации. Такая неопределенность повышает риск нарушения требований к защите персональных данных, использования недостоверных показателей при оценивании курсантов и возникновения споров относительно происхождения зафиксированных результатов.

Таким образом, информационное сопровождение физической подготовки курсантов целесообразно рассматривать как самостоятельную составляющую образовательной системы [3, 4]. Его эффективная организация требует согласованного применения технических, организационных и правовых средств. Цифровые инструменты должны внедряться одновременно с установлением правил сбора, проверки, хранения и использования данных, а также с закреплением ответственности лиц, участвующих в соответствующих информационных процессах [5]. Многие исследователи информационного права отмечают, что цифровая трансформация требует не только технологического обновления, но и формирования правовых моделей, обеспечивающих прозрачность цифровых процессов и защищенность участников соответствующих отношений<sup>3</sup>.

Под информационно-правовым обеспечением программ физической подготовки предлагается понимать согласованную совокупность правовых норм, локальных актов, информационных ресурсов, цифровых технологий и контрольных процедур, обеспечивающих законное и достоверное формирование, обработку, использование, хранение и уничтожение сведений, связанных с планированием, проведением и оценкой занятий.

По мнению А.П. Стовбура, Д.Б. Коврижина, А.Н. Крутого, информационное обеспечение представляет собой специально организованную работу с информационными ресурсами, направленную на предоставление военнослужащим необходимых сведений и обеспечение эффективного решения задач физической подготовки [6].

А.Л. Славко, И.А. Корышев отмечают, что профессиональная подготовка курсантов должна основываться на взаимосвязи правовой и физической составляющих, поскольку содержание физической подготовки и формирование профессиональных компетенций осуществляются в рамках нормативно установленной служебной деятельности [7]. При реализации программ физической подготовки информационно-правовое обеспечение позволяет упорядочить нормативно значимую информацию, довести ее до участников образовательного процесса и использовать в учебной работе.

Информационно-правовое обеспечение представляет собой совокупность принципов, а также инструментов и средств правового регулирования [8]. Кроме того, оно предполагает не только защиту сведений от неправомерного доступа, но и установление правил работы с ними на всех этапах: от определения целей сбора до завершения хранения. В его основу следует положить законность обработки и ясность ее целей. Состав собираемых сведений должен ограничиваться тем, что необходимо для решения поставленных задач, а доступ к ним — соответствовать должностным полномочиям работников. Важны также достоверность результатов обработки, возможность их проверки и отслеживания изменений в электронных записях. Отдельного внимания требуют сроки хранения сведений, совместимость информационных систем и доступность информации для уполномоченных пользователей. При этом применение автоматизированных средств не должно исключать контроль со стороны ответственного работника. Юридически значимые решения недопустимо принимать исключительно на основе алгоритма, принципы работы которого непрозрачны.

<sup>3</sup> Медведева Л.В. Система информационного обеспечения подготовки младшего командного состава в ВУЗе МЧС России / Л.В. Медведева, А.С. Евдокимов, А.С. Константинова // Традиции и инновации

в образовании : сб. ст. юбилейной XX Межд. науч.-практ. конф. Посвящается 85-летию ЛОИРО, Санкт-Петербург, 30 марта 2017 г. / Научные редакторы О.В. Ковальчук, В.П. Панасюк, А.Е. Марон. СПб. : Ленинградский областной институт развития образования, 2017. С. 299—305. EDN: ZGBOKX.

Основные категории информации, используемой в процессе физической подготовки

| КАТЕГОРИЯ ИНФОРМАЦИИ                        | ПРИМЕРЫ СВЕДЕНИЙ                                                               | ПРАВОВОЙ РЕЖИМ                                                                    | ОСНОВНЫЕ ТРЕБОВАНИЯ                                                                              |
|---------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>Идентификационные сведения</b>           | Ф.И.О., номер учебной группы, идентификатор пользователя                       | Персональные данные                                                               | Ограничение состава полей, идентификация пользователя, защита от несанкционированного доступа    |
| <b>Сведения об образовательном процессе</b> | Расписание, посещаемость, выполненная нагрузка, темы занятий                   | Персональные данные и документы образовательного учёта                            | Указание источника записи, даты и ответственного лица                                            |
| <b>Результаты контроля</b>                  | Время, расстояние, количество повторений, номер попытки, оценка                | Юридически значимая образовательная информация                                    | Единицы измерения, версия норматива, подтверждение результата, порядок исправления и обжалования |
| <b>Сведения о состоянии здоровья</b>        | Допуск, ограничения, противопоказания, результаты медицинского контроля        | Специальная категория персональных данных                                         | Обособленный доступ, минимизация раскрываемых сведений, повышенные меры защиты                   |
| <b>Телеметрические показатели</b>           | Частота сердечных сокращений, продолжительность нагрузки, маршруты перемещения | Персональные данные; в отдельных случаях сведения о здоровье                      | Обоснование необходимости, точность устройств, ограничение геолокации и сроков хранения          |
| <b>Фото- и видеоматериалы</b>               | Видеозапись выполнения упражнения, фотографии с занятий                        | Персональные данные; при использовании для установления личности — биометрические | Определение цели фиксации, круга пользователей, срока хранения и порядка удаления                |
| <b>Аналитические массивы</b>                | Средние показатели группы, динамика результатов, распределение нагрузок        | Обезличенные либо персональные данные в зависимости от способа формирования       | Предотвращение повторной идентификации, использование минимально необходимой детализации         |

В процессе реализации программ физической подготовки формируются различные категории информации (табл. 1). Правовой режим данных определяется не названием используемого устройства или системы, а содержанием сведений, целью их обработки и возможностью соотнесения с конкретным человеком.

Сведения о состоянии здоровья требуют особого режима обработки и в основном необходима при работе со студентами, которые обучаются в вузах МЧС России. В отличие от них, курсанты при поступлении в образовательную организацию проходят военно-врачебную комиссию и положительное заключение получают в случае отличного состояния здоровья (категория здоровья А). Преподавателю в большинстве случаев не требуется медицинская документация или диагноз, а необходима функциональная информация о допуске и допустимых ограничениях. Передача минимального набора сведений соответствует принципу ограничения обработки заранее установленной целью.

Показатели носимых устройств также не должны автоматически рассматриваться как обычные технические данные. Если они характеризуют физиологическое состояние конкретного курсанта, их обработка требует правовой и организационной защиты, соответствующей фактическому содержанию информации.

Для научной работы и подготовки отчетов предпочтительно использовать агрегированные или обезличенные массивы. При этом небольшая численность группы, сочетание пола, возраста, подразделения и индивидуальных результатов может позволить повторно установить личность. Обезличивание должно оцениваться не формально, а с учетом реального риска идентификации [9].

Информационно-правовое обеспечение должно формироваться как иерархическая система. Федеральное законодательство закрепляет общие права, обязанности и ограничения, а локальное регулирование переводит их в конкретные алгоритмы действий работников и пользователей информационной системы [10].

На этой основе предлагается пятиуровневая модель информационно-правового обеспечения программ физической подготовки курсантов. Под уровнем модели понимается взаимосвязанная совокупность правовых, организационных, информационных и технологических решений, направленных на обеспечение правомерности обработки сведений, достоверности результатов контроля и обоснованности принимаемых образовательных решений.

**Уровни модели информационно-правового обеспечения программ физической подготовки**

| УРОВЕНЬ                  | ОСНОВНОЕ СОДЕРЖАНИЕ                                                                                                                                                                                               | ДОКУМЕНТИРУЕМЫЙ РЕЗУЛЬТАТ                                                                                                              |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Нормативно-целевой       | Определение целей обработки информации, состава необходимых сведений, правовых оснований, допустимых способов использования и границ автоматизации                                                                | Перечень целей обработки; реестр категорий данных; локальные нормативные акты; перечень применяемых нормативов и их версий             |
| Организационный          | Распределение полномочий и ответственности между руководителями подразделений, преподавателями, медицинскими работниками, администраторами информационных систем и работниками, обеспечивающими защиту информации | Матрица доступа; перечень ответственных лиц; порядок взаимодействия подразделений; программа инструктажа работников                    |
| Информационно-процессный | Регламентация получения, проверки, регистрации, изменения, передачи, использования, архивирования и уничтожения сведений                                                                                          | Карта движения данных; формы первичных записей; порядок исправления ошибок; сроки хранения и уничтожения информации                    |
| Технологический          | Реализация установленных требований средствами информационных систем, электронных журналов, устройств регистрации и программ аналитической обработки                                                              | Настроенные права доступа; журналы событий; резервное копирование; контроль целостности; фиксация источника и времени получения данных |
| Контрольно-аналитический | Проверка правомерности цифровых процедур, качества информационных ресурсов и обоснованности сформированных оценок                                                                                                 | Результаты внутреннего контроля; система показателей; перечень выявленных нарушений; план корректирующих мероприятий                   |

Нормативно-целевой уровень определяет границы всей системы. Его формирование целесообразно начинать не с выбора программного обеспечения или технического устройства, а с установления конкретных образовательных и управленческих целей. Для каждого элемента данных должны быть определены цель получения, источник, перечень операций, круг пользователей, срок хранения и порядок прекращения обработки. Если необходимость использования отдельного показателя не может быть обоснована задачами образовательной деятельности, контроля физической подготовленности или обеспечения безопасности занятий, такой показатель не должен включаться в информационный ресурс.

Отдельного учета требуют версии нормативов физической подготовки. Результат курсанта должен соотноситься именно с тем нормативом и той методикой оценки, которые действовали на момент выполнения упражнения. Изменение нормативных требований не должно приводить к автоматическому пересчету ранее полученных результатов без установленного основания. Поэтому в электронной записи необходимо сохранять не только итоговую оценку, но и обозначение упражнения, версию норматива, дату его применения и алгоритм перевода первичного результата в оценочный показатель.

На организационном уровне осуществляется распределение полномочий. Образовательная организация определяет работников, которые вправе вносить первичные данные, подтверждать результаты, исправлять технические ошибки, получать аналитические отчеты и контролировать соблюдение установленных процедур. Доступ следует предоставлять исходя из

выполняемой функции, а не только из принадлежности работника к определенному подразделению.

Педагогический и медицинский информационные контуры целесообразно разграничивать. Преподавателю физической подготовки, как правило, необходимы сведения о возможности участия курсанта в занятиях, наличии ограничений и допустимом уровне нагрузки. Передача подробных сведений о диагнозе или результатах медицинского обследования допустима только при наличии обоснованной необходимости. В электронном журнале в большинстве случаев достаточно отражать функциональное решение: «допущен», «допущен с ограничениями» или «не допущен», а содержание медицинских документов хранить в информационном контуре с более узким кругом пользователей.

Информационно-процессный уровень охватывает весь жизненный цикл сведений: от получения первичного результата до архивирования или уничтожения записи. Он предусматривает проверку корректности измерения, идентификацию курсанта, регистрацию данных, расчет оценки и подтверждение результата уполномоченным работником. При необходимости в запись вносятся исправления, после чего сведения используются в текущем и итоговом контроле. Для каждого этапа необходимо определить исполнителя, срок выполнения и документируемый результат.

Корректировка электронного журнала должна сохранять возможность восстановления истории записи. Наряду с первоначальным и новым значениями следует фиксировать дату и основание изменения, а также сведения о работнике, подтвердившем исправление. Это позволяет отличать устранение технической ошибки

Риски обработки информации и меры их ограничения

| РИСК                                                 | ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ                                                                                      | МЕРЫ ОГРАНИЧЕНИЯ                                                                                                      |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Избыточный сбор показателей                          | Формирование подробного профиля курсанта, не связанного непосредственно с образовательной целью            | Реестр целей обработки; периодическая проверка состава полей; отключение необязательных функций устройств             |
| Объединение медицинских и учебных сведений           | Получение преподавателями и администраторами излишней информации о состоянии здоровья                      | Разделение информационных контуров; передача минимально необходимого медицинского заключения; отдельные права доступа |
| Использование общих учетных записей                  | Невозможность установить автора записи или изменения                                                       | Индивидуальная аутентификация; запрет передачи учетных данных; ведение журналов событий                               |
| Бесследное изменение результата                      | Искажение сведений и снижение достоверности контроля                                                       | Версионность записей; фиксация причины, даты и автора изменения; подтверждение корректировки                          |
| Ошибка измерительного устройства или передачи данных | Неправильная оценка уровня физической подготовленности                                                     | Контроль исправности; проверка единиц измерения и синхронизации; подтверждение результата преподавателем              |
| Вторичное использование сведений                     | Использование данных для целей, не определенных при их сборе; повторная идентификация в научных материалах | Отдельная оценка новой цели; агрегирование и обезличивание; исключение публикации малых выборок                       |
| Непрозрачная оценочная аналитика                     | Невозможность объяснить причину сформированной оценки или рекомендации                                     | Документирование алгоритма и его версии; сохранение исходных показателей; проверка решения уполномоченным работником  |
| Неограниченное хранение                              | Увеличение вероятности неправомерного доступа и использования устаревших данных                            | Установление сроков хранения; периодический пересмотр информационных массивов; документирование уничтожения           |
| Недоступность информационной системы                 | Нарушение порядка проведения контроля и утрата результатов                                                 | Резервное копирование; проверка восстановления; временная процедура автономной фиксации результатов                   |

от регистрации повторного выполнения упражнения или пересмотра результата по обращению курсанта.

Технологический уровень обеспечивает реализацию правовых и организационных требований средствами информационной системы. Его основу составляют индивидуальная идентификация пользователей, ролевое разграничение доступа, регистрация событий и времени операций, сохранение истории изменений, резервное копирование, контроль целостности и восстановление данных. Общие учетные записи преподавателей и администраторов затрудняют установление лица, совершившего конкретное действие, и тем самым снижают доказательственное значение электронных записей.

При поступлении результатов от носимых устройств или автоматизированных измерительных комплексов необходимо фиксировать источник показателя и условия его получения. Электронная запись должна включать тип или идентификатор устройства, дату и время измерения, вид упражнения, единицу измерения, способ передачи данных и результат проверки уполномоченным работником. Если полученный показатель

непосредственно влияет на оценку, требуется также контролировать исправность оборудования, корректность синхронизации и соответствие алгоритма расчета утвержденной методике.

Контрольно-аналитический уровень направлен на выявление ошибок, нарушений и необоснованных отклонений. Аналитические инструменты позволяют отслеживать динамику результатов, обнаруживать аномальные значения и несоответствия между первичными данными и итоговой оценкой, определять необходимость дополнительной проверки. Однако выводы автоматизированной обработки должны служить основанием для такой проверки, а не подменять решение преподавателя или аттестационного органа.

Особое значение в предлагаемой модели приобретает непрерывная связь между утвержденным нормативом, условиями выполнения упражнения, первичным результатом, проверенной электронной записью, оценкой и образовательным решением. Для каждого решения необходимо сохранять возможность установить примененный норматив, условия выполнения упражнения, способ получения результата, лицо,



подтвердившее его корректность, и порядок расчета оценки. Отсутствие любого из этих элементов снижает проверяемость результата и затрудняет разрешение спорных ситуаций.

Использование электронных журналов, мобильных приложений, носимых устройств и автоматизированных аналитических модулей связано с рядом рисков, которые представлены в таблице 3.

Практическое внедрение модели целесообразно организовать поэтапно. Сначала необходимо установить, какие средства используются для регистрации результатов: электронные журналы, информационные системы, носимые устройства, таблицы и другие инструменты. На основе этой инвентаризации составляется карта данных, в которой для каждого показателя определяются цель обработки, источник получения, круг пользователей и срок хранения. Далее разрабатываются или уточняются локальные нормативные акты, распределяются права доступа и закрепляется порядок исправления электронных записей. После этого выполняется настройка технических средств и проверяется полнота регистрации операций с данными. Следующий этап включает обучение работников и апробацию установленных процедур. Завершает внедрение внутренний контроль, позволяющий оценить работу модели по предложенным показателям, выявить недостатки и определить меры по их устранению.

Модель не привязана к конкретному программному обеспечению или оборудованию. Ее требования могут применяться при использовании разных электронных журналов, платформ дистанционного обучения и носимых устройств. Благодаря этому замена технических средств не требует пересмотра базовых правил работы с информацией. Выбор и настройка системы должны опираться на установленные требования к обработке данных, а не определять эти требования исходя лишь из доступных функций.

### **Заключение**

Проведенный анализ позволил конкретизировать понятие информационно-правового обеспечения программ физической подготовки курсантов вузов МЧС России. Оно объединяет взаимосвязанные меры правового, организационного, информационно-процессного, технологического и контрольного характера. Эти меры распространяются на весь жизненный цикл сведений — начиная с определения целей их получения и заканчивая прекращением хранения и уничтожением с документальным подтверждением. Предложенная пятиуровневая модель обеспечивает согласование требований законодательства и локального регулирования с фактическими процедурами регистрации и оценки результатов.

### **Литература**

1. Цифровая трансформация образования: от изменения средств к развитию деятельности / П.Д. Рабинович, К.Е. Заведенский, М.Э. Кушнир [и др.] // Информатика и образование. 2020. № 5 (314). С. 4—14. DOI: 10.32517/0234-0453-2020-35-5-4-14. EDN: OUUEQK.
2. Кокшаров Е.В. Адаптация курсантов вузов МЧС России к высоким физическим нагрузкам // Россия и мировое сообщество: проблемы демографии, экологии и здоровья населения : сб. ст. VII Межд. науч.-практ. конф., Пенза, 15—16 июля 2024 г. Пенза: Пензенский государственный аграрный университет, 2024. С. 103—106. EDN: MZGIF.
3. Карапузиков А.А., Мураев Н.П. Роль информационного обеспечения в системе подготовки курсантов вузов МЧС России // Вестник Уфимского юридического института МВД России. 2025. № 2 (108). С. 168—174. EDN: JYIMGA.
4. Силкин Н.Н. Использование информационных технологий в физическом воспитании курсантов и слушателей средствами физической подготовки / Н.Н. Силкин, А.А. Вяткин, Г.А.Ю. Романова // Актуальные проблемы и направления цифровой трансформации образования : мат. Всерос. науч.-практ. конф., Псков, 23—24 ноября 2021 г. Псков: Псковский государственный университет, 2021. С. 186—192. EDN: VRYGFP.
5. Кокшаров Е.В. Цифровые технологии в системе физической подготовки курсантов вузов МЧС России: Актуальность, проблематика и направления исследования // Правовая информатика. 2026. № 1. С. 167—174. DOI: 10.24412/1994-1404-2026-1-00-18. EDN: IGGOBV.
6. Стовбур А.П., Коврижин Д.Б., Крутой А.Н. Информационное обеспечение физической подготовки военнослужащих // Физическая культура. Спорт. Туризм. Двигательная рекреация. 2019. Т. 4. № 4. С. 49—54. DOI: 10.24411/2500-0365-2019-14408.
7. Славко А.Л., Корышев И.А. Правовая и физическая составляющие профессиональной подготовки курсантов образовательных организаций МВД России // Психология и педагогика служебной деятельности. 2022. № 1. С. 152—155. DOI: 10.24412/2658-638X-2022-1-152-155. EDN: BHVMVT.
8. Ефремов А.А. Информационно-правовое обеспечение достижения национальных целей развития Российской Федерации: вызовы и перспективы // Актуальные проблемы российского права. 2026;21(6):69-79. DOI: 10.17803/1994-1471.2026.187.6.069-079.

9. Мищенко Е.Ю., Соколов А.Н. Алгоритмы реализации методов обезличивания персональных данных в распределенных информационных системах // Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22. № 1. С. 66—70. DOI: 10.21293/1818-0442-2019-22-1-7-66-70. EDN: QMMSYL.
10. Троян Н.А. Информационно-правовое обеспечение развития национальной системы правовой информации в Российской Федерации в условиях цифровой трансформации // Мониторинг правоприменения. 2020. № 4 (37). С. 28—32. DOI: 10.21681/2226-0692-2020-4-28-32. EDN: APNWF.

SECTION:  
REGULATORY INFORMATICS

## INFORMATION AND LEGAL SUPPORT FOR PHYSICAL TRAINING PROGRAMS FOR CADETS IN EDUCATIONAL ORGANIZATIONS OF THE EMERCOM OF RUSSIA

Koksharov E.V.<sup>4</sup>, Gareev D.R.<sup>5</sup>

**Keywords:** digital monitoring, personal data, information and legal support, development of professional competencies, information processing, digital technologies, information framework, performance standards, information resources.

### Abstract

**Purpose of work:** to provide a theoretical rationale for a model of information and legal support for physical training programs for cadets at higher education institutions of the Ministry of Emergency Situations of Russia, as well as to define the legal regimes governing the information processed.

**Research method:** a systems and structural analysis of regulatory legal acts and academic literature related to educational activities, personal data processing, and the use of digital technologies.

**Results of the study:** The content of information and legal support in relation to physical training programs has been clarified, and the risks of unlawful processing, distortion, and excessive use of data have been identified. A model comprising regulatory and target-oriented, organizational, information-process, technological, and control-analytical levels has been proposed. A functional approach is suggested as the basis for allocating access rights: the scope of accessible information and the list of permitted actions should correspond to the duties of a particular employee. The powers to enter primary data, verify results, correct technical errors, and monitor compliance with procedures should be assigned separately, ensuring the possibility of identifying the participants and sequence of each modification. The expediency of differentiating educational and medical information frameworks has been substantiated. For organizing classes, instructors primarily need information on a cadet's authorization to participate, restrictions on performing exercises, and permissible workload.

**Practical value:** The proposed model makes it possible to improve the reliability of assessment results, ensure the protection of health-related information, and establish a verifiable link between approved standards, electronic records, and educational decisions.

### References

1. Tsifrovaia transformatsiia obrazovaniia: ot izmeneniia sredstv k razvitiu deiatel'nosti / P.D. Rabinovich, K.E. Zavedenskii, M.E. Kushnir [i dr.] // Informatika i obrazovanie. 2020. No. 5 (314). S. 4—14. DOI: 10.32517/0234-0453-2020-35-5-4-14. EDN: OUUEQK.
2. Koksharov E.V. Adaptatsiia kursantov vuzov MChS Rossii k vysokim fizicheskim nagruzkam // Rossiia i mirovoe soobshchestvo: problemy demografii, ekologii i zdorov'ia naseleniia : sb. st. VII Mezhd. nauch.-prakt. konf., Penza, 15—16 iulia 2024 g. Penza: Penzenskii gosudarstvennyi agrarnyi universitet, 2024. S. 103—106. EDN: MZGIFF.

<sup>4</sup> **Evgeny V. Koksharov**, Associate Professor of the Department of Physical Education and Sports, Ural Institute of the State Fire Service of the Ministry of Emergency Situations of Russia, Ekaterinburg, Russian Federation.

E-mail: [sheff.patriot@yandex.ru](mailto:sheff.patriot@yandex.ru)

<sup>5</sup> **Dmitry R. Gareev**, Ph.D. (Pedagogy), Associate Professor of the Department of Physical Education, Ural State Medical University, Ekaterinburg, Russian Federation.

E-mail: [dimagario@yandex.ru](mailto:dimagario@yandex.ru)

3. Karapuzikov A.A., Muraev N.P. Rol' informatsionnogo obespecheniia v sisteme podgotovki kursantov vuzov MChS Rossii // Vestnik Ufimskogo iuridicheskogo instituta MVD Rossii. 2025. No. 2 (108). S. 168—174. EDN: JYIMGA.
4. Silkin N.N. Ispol'zovanie informatsionnykh tekhnologii v fizicheskom vospitanii kursantov i slushatelei sredstvami fizicheskoi podgotovki / N.N. Silkin, A.A. Viatkin, G.a.lu. Romanova // Aktual'nye problemy i napravleniia tsifrovoi transformatsii obrazovaniia : mat. Vseros. nauch.-prakt. konf., Pskov, 23—24 noiabria 2021 g. Pskov: Pskovskii gosudarstvennyi universitet, 2021. S. 186—192. EDN: VRYGFP.
5. Koksharov E.V. Tsifrovye tekhnologii v sisteme fizicheskoi podgotovki kursantov vuzov MChS Rossii: Aktual'nost', problematika i napravleniia issledovaniia // Pravovaia informatika. 2026. No. 1. S. 167—174. DOI: 10.24412/1994-1404-2026-1-00-18. EDN: IGGGBV.
6. Stovbur A.P., Kovrizhin D.B., Krutoi A.N. Informatsionnoe obespechenie fizicheskoi podgotovki voennosluzhashchikh // Fizicheskaiia kul'tura. Sport. Turizm. Dvigatel'naia rekreatsiia. 2019. T. 4. No. 4. S. 49—54. DOI: 10.24411/2500-0365-2019-14408.
7. Slavko A.L., Koryshev I.A. Pravovaia i fizicheskaiia sostavliaiushchie professional'noi podgotovki kursantov obrazovatel'nykh organizatsii MVD Rossii // Psikhologiiia i pedagogika sluzhebnoi deiatel'nosti. 2022. No. 1. S. 152—155. DOI: 10.24412/2658-638X-2022-1-152-155. EDN: BHVMVT.
8. Efremov A.A. Informatsionno-pravovoe obespechenie dostizheniia natsional'nykh tselei razvitiia Rossiiskoi Federatsii: vyzovy i perspektivy // Aktual'nye problemy rossiiskogo prava. 2026;21(6):69-79. DOI: 10.17803/1994-1471.2026.187.6.069-079.
9. Mishchenko E.lu., Sokolov A.N. Algoritmy realizatsii metodov obezlichivaniia personal'nykh dannykh v raspredelennykh informatsionnykh sistemakh // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki. 2019. T. 22. No. 1. S. 66—70. DOI: 10.21293/1818-0442-2019-22-1-7-66-70. EDN: QMMSYL.
10. Troian N.A. Informatsionno-pravovoe obespechenie razvitiia natsional'noi sistemy pravovoi informatsii v Rossiiskoi Federatsii v usloviakh tsifrovoi transformatsii // Monitoring pravoprimeneniia. 2020. No. 4 (37). S. 28—32. DOI: 10.21681/2226-0692-2020-4-28-32. EDN: APNWYF.



# НОРМАТИВНО-ОРИЕНТИРОВАННЫЙ МЕТОД ОБОСНОВАНИЯ РЕШЕНИЙ ОБ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ДЕЯТЕЛЬНОСТИ

Свиштунов А.В.<sup>1</sup>

**Ключевые слова:** регулятивная информатика, системный анализ, нормативно обусловленные процессы, анализ нормативного поля, целевая процессная модель, существующие информационные системы, реконструкция состояния автоматизации, согласование процессов и информационных систем, уровни доказательности, прослеживаемость требований.

## Аннотация

**Цель исследования.** Разработать нормативно-ориентированный метод обоснования решений об автоматизации нормативно обусловленных процессов деятельности в существующем контуре информационных систем, в котором целевой процесс и ограничения автоматизации формируются независимо от действующих ИС, а сложившееся состояние реконструируется по их функциям.

**Используемые методы.** Применены анализ нормативного поля и процессный анализ, нормализация и процессная интерпретация функций существующих информационных систем, сопоставление значимых элементов целевого и сложившегося состояний, а также раздельная фиксация степени подтвержденности каждого вывода и результата его проверки относительно целевого правила. Использованы правила выявления и разрешения противоречивых свидетельств и логической агрегации частных результатов.

**Результаты исследования.** Разработан нормативно-ориентированный метод обоснования решений об автоматизации нормативно обусловленных процессов деятельности. В методе нормативное поле используется для формирования целевого процесса, обязательных результатов и границ допустимого участия информационных систем, а сложившееся состояние реконструируется по функциям существующих ИС и подтверждающим их свидетельствам. Сопоставление выполняется на уровне значимых элементов процесса и проверяемых частей требуемого обеспечения с учетом контекста применения. Для каждой связи раздельно фиксируются степень подтвержденности вывода и результат проверки относительно целевого правила, что позволяет отличать отсутствие сведений от установленного несоответствия и неразрешённого конфликта. Выявленные расхождения используются для формирования прослеживаемых кандидатных вариантов реализации, требующих последующей архитектурной, технической и экономической оценки. Документальная апробация первого этапа на материалах пяти информационных систем показала применимость нормализации функций и их предварительного сопоставления с целевыми процессами на уровне документированных сведений; центральное элементное преобразование и фактическое использование функций требуют дальнейшей проверки.

DOI: 10.24412/1994-1404-2026-3-248-261

## Введение

При автоматизации нормативно обусловленной деятельности состав функций существующих информационных систем не может рассматриваться как описание целевого процесса. Система фиксирует решения, принятые в определённый момент времени, тогда как обязанности, полномочия, сроки, условия и обязательные результаты деятельности могут изменяться независимо от программной реализа-

ции. В органах публичной власти и крупных регулируемых организациях это особенно заметно: один процесс нередко распределён между несколькими приложениями, а одинаковые по названию действия могут выполняться по различающимся правилам. Поэтому вопрос о развитии конкретной системы должен ставиться после определения целевой организации деятельности и нормативных границ допустимой автоматизации.

<sup>1</sup> Свиштунов Андрей Васильевич, кандидат технических наук, старший научный сотрудник, руководитель проектов Управления проектирования и разработки информационных систем филиала публично-правовой компании «Роскадастр» Центр информационных технологий «Роскадастр-Инфотех», Москва, Россия.  
E-mail: SvistunovAV@kadastr.ru



**Практическая дилемма: от чего отталкиваться при решении об автоматизации**

Типичная управленческая ситуация выглядит проще, чем аналитическая задача, которая за ней стоит. Возникает поручение привести деятельность и информационные системы в соответствие с изменившимся порядком работы. У заказчика есть нормативные и организационные основания, у ИТ-подразделения — перечни функций и схемы интеграций, у пользователей — сложившаяся практика. Эти три представления нередко расходятся. Система может содержать нужную по названию функцию, но реализовывать устаревшее правило; несколько систем могут частично обеспечивать один процесс; автоматизированное действие может оказаться тем, которое по актуальному порядку должно оставаться за человеком.

Отсюда возникает практическая дилемма. Если начать анализ с существующей системы, её сложившаяся структура незаметно превращается в исходное требование и закрепляет прежнюю организацию деятельности. Если исходить только из нормативной модели, можно не увидеть уже работающие функции, данные и интеграции, которые целесообразно сохранить. Поэтому исходный вопрос для лица, принимающего решение, формулируется не как «какую систему модернизировать?», а как «что должно быть обеспечено в целевом процессе, что уже обеспечивается существующим ИТ-контуром, насколько это доказано и какие расхождения требуют изменений?». Предлагаемый метод строится именно вокруг последовательного ответа на эти вопросы.

В настоящей работе под «регулятивной информатикой» понимается область, в которой нормативные и организационно-регулятивные основания деятельности преобразуются в формализованные представления процессов, ограничений автоматизации, требований и решений об информационном обеспечении деятельности.

Область применения метода ограничена нормативно обусловленной деятельностью, для которой целевая процессная модель формируется относительно зафиксированного корпуса обязательных источников, а решение об автоматизации принимается в условиях уже существующего контура одной или нескольких информационных систем.

Работы по существующим и legacy-системам связывают трудности развития с функциональным устареванием и зависимостями ИТ-ландшафта [1, 2], правовые аспекты цифровой трансформации — [3]. Нормативно обусловленные требования рассматриваются в [4—7], conformance checking и процессная аналитика — в [8—11], связь процессов, требований и ИС — в [5, 12—14]. Эти подходы не заменяют реконструкцию сложившейся автоматизации из разнородных свидетельств.

Исходным этапом является идентификация процессов по нормативным и иным обязательным ис-

точникам. Такой метод для нормативно насыщенных областей предложен О.А. Шелестович [4]. Здесь этот результат используется как основание для следующего шага: определения границ допустимой автоматизации и формирования целевого состояния для последующего сопоставления с реконструированным состоянием существующих ИС.

В архитектуре сквозной прослеживаемости [14] задана цепочка «обязательное основание — предписание — процесс — решение об автоматизации — требование к системе». Настоящая работа конкретизирует предшествующий требованиям этап: формирование целевого состояния, независимую реконструкцию существующей автоматизации и анализ их расхождений с сохранением доказательственных оснований.

**Смежные подходы и постановка задачи**

Ближайшие современные подходы закрывают отдельные части задачи: regulatory requirements engineering — извлечение и проверку нормативных требований [7], conformance checking — сопоставление выполнения с заданной моделью [9, 11], прослеживаемость — связи процессов, требований и архитектурных решений [12—14]. Поэтому новизна не связывается с этими операциями как таковыми.

Предлагаемый метод сосредоточен на получении проверяемого вывода о состоянии автоматизации при неполных и потенциально противоречивых сведениях о нескольких ИС. Задача разделена на формирование нормативно обусловленной цели, реконструкцию сложившегося состояния и их доказательно контролируемое сопоставление; E0—E3 характеризуют силу свидетельств.

**Общая схема метода**

Метод опирается на два независимо формируемых представления. Из обязательных оснований строятся целевой процесс и ограничения автоматизации, после чего в их пределах фиксируется целевое состояние. Сложившееся состояние реконструируется по функциям существующих ИС и подтверждающим их свидетельствам.

Если нормативное основание не задаёт единственную форму участия ИС, целевая форма фиксируется отдельным организационным или проектным решением. Функции существующих ИС нормализуются и получают процессную интерпретацию независимо от этой цели.

Сопоставление выполняется по значимым элементам и контекстам; расхождения оцениваются с учётом критичности, маршрута, правила и доказательности и используются для формирования кандидатных вариантов реализации.

В прикладном смысле схема рис. 1 читается как четыре последовательных шага. Сначала устанавливается, как должна быть организована деятельность и где проходят границы допустимой автоматизации. Затем



Рисунок 1. Нормативно-ориентированная схема обоснования решения об автоматизации

независимо выясняется, что реально или документированно обеспечивают существующие системы. После этого обе картины приводятся к сопоставимому процессному представлению и выявляются не просто «отсутствующие функции», а конкретные расхождения по действиям, результатам, полномочиям, правилам и форме участия ИС. Только на последнем шаге формируются кандидатные варианты: развивать одну систему, несколько систем, создавать новый контур либо сочетать эти решения. Тем самым технический выбор переносится из начала анализа в его завершение.

### Формирование целевой процессной модели

Нормативное поле рассматривается как совокупность нормативных и обязательных организационных источников, определяющих деятельность. Из них выделяются обязанности, полномочия, запреты, сроки, условия применимости и обязательные результаты; для каждого предписания устанавливаются процесс, участники, маршруты, входы, выходы и ответственность. Переход от нормативных оснований к процессному и формализованному представлению деятельности развивается в работах [4—7].

Структура существующих приложений не принимается за целевую: границы процессов формируются независимо от ИС. Цепочка прослеживаемости [14] используется здесь только как основание формирования целевого представления до этапа требований.

Для каждого значимого элемента определяется нормативно допустимая форма участия информационной системы. Источник может прямо предписывать электронную форму, ограничивать или исключать автоматизацию либо допускать несколько вариантов. В первых двух случаях ограничение переносится в целевую модель непосредственно; при наличии альтернатив фиксируется множество допустимых форм, а конкретная целевая форма устанавливается отдельным организационным или проектным решением с сохранением его основания. Поэтому метод не выводит технологическое решение из нормы: нормативное поле задаёт обязательные требования и границы допустимого, внутри которых формируется целевое состояние автоматизации.

### Реконструкция сложившегося состояния автоматизации

Второй поток начинается не с процессов, а с функций существующих информационных систем. Их описания неоднородны по уровню детализации и нередко объединяют несколько действий в одной формулировке. Поэтому прямое сопоставление названия функции с названием процесса не используется: функции предварительно приводятся к процессно интерпретируемому виду. Связь процессных представлений, требований и системной архитектуры рассматривается в работах [5, 12—14]; в предлагаемом методе эта задача решается

через процессную интерпретацию функций существующих ИС, а не через прямое сопоставление названий процессов и функций.

Нормализация включает разделение составных формулировок, если в них присутствуют самостоятельные операции или результаты, и объединение дублирующих описаний при сохранении их источников. Технические функции, не соотносимые с самостоятельным предметным действием или результатом, сохраняются как характеристики ИС, но не образуют самостоятельных элементов целевого процесса. Для нормализованной функции устанавливаются создаваемый результат или изменение состояния, выполняемая операция и форма участия системы, объект деятельности и данные, роль, условия и маршрут, а также контекст эксплуатации.

Полученная процессная интерпретация используется для поиска значимого элемента целевого процесса, которому функция может соответствовать. На этом этапе формируется только предварительная связь; сходство терминов, экранов, полей или документов служит признаком для поиска, но не заменяет содержательной проверки. Если функция не соотносится с элементами рассматриваемого целевого процесса, она не включается в реконструированное состояние этого процесса и не объявляется избыточной автоматически, поскольку может обслуживать другую деятельность.

Сложившееся состояние формируется из принятых связей при выбранном пороге: E0 отражает документированное представление, E1 — установленный механизм реализации или исполнения, E2 — фактическое исполнение, E3 — проверенный результат. Поэтому каждый вывод имеет явную доказательственную силу.

### Единица анализа и контекст

Общей единицей, в которой сводятся целевое и реконструированное состояния, является значимый элемент процесса: действие, решение, проверка, изменение состояния, операция с данными или документом, информационный обмен либо результат, для которого может быть отдельно установлена требуемая форма обеспечения. Процесс задаёт общий результат, маршрут — один из способов его достижения, а функция существующей системы рассматривается как возможное средство автоматизации конкретного элемента, но не как объект, сопоставимый с процессом в целом.

Элемент должен сохранять предметный смысл и одновременно допускать проверку связи с функцией. Экран, кнопка или программный модуль сами по себе элементами процесса не являются. Объект данных, документ или сервис выделяются отдельно только тогда, когда их создание, изменение, передача или получение образует нормативно либо организационно значимый результат.

Связь всегда фиксируется в контексте  $x$ , который включает версию системы, подразделение или площадку, категорию пользователей, период и условия

применимости рассматриваемого случая: тип обращения или объекта, состояние, пороговые значения и иные данные, определяющие ветвь процесса. Если элемент обеспечивается несколькими ИС, контекст содержит согласованную конфигурацию их версий. Сведения из разных контекстов не объединяются в вывод о сложившемся состоянии без дополнительного обоснования; тот же контекст используется при сопоставлении с целевым состоянием.

### Практический смысл формализации

Формальная запись далее нужна не для замены экспертного или управленческого решения математической формулой, а для воспроизводимости анализа. Обозначение  $m$  можно читать как паспорт проверяемого утверждения: какая система и функция рассматриваются, какую конкретную часть целевого обеспечения они затрагивают, в каком контексте это справедливо, чем вывод подтверждён и соответствует ли он целевому правилу. Части  $q$  — это не абстрактные математические объекты, а минимальные проверяемые вопросы вроде «предоставлены ли данные для решения», «зафиксирован ли результат» или «сохранено ли принятие решения за человеком». Уровни E0—E3 отвечают на вопрос «насколько доказан вывод», знак  $v$  — «соответствует ли установленное состояние цели», а итоговый показатель соответствия используется лишь как компактная фиксация того, доказано ли соответствие процесса при выбранной требовательности к свидетельствам.

### Правила установления связи

После нормализации и процессной интерпретации для функции формируется предварительная предметная связь с элементом процесса и, после декомпозиции целевой формы, с конкретной проверяемой частью  $q$ . Запись сохраняет систему, функцию, элемент, проверяемую часть, контекст, наблюдаемую форму участия, уровень доказательности, результат проверки и процедурный статус.

$$m = \langle S, f, u, q, x, h, e, v, \sigma \rangle. \quad (1)$$

В записи (1)  $S_i$  — система;  $f$  — её функция;  $u$  — элемент процесса;  $q$  — атомарная проверяемая часть целевой формы обеспечения или ограничения участия ИС;  $x$  — контекст;  $h$  — наблюдаемая форма участия;  $e$  — уровень доказательности E0—E3;  $v$  — результат проверки относительно  $q$ : соответствует (+), не соответствует (–) или не установлен (?);  $\sigma$  — статус предметной связи. Для предварительной связи  $q$  и  $v$  могут быть не заданы, но до агрегирования они обязательны. Предметная связь сохраняется и при  $v = -$ . Реестр связи хранит версию  $S_i$ , версию целевой модели, источники и проверенные фрагменты, подтверждающие и опровергающие свидетельства. Для требования, не выражаемого функцией ИС, например сохранения решения

Минимальные признаки связи

| ПРИЗНАК                           | ТИП ПРИЗНАКА                            | ПРОВЕРОЧНЫЙ ВОПРОС                                                               | ПРАВИЛО РЕШЕНИЯ                                                                                                 |
|-----------------------------------|-----------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Результат или изменение состояния | Проверка соответствия                   | Соответствует ли фактический результат результату, заданному $q$ ?               | Несовпадение даёт $V = -$ ; предметная связь с $q$ сохраняется при идентичном обеспечивающем действии и объекте |
| Операция и форма участия системы  | Предметная связь с $q$                  | Выполняет ли функция обеспечивающее действие или преобразование, заданное $q$ ?  | Несовпадение операции с $q$ исключает эту предметную связь; форма участия оценивается через $V$                 |
| Объект деятельности и данные      | Предметная связь с $q$ , если применимо | Совпадают ли предметный объект, идентификаторы и смысл состояния, заданные $q$ ? | Несовпадение предметного объекта исключает связь с $q$ ; отклонение целевого состояния фиксируется через $V$    |
| Роль и полномочия                 | Проверка соответствия, если применимо   | Соответствуют ли наблюдаемая роль и полномочия требованиям $q$ ?                 | Несовпадение полномочий даёт $V = -$ ; предметная связь сохраняется                                             |
| Условия и маршрут                 | Применимость связи, если применимо      | Совпадают ли условие применимости $q$ , ветвь и ожидаемый выход?                 | Связь действует только для совпадающего условия и маршрута                                                      |
| Контекст эксплуатации             | Обязательный                            | Для какой версии, площадки и периода справедлив вывод?                           | Вывод без контекста не агрегируется                                                                             |

за человеком, используется отдельная запись проверки с  $u$ ,  $q$ ,  $x$ ,  $e$  и  $v$ .

Минимальные признаки приведены в таблице 1. Предметная идентичность устанавливается относительно конкретной части  $q$ , а не всего элемента  $u$ : операция функции должна соответствовать обеспечивающему действию или преобразованию, заданному  $q$ , и относиться к тому же предметному объекту. Соответствие результата, роли, правила и формы участия целевому состоянию проверяется отдельно и отражается в  $V$ . Условия, маршрут и контекст определяют область применимости связи.

Выполнение признаков предметной идентичности позволяет принять содержательную гипотезу о связи функции с конкретной  $q$ . Такая связь ещё не свидетельствует ни о наличии функции в промышленной версии системы, ни о её фактическом использовании и тем более о соответствии целевому правилу. Поэтому далее раздельно устанавливаются уровень доказательности  $e$  и результат проверки  $V$ .

#### Подтверждение связи и конфликты источников

Уровень доказательности относится к конкретной предметной связи или записи проверки в контексте. E0—E3 характеризуют силу свидетельства независимо от того, относится ли проверяемая  $q$  к системной или человеческой части обеспечения. Уровень  $e$  и знак результата  $V$  образуют две независимые характеристики.

Уровень определяется наиболее сильным подтверждённым типом утверждения, а не накоплением всех артефактов. Для системной части E1 означает

обнаруженную реализацию функции, для человеческой — наличие установленного механизма исполнения: роли, полномочия и порядка. E2 требует подтверждения фактического исполнения. Для E3 заранее задаются критерий результата, область и период либо объём проверки; E3 присваивается по факту воспроизводимой проверки независимо от её положительного или отрицательного исхода, фиксируемого в  $V$ .

Документированное утверждение без обнаруженного механизма остаётся на E0; обнаруженный механизм без подтверждения исполнения — на E1; интервью без проверяемого подтверждения не даёт E2. Если функция или человеческое действие предметно связано с  $q$ , но правило, роль, результат или форма участия противоречат цели, запись и свидетельства сохраняются с  $V=-$  и не покрывают  $q$ . Применимое неразрешённое отрицательное свидетельство сохраняется независимо от выбранного  $t$ : повышение порога само по себе не превращает нарушение в соответствие; свидетельство снимается только после документированного разрешения, признания неприменимым либо опровержения более сильным актуальным свидетельством в том же контексте.

#### Проверка соответствия целевому состоянию

Доля принятых связей сама по себе не определяет соответствие реконструированного состояния целевому. Перед агрегированием формируются множества элементов и маршрутов, входящие в критерий соответствия, и фиксируются основания их построения. Классификацию выполняет аналитик по источникам



Таблица 2

Уровни подтверждения связи

| УРОВЕНЬ | ЧТО ПОДТВЕРЖДАЕТСЯ                                                                                                                                          | ТИПОВОЙ АРТЕФАКТ                                                                                                                     | ДОПУСТИМЫЙ ВЫВОД                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| E0      | Документировано проверяемое утверждение о системной или человеческой части $q$                                                                              | Техническое задание, руководство, регламент, описание роли или порядка исполнения                                                    | Зафиксирована гипотеза о способе обеспечения; фактическое исполнение не доказано |
| E1      | Обнаружен установленный механизм реализации или исполнения                                                                                                  | Для ИС — модуль, конфигурация, интерфейс, схема данных; для человеческой части — установленная роль, полномочие и порядок исполнения | Механизм существует; фактическое исполнение не доказано                          |
| E2      | Фактическое исполнение системной функции или человеческого действия подтверждено в заданном контексте                                                       | Журнал, транзакция, наблюдение, подтверждённый сценарий, протокол выполнения                                                         | Фактическое участие подтверждено; знак соответствия фиксируется отдельно в $V$   |
| E3      | Результат системной или человеческой части проверен по заранее заданному критерию в установленной области; исход может быть положительным или отрицательным | Контрольная выборка, история данных, протокол проверки, подтверждённый результат исполнения                                          | E3 фиксирует силу проверки; соответствие или нарушение отражается отдельно в $V$ |

целевой модели, а утверждает субъект, уполномоченный принимать решения о целевой организации процесса. Правила приведены в таблице 3; при этом  $U_{crit}(p,x) \subseteq U_{req}(p,x)$ : каждый критический элемент, обязательный вне выбора альтернативного маршрута, является обязательным. Критичность элементов внутри альтернативных маршрутов учитывается при подтверждении соответствующего маршрута.

Несоответствие устанавливается, когда сложившееся состояние достаточно подтверждено, но отличается от целевого; конфликт — когда несовместимые свидетельства или правила не позволяют сделать однозначный вывод. Одна  $q$  не покрывается набором

частичных функций: самостоятельные операции предварительно выделяются как отдельные  $q$ . Для каждой обязательной передачи между  $q$  либо между элементами формируется отдельная запись проверки с исходной и принимающей частями, контекстом  $x$ , уровнем  $e$  и результатом  $v$ . Передача подтверждена при пороге  $\tau$  только при наличии применимой записи с  $e \geq \tau$  и  $v = +$  и отсутствии применимого неразрешённого  $v = -$ . Отрицательное свидетельство блокирует передачу независимо от  $\tau$  до документированного разрешения, признания неприменимым либо опровержения более сильным актуальным свидетельством в том же контексте.

Таблица 3

Правила формирования элементов пороговой модели

| ОБЪЕКТ                                   | ОСНОВАНИЕ И ПРАВИЛО ФОРМИРОВАНИЯ                                                                                                                                                                                                                                                   | ОТВЕТСТВЕННЫЙ СУБЪЕКТ                                                  | АРТЕФАКТ ФИКСАЦИИ                        |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|------------------------------------------|
| $U_{req}(p,x)$ :<br>обязательный элемент | Включаются элементы, обязательные в контексте $X$ независимо от выбора допустимого альтернативного маршрута. Элементы, относящиеся только к отдельному альтернативному маршруту, учитываются при подтверждении соответствующего маршрута.                                          | Уполномоченный владелец или заказчик процесса                          | Реестр элементов со ссылкой на основание |
| $U_{crit}(p,x)$ :<br>критический элемент | Обязательный элемент, отсутствие или неверное выполнение которого делает результат нормативно недопустимым, исключает обязательный результат либо нарушает некомпенсируемый запрет или контроль. Критичность элементов альтернативного маршрута учитывается внутри этого маршрута. | Уполномоченный владелец процесса по установленной экспертной процедуре | Реестр элементов с признаком критичности |
| Необязательный элемент                   | Не требуется для нормативно допустимого результата; может повышать эффективность, удобство или качество исполнения.                                                                                                                                                                | Владелец процесса или субъект проектного решения                       | Целевая модель процесса                  |
| $R_{req}(p,x)$ :<br>обязательный маршрут | Маршрут должен быть доступен в контексте $X$ для достижения обязательного результата при наступлении условия его применения.                                                                                                                                                       | Уполномоченный владелец процесса                                       | Модель маршрутов или регламент           |

| ОБЪЕКТ                                            | ОСНОВАНИЕ И ПРАВИЛО ФОРМИРОВАНИЯ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ОТВЕТСТВЕННЫЙ СУБЪЕКТ                                       | АРТЕФАКТ ФИКСАЦИИ                          |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|--------------------------------------------|
| $Alt(p, x)$ :<br>семейство групп альтернатив      | Содержит группы $A$ взаимозаменяемых маршрутов, каждый из которых допустим для одного целевого результата в контексте $X$ . Группы и их состав фиксируются до агрегирования.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Уполномоченный владелец процесса                            | Модель процесса с идентификатором группы   |
| Требуемая форма обеспечения                       | Фиксируется как автоматическая, информационно поддерживаемая ручная, ручная или смешанная. При нескольких допустимых формах выбор закрепляется отдельным организационным или проектным решением.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Субъект, уполномоченный утверждать целевое состояние        | Карта целевого состояния автоматизации     |
| $P(u, x)$ :<br>части требуемого обеспечения       | Целевая форма элемента раскладывается на атомарные проверяемые части $q$ , каждая из которых имеет самостоятельное обеспечивающее действие или ограничение и проверяемый результат. Совместно необходимые $q$ образуют AND-набор, взаимозаменяемые — OR-группу. Если для одной предполагаемой $q$ требуются несколько самостоятельных операций, она до агрегирования декомпозируется на отдельные $q$ ; обязательные передачи между ними фиксируются и проверяются отдельно. Для ручной и смешанной формы отдельно задаётся $q$ сохранения действия или решения за человеком.                                                                                                                                                           | Субъект, утверждающий целевое состояние                     | Карта целевого состояния                   |
| $Q_{\tau}(p, x)$ :<br>подтверждённое обеспечение  | Элемент входит в $Q_{\tau}(p, x)$ , если при $\tau$ подтверждены все необходимые $q$ из $P(u, x)$ , один вариант каждой OR-группы и все обязательные передачи между $q$ внутри элемента. Системная $q$ покрывается принятой $m$ , явно отнесённой к $q$ , $s \geq \tau$ и $v = +$ ; частичные связи не суммируются для покрытия недекомпозированной $q$ . Альтернативные функции могут покрывать одну $q$ , если каждая по отдельности удовлетворяет её действию и результату. Для человеческой $q$ требуется положительная запись проверки $s \geq \tau$ . Передачи подтверждаются при том же $\tau$ по общему правилу. Любое применимое неразрешённое $v = -$ блокирует соответствующую $q$ или передачу независимо от $e$ и $\tau$ . | Аналитик по целевой форме и свидетельствам                  | Реестр связей, записи проверок, карта цели |
| $R^+_{\tau}(p, x)$ :<br>подтверждённый маршрут    | Маршрут включается, если все обязательные для него элементы входят в $Q_{\tau}(p, x)$ , обязательные передачи между элементами и частями разных элементов подтверждены при том же пороге $\tau$ по общему правилу и внутри маршрута отсутствует неразрешённый критический конфликт. Конфликт внутри одной альтернативы исключает эту альтернативу, но не блокирует другую допустимую альтернативу.                                                                                                                                                                                                                                                                                                                                      | Аналитик по целевой модели и подтверждённым связям          | Модель маршрутов и реестр связей           |
| $C^{crit}_{\tau}(p, x)$ :<br>критический конфликт | Включаются неразрешённые критические конфликты по элементам и ограничениям, обязательным независимо от выбора альтернативного маршрута либо общим для всех его допустимых альтернатив. Конфликт, относящийся только к одной альтернативе, учитывается при формировании $R^+_{\tau}(p, x)$ и не включается в глобальное множество, если не затрагивает общие элементы или ограничения.                                                                                                                                                                                                                                                                                                                                                   | Уполномоченный эксперт или экспертная группа                | Журнал конфликтов                          |
| Несоответствие                                    | Фиксируется, когда сложившееся состояние установлено с требуемой доказательностью, но отличается от целевого; при однозначных свидетельствах конфликтом не является.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Аналитик; результат принимается в порядке применения метода | Реестр расхождений                         |

Условия агрегирования соответствия

| ЭЛЕМЕНТ ИЛИ ВЕТЬ ПРОЦЕССА | ПРАВИЛО АГРЕГАЦИИ                                                                                                                                                                                                                                                                                                       |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Критический элемент       | Целевая форма обеспечения должна быть подтверждена; отсутствие или спорность критического элемента блокирует положительный вывод о соответствии                                                                                                                                                                         |
| Обязательный элемент      | Должна быть подтверждена требуемая форма: автоматизация либо сохранение действия за человеком с необходимым информационным обеспечением                                                                                                                                                                                 |
| Необязательный элемент    | Не влияет на соответствие, но учитывается при оценке эффективности                                                                                                                                                                                                                                                      |
| Условная ветвь            | Проверяется во всех контекстах, где выполняется условие применения                                                                                                                                                                                                                                                      |
| Альтернативные маршруты   | Для положительного вывода достаточно хотя бы одного утверждённого маршрута в каждой группе взаимозаменяемых вариантов                                                                                                                                                                                                   |
| Параллельные ветви        | Подтверждаются все ветви, результаты которых обязательны                                                                                                                                                                                                                                                                |
| Ручное действие           | Положительный вывод требует подтверждения на выбранном уровне, что действие или решение сохраняется за человеком; отсутствие сведений о подмене недостаточно. При необходимости одновременно подтверждаются системные функции информационной поддержки.                                                                 |
| Обязательная передача     | Подтверждается отдельной записью проверки $s \geq \tau$ и $V = +$ ; проверяются исходная и принимающая части, идентификаторы, данные или документ, состояние, направление передачи, ответственность и обработка ошибки. Применимое неразрешённое $V = -$ блокирует подтверждение передачи независимо от порога $\tau$ . |

Показатель вычисляется только после завершения подготовки входной модели: утверждена версия целевого процесса относительно зафиксированного нормативного корпуса; задано множество значимых элементов  $U(p)$ , для каждого применимого элемента сформирован атомарный состав  $P(u, x)$ , задано семейство маршрутов  $R(p, x)$ , отношение принадлежности элементов маршрутам, обязательные передачи между  $q$  и элементами с правилами их проверки и семейство групп альтернатив  $Alt(p, x)$ ; для пустых множеств зафиксировано содержательное основание. Для незавершённой или не проверенной на полноту модели  $s_\tau(p, x)$  не вычисляется.

Введём бинарный показатель  $s_\tau(p, x)$  как индикатор подтверждённого соответствия:  $s_\tau(p, x)=1$  означает, что реконструированное состояние процесса  $p$  в контексте  $X$  подтверждено соответствует целевому состоянию при пороге  $\tau$ ; значение 0 само по себе не означает установленного несоответствия.

Пусть  $\tau \in \{0, 1, 2, 3\}$  — порог подтверждения;  $U_{req}(p, x)$ ,  $R_{req}(p, x)$  и  $Alt(p, x)$  формируются по правилам таблицы 3;  $Q_\tau(p, x)$  — элементы, для которых подтверждена требуемая целевая форма;  $R_\tau^+(p, x)$  — подтверждённые маршруты;  $C_\tau^{crit}(p, x)$  — неразрешённые критические конфликты общего действия. Значение  $s_\tau(p, x)=1$  устанавливается тогда и только тогда, когда выполнены условия (2).

$$\begin{aligned}
 s_\tau(p, x) = 1 \Leftrightarrow & \\
 U_{req}(p, x) \subseteq Q_\tau(p, x); & \\
 R_{req}(p, x) \subseteq R_\tau^+(p, x); & \\
 (\forall A \in Alt(p, x))(\exists r \in A: r \in R_\tau^+(p, x)); & \\
 C_\tau^{crit}(p, x) = \emptyset. &
 \end{aligned}
 \quad (2)$$

Значения  $\tau = 0, 1, 2$  и  $3$  соответствуют типам доказанного утверждения.  $s_0(p, x)=1$  означает соответствие лишь на уровне документированных утверждений; для вывода о фактическом использовании нужен  $\tau \geq 2$ . При  $s_\tau(p, x)=0$  сохраняется причина: установленное несоответствие, недостаточность свидетельств или конфликт. Для чисто ручной формы системная  $m$  может отсутствовать, но требуется положительное свидетельство  $e \geq \tau$ , что действие остаётся за человеком. Для смешанной формы подтверждаются системные и человеческая части. Неразрешённое свидетельство запрещённой подмены блокирует соответствующую  $q$  независимо от своего  $e$ .

### Иллюстративный пример применения метода

Пример синтетический и к апробации не относится. Пусть обязательный элемент  $u \in U_{req}(p, x)$  — юридически значимое решение, которое по целевой модели принимает сотрудник.  $P(u, x)$  включает  $q_1$  «предоставить сотруднику данные для решения»,  $q_2$  «зафиксировать решение, принятое сотруд-

ником» и  $q_H$  «решение принимает человек». Для  $q_1$ ,  $q_2$  и  $q_H$  имеются положительные ЕЗ-свидетельства с  $V=\pm$ . Одновременно журнал эксплуатации содержит применимое Е2-свидетельство того, что в той же области применимости ИС в отдельных случаях принимает итоговое решение автоматически; запись относится к  $q_H$  и имеет  $V=-$ , а её применимость не разрешена. Поэтому  $q_H$  не считается подтверждённой и  $u \notin Q_3(p, x)$ , вследствие чего  $s_3(p, x)=0$ . Если бы отрицательное Е2-свидетельство ошибочно отбрасывалось только из-за порога  $\tau=3$ , все положительные части имели бы ЕЗ и возник бы ложноположительный вывод. В предлагаемом методе отрицательная запись сохраняется до документированного разрешения; именно это, а не нехватка положительных ЕЗ-свидетельств, блокирует вывод.

### Требования к проверке воспроизводимости

Воспроизводимость центрального преобразования проверяется на одной утверждённой целевой модели: аналитики получают одинаковые элементы,  $P(u, x)$ , маршруты и контексты и независимо оценивают нормализованные функции, человеческие записи проверки и свидетельства. Общий набор единиц сравнения образует объединение кандидатов, выявленных хотя бы одним аналитиком; для второго аналитика отсутствие соответствующей записи кодируется как отдельная категория «не выявлено», а не как пропуск. Сравняются отнесение к  $q$ ,  $h$ ,  $v$  и  $\sigma$  с использованием коэффициента Коэна  $K$ ; для порядкового уровня Е0—Е3 применяется взвешенный  $K$  с линейными весами. Категория «не применимо» исключается из конкретного сравнения только при независимом совпадающем решении обоих аналитиков. Дополнительно сопоставляются сформированные  $Q_\tau(p, x)$  и итоговые  $s_\tau(p, x)$ . Показатели рассчитываются до согласования; затем разногласия рассматривает третий эксперт, исходные оценки сохраняются. Воспроизводимость построения самой целевой модели относится к предшествующему этапу нормативно-процессного анализа.

В документальной апробации такая проверка не выполнялась; воспроизводимость элементного сопоставления не оценивалась.

При наличии пригодных событийных журналов реконструированный маршрут сопоставляется с наблюдаемым потоком выполнения [8—10]; такие сведения могут усиливать подтверждение Е2—Е3. В настоящей работе доступны только данные для  $\tau = 0$ .

### Документальная апробация первого этапа метода

Для документальной апробации первого этапа использован обезличенный корпус федеральной регулируемой организации: описания пяти взаимосвязанных информационных систем одного организационного контура, 24 функциональных раздела и 501 нормали-

зованная формулировка функции. До анализа была зафиксирована версия реестра из 97 целевых процессов, сформированная независимо от приложений по признакам самостоятельного результата, ответственной роли, входов, выходов и нормативного либо организационного основания.

Прямое документированное соответствие фиксировалось, если описания функций охватывали обязательный результат и ключевые действия процесса; частичное или требующее изменения — при неполном покрытии, устаревшем правиле либо иной целевой границе; отсутствие соответствия — если содержательно соотносимая функция в корпусе не выявлялась. Эта укрупнённая классификация не является значением  $S_0(p, x)$ , поскольку элементы и множества пороговой модели не формировались. Для 47 процессов промежуточной категории отдельно сохранялась причина отнесения. Всего 23 процесса имели прямое документированное соответствие, 47 — частичное или требующее изменения, 27 — без выявленного соответствия; все положительные утверждения остались на Е0.

Значимые элементы построчно не выделялись. Поэтому апробация подтверждает только нормализацию функций и предварительное преобразование документированных функций в процессное представление; элементное сопоставление, функциональное дублирование реализации, конфликты правил, техническая реализация, фактическое использование и воспроизводимость экспертной разметки не проверялись.

Результаты показывают применимость первого этапа для систематизации корпуса описаний и подготовки данных к детальному элементному сопоставлению. Исходные формулировки функций и номенклатура документов не раскрываются из-за ограничений публикации обезличенного корпуса, поэтому корректность отдельных нормализаций и категорий 23/47/27 не может быть независимо проверена по материалам статьи. Эти результаты следует рассматривать как документальную апробацию подготовительного этапа, а не как валидацию центрального преобразования  $m \rightarrow Q_\tau \rightarrow s_\tau$ . Последующая проверка требует элементного сопоставления на выборке процессов, независимой разметки и технических либо эксплуатационных материалов.

### Выявление расхождений и обоснование способа реализации

После приведения обоих состояний к общей процессной структуре сопоставление выполняется на уровне значимых элементов, маршрутов и контекстов. Результатом является структурированное описание расхождений: отсутствия или недостаточности требуемого системного обеспечения, частичного обеспечения результата, различий правил, ролей или контекстов, а также распределения одного элемента между несколькими системами. Функция вне границ рассматриваемого процесса не считается избыточной автоматически.



Таблица 5

**Результаты и ограничения документальной апробации первого этапа метода**

| ПОКАЗАТЕЛЬ                            | ЗНАЧЕНИЕ       | ИНТЕРПРЕТАЦИЯ                                                                                                   |
|---------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------|
| Информационные системы                | 5              | Взаимосвязанные системы одного организационного контура                                                         |
| Функциональные разделы                | 24             | Разделы описаний систем и подсистем                                                                             |
| Нормализованные функции               | 501            | Сложные формулировки разделены, дублирующие описания объединены                                                 |
| Целевые процессы                      | 97             | Фиксированная версия реестра, сформированная независимо от приложений                                           |
| Значимые элементы процессов           | Не выделялись  | Пилот выполнен на уровне процессов; элементное сопоставление не проверялось                                     |
| Прямое документированное соответствие | 23 (23,7 %)    | Основной результат и ключевые действия описаны; фактическое использование не доказано                           |
| Частичное или требующее изменения     | 47 (48,5 %)    | Фрагментарное описание, устаревшее правило либо иная целевая граница; конкретная причина фиксировалась отдельно |
| Соответствие не выявлено              | 27 (27,8 %)    | Отсутствие в документации не доказывает фактическое отсутствие                                                  |
| Связи Е1—Е3                           | 0              | Технические и эксплуатационные артефакты не исследовались                                                       |
| Независимая разметка                  | Не проводилась | Воспроизводимость установления связей на уровне элементов не оценивалась                                        |

Таблица 6

**Правила формирования варианта реализации**

| ПРИЗНАКИ ДЛЯ ФОРМИРОВАНИЯ КАНДИДАТА                                                                                                                                                                                           | КАНДИДАТНЫЙ ВАРИАНТ     | НЕОБХОДИМАЯ ДОПОЛНИТЕЛЬНАЯ ПРОВЕРКА                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Одна ИС уже обеспечивает связный основной контур процесса и существенную часть требуемого информационного обеспечения; выявленные расхождения локальны и могут быть устранены в пределах её функций, данных и ответственности | Развитие одной ИС       | Техническая реализуемость локальных изменений, влияние на данные и интеграции, отсутствие нарушения нормативных ограничений                                                             |
| Целевой результат распределён между несколькими ИС; границы ответственности устойчивы, обязательные передачи обеспечимы                                                                                                       | Развитие нескольких ИС  | Реализуемость обязательных передач, совместимость версий и данных, устойчивость распределённых границ ответственности                                                                   |
| Критические или сквозные элементы выходят за сложившиеся границы функций, данных или ответственности существующих ИС либо их распределение противоречит целевой модели                                                        | Новая система           | Отдельная архитектурная и техническая оценка должна подтвердить, что развитие действующих ИС не обеспечивает целевое состояние либо является неприемлемым по установленным ограничениям |
| Подтверждённая автоматизация частично сохраняется, но отсутствующие критические или сквозные элементы требуют отдельного контура                                                                                              | Комбинированный вариант | Архитектурная проверка границ нового и сохраняемого контуров, интеграций, первичного ведения данных и ответственности                                                                   |

Значимость расхождения определяется ролью элемента, нормативным ограничением и уровнем подтверждения существующей автоматизации. По условиям таблицы 6 формируется один или несколько кандидатных вариантов реализации. Таблица не подтверждает техническую, архитектурную или экономическую реализуемость изменений: для каждого кандидата указывается дополнительная проверка, без которой он не получает статус обоснованного к реализации варианта.

Для руководителя или заказчика итог метода должен читаться не как набор обозначений, а как прослеживаемая карта решения: какое целевое требование рассматривается; как оно обеспечивается сейчас; какими источниками это подтверждено; где установлено расхождение или недостаточно сведений; какие варианты изменения ИС из этого следуют и что ещё требуется проверить до выбора. Поэтому таблица 6 не заменяет управленческое решение, а отделяет доказанную часть обоснования от последующей оценки стоимости, сроков, архитектурных последствий и рисков.

Для каждого кандидата отдельно проверяются обязательные и выбранные альтернативные маршруты, нормативные ограничения, доказательность, данные, ответственность и реализуемость изменений. Неподтверждённая реализуемость означает статус «требуется оценки» и не служит основанием исключать другие кандидаты. Метод не ранжирует допустимые варианты по стоимости или эффективности; такой выбор требует профильных оценок. Обоснование сохраняет связь с выявленными расхождениями и служит входом для последующей формализации требований к автоматизированной системе<sup>2</sup>.

### Обсуждение и ограничения

Научный вклад не состоит в нормативном моделировании, conformance checking или прослеживаемости. Отличие метода — доказательственная реконструкция состояния нескольких ИС при отсутствии единой надёжной модели *as-is*: свидетельства адресуются атомарным *q*, а уровень *e* отделяется от результата *V*. Предметная связь может не дать положительного покрытия, а неразрешённое отрицательное свидетельство сохраняет блокирующее значение независимо от порога.

Conformance checking сопоставляет наблюдаемое выполнение с заданной моделью [9, 11]. Метод рассчитан на отсутствие пригодных журналов и единой проверенной модели фактического исполнения, когда состояние реконструируется из разнородных свидетельств по нескольким ИС. Regulatory requirements engineering [7, 14] связывает нормативное содержание с инженерными спецификациями; поэтому нор-

мативное происхождение цели не заявляется как новый результат. Работа конкретизирует доказательную процедуру предшествующего требованиям этапу архитектуры [14].

Метод не формирует управленческое решение автоматически и не подтверждает реализуемость кандидатного варианта. Он устанавливает подтверждённое соответствие или фиксирует причину отрицательного результата, выявляет варианты, непосредственно противоречащие целевому состоянию, и формирует прослеживаемые кандидаты для последующей архитектурной, технической, экономической, правовой и риск-ориентированной оценки. Выводы о фактическом использовании функций требуют порога не ниже  $\tau=2$ .

Основными угрозами валидности остаются неполнота нормативного корпуса, выбор уровня детализации целевой процессной модели, экспертная вариативность нормализации функций и неполнота технических и эксплуатационных свидетельств.

Для применения в крупной организации нужны единые идентификаторы процессов, элементов, систем, функций и контекстов и определённые владельцы данных, систем и нормативных оснований. Специализированная платформа не обязательна; достаточно репозитория, сохраняющего версии, источники, связи, уровни подтверждения и историю решений.

### Заключение

Обоснование решения об автоматизации нормативно обусловленной деятельности начинается с определения целевого процесса и границ допустимой автоматизации. При нескольких допустимых формах целевое состояние фиксируется отдельным организационным или проектным решением, после чего в той же процессной системе координат реконструируется сложившееся состояние.

Метод задаёт два независимых преобразования: нормативные основания — в целевой процесс и зафиксированную целевую форму; функции существующих ИС — в реконструированное состояние с доказательной основой. Механизм  $m \rightarrow q \rightarrow Q_\tau \rightarrow S_\tau$  отделяет предметную идентичность операции относительно атомарной *q* от результата проверки *V* и связывает доказательства с конкретными частями требуемого обеспечения. Расхождения формируют прослеживаемую основу кандидатных вариантов; их реализуемость устанавливается отдельно.

Апробация первого этапа подтвердила применимость нормализации функций и предварительной процессной классификации, но не проверила центральное элементное преобразование, фактическое использование и воспроизводимость разметки. Полная проверка требует технических и эксплуатационных материалов, независимой разметки элементов и *q* и проверки перехода  $m \rightarrow q \rightarrow Q_\tau \rightarrow S_\tau$  на раскрываемом или воспроизводимом корпусе.

<sup>2</sup> ГОСТ 34.602—2020. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Официальная карточка Росстандарта: <https://protect.gost.ru/gost/details/5876f733-ee91-431a-8cb6-9e02ea2436ac> (дата обращения: 13.09.2026).

**Информация о финансировании.**

Исследование выполнено в инициативном порядке.

**Литература**

1. Соколов Б.В., Миронов А.Н., Шестопалова О.Л. Проактивная модернизация информационных систем на основе мониторинга функционального устаревания // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2023. № 2. С. 5—21. DOI: 10.17308/sait/1995-5499/2023/2/5-21.
2. Irani Z., Abril R.M., Weerakkody V., Omar A., Sivarajah U. The Impact of Legacy Systems on Digital Transformation in European Public Administration: Lesson Learned from a Multi Case Analysis // Government Information Quarterly. 2023. Vol. 40. No. 1. Article 101784. DOI: 10.1016/j.giq.2022.101784.
3. Тихомиров Ю.А., Кичигин Н.В., Цомартова Ф.В., Бальхаева С.Б. Право и цифровая трансформация // Право. Журнал Высшей школы экономики. 2021. № 2. С. 4—23. DOI: 10.17323/2072-8166.2021.2.4.23.
4. Шелестович О.А. Метод идентификации процессов деятельности при создании информационных систем // Правовая информатика. 2026. № 2. С. 114—126.
5. Антонов В.В., Конев К.А., Пальчевский Е.В., Родионова Л.Е., Баймурзина Л.И. Обеспечение актуальности знаний о бизнес-процессе предприятия на основе онтологической модели // Онтология проектирования. 2024. Т. 14. № 1. С. 107—118. DOI: 10.18287/2223-9537-2024-14-1-107-118.
6. Богданова Т.К., Жукова Л.В. Информационно-логическая модель экспресс-анализа соответствия состояния предприятия, удовлетворяющего нормативам и регламентам, на основе общедоступных данных // Бизнес-информатика. 2022. Т. 16. № 1. С. 42—55. DOI: 10.17323/2587-814X.2022.1.42.55.
7. Kosenkov O., Elahidoost P., Gorschek T., Fischbach J., Mendez D., Unterkalmsteiner M., Fucci D., Mohanani R. Systematic Mapping Study on Requirements Engineering for Regulatory Compliance of Software Systems // Information and Software Technology. 2025. Vol. 178. Article 107622. DOI: 10.1016/j.infsof.2024.107622.
8. Васильева Е.В., Долганова О.И. Возможности совершенствования процессов подготовки правовых актов государственными органами на основе подхода Process mining // Управление. 2022. Т. 10. № 4. С. 96—110. DOI: 10.26425/2309-3633-2022-10-4-96-110.
9. Carmona J., van Dongen B., Weidlich M. Conformance Checking: Foundations, Milestones and Challenges // Process Mining Handbook / eds. W.M.P. van der Aalst, J. Carmona. Cham: Springer, 2022. P. 155—190. DOI: 10.1007/978-3-031-08848-3\_5.
10. Варнухов А.Ю. Скрытая марковская модель: метод построения модели бизнес-процесса // Бизнес-информатика. 2024. Т. 18. № 3. С. 41—55. DOI: 10.17323/2587-814X.2024.3.41.55.
11. Grohs M., Klessascheck F., Jänicke-Helling A., Pufahl L., Rehse J.-R. Can Conformance Checking Monitor Process Compliance? A Taxonomy of Regulations for Business Processes // Process Science. 2026. Vol. 3. Article 11. DOI: 10.1007/s44311-026-00044-w.
12. Позин Б.А., Циперман Г.Н. Прослеживаемость требований как основа проектирования функционально-логической архитектуры программной системы // Труды Института системного программирования РАН. 2022. Т. 34. № 1. С. 23—34. DOI: 10.15514/ISPRAS-2022-34(1)-2.
13. Mucha J., Kaufmann A., Riehle D. A Systematic Literature Review of Pre-Requirements Specification Traceability // Requirements Engineering. 2024. Vol. 29. P. 119—141. DOI: 10.1007/s00766-023-00412-z.
14. Свистунов А.В., Митавский Д.В. Нормативно-ориентированная архитектура сквозной прослеживаемости требований к информационным системам // Правовая информатика. 2026. № 2. С. 346—369. DOI: 10.24412/1994-1404-2026-2-346-369.

# A NORMATIVELY ORIENTED METHOD FOR SUBSTANTIATING DECISIONS ON THE AUTOMATION OF ACTIVITY PROCESSES

Svistunov A.V.<sup>3</sup>

**Keywords:** regulatory informatics, systems analysis, normatively governed processes, normative field analysis, target process model, existing information systems, reconstruction of the automation state, process—information system alignment, evidence levels, requirements traceability.

## Abstract

**Objective.** To develop a normatively oriented method for substantiating decisions on the automation of normatively governed activity processes within an existing information-systems landscape, in which the target process and automation constraints are defined independently of the currently operating systems, while the established automation state is reconstructed from their functions.

**Methods.** The study employs normative field analysis and process analysis, normalization and process-oriented interpretation of the functions of existing information systems, and matching of significant elements of the target and established states. It also separates the degree of evidential support for each conclusion from the outcome of its verification against the target rule. Rules for identifying and resolving conflicting evidence and for logically aggregating partial results are also applied.

**Results.** A normatively oriented method for substantiating decisions on the automation of normatively governed activity processes has been developed. Within the method, the normative field is used to derive the target process, mandatory outcomes, and the boundaries of permissible participation of information systems, while the established automation state is reconstructed from the functions of existing systems and the evidence supporting them. Matching is performed at the level of significant process elements and verifiable parts of the required provision, taking the context of application into account. For each identified relation, the degree of evidential support and the outcome of verification against the target rule are recorded separately. This makes it possible to distinguish a lack of evidence from an established non-conformity or an unresolved conflict. The identified discrepancies are used to formulate traceable candidate implementation options that require subsequent architectural, technical, and economic assessment. A documentary pilot of the first stage, based on materials from five information systems, demonstrated the applicability of function normalization and preliminary matching to target processes using documented evidence. The core element-level transformation and the actual use of the identified functions require further verification.

## References

1. Sokolov B.V., Mironov A.N., Shestopalova O.L. Proaktivnaia modernizatsiia informatsionnykh sistem na osnove monitoringa funktsional'nogo ustarevaniia // Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriia: Sistemnyi analiz i informatsionnye tekhnologii. 2023. No. 2. S. 5—21. DOI: 10.17308/sait/1995-5499/2023/2/5-21.
2. Irani Z., Abril R.M., Weerakkody V., Omar A., Sivarajah U. The Impact of Legacy Systems on Digital Transformation in European Public Administration: Lesson Learned from a Multi Case Analysis // Government Information Quarterly. 2023. Vol. 40. No. 1. Article 101784. DOI: 10.1016/j.giq.2022.101784.
3. Tikhomirov Iu.A., Kichigin N.V., Tsomartova F.V., Bal'khaeva S.B. Pravo i tsifrovaia transformatsiia // Pravo. Zhurnal Vysshei shkoly ekonomiki. 2021. No. 2. S. 4—23. DOI: 10.17323/2072-8166.2021.2.4.23.
4. Shelestovich O.A. Metod identifikatsii protsessov deiatel'nosti pri sozdanii informatsionnykh sistem // Pravovaia informatika. 2026. No. 2. S. 114—126.
5. Antonov V.V., Konev K.A., Pal'chevskii E.V., Rodionova L.E., Baimurzina L.I. Obespechenie aktual'nosti znaniia o biznes-protsesse predpriatiia na osnove ontologicheskoi modeli // Ontologiiia proektirovaniia. 2024. T. 14. No. 1. S. 107—118. DOI: 10.18287/2223-9537-2024-14-1-107-118.

<sup>3</sup> **Andrey V. Svistunov**, Ph.D. (Technology), Senior Researcher, Project Manager of the Information Systems Design and Development Department at the Roskadastr-Infotech Center for Information Technologies, a branch of the Public Law Company Roskadastr, Moscow, Russia.

E-mail: SvistunovAV@kadastr.ru



6. Bogdanova T.K., Zhukova L.V. Informatsionno-logicheskaya model' ekspress-analiza sootvetstviia sostoiianiia predpriiatiia, udovletvoraiushchego normativam i reglamentam, na osnove obshchedostupnykh dannykh // *Biznes-informatika*. 2022. T. 16. No. 1. S. 42—55. DOI: 10.17323/2587-814X.2022.1.42.55.
7. Kosenkov O., Elahidoost P., Gorshek T., Fischbach J., Mendez D., Unterkalmsteiner M., Fucci D., Mohanani R. Systematic Mapping Study on Requirements Engineering for Regulatory Compliance of Software Systems // *Information and Software Technology*. 2025. Vol. 178. Article 107622. DOI: 10.1016/j.infsof.2024.107622.
8. Vasil'eva E.V., Dolganova O.I. Vozmozhnosti sovershenstvovaniia protsessov podgotovki pravovykh aktov gosudarstvennymi organami na osnove podkhoda Process mining // *Upravlenie*. 2022. T. 10. No. 4. S. 96—110. DOI: 10.26425/2309-3633-2022-10-4-96-110.
9. Carmona J., van Dongen B., Weidlich M. Conformance Checking: Foundations, Milestones and Challenges // *Process Mining Handbook* / eds. W.M.P. van der Aalst, J. Carmona. Cham: Springer, 2022. P. 155—190. DOI: 10.1007/978-3-031-08848-3\_5.
10. Varnukhov A.Iu. Skrytaia markovskaia model': metod postroeniia modeli biznes-protssessa // *Biznes-informatika*. 2024. T. 18. No. 3. S. 41—55. DOI: 10.17323/2587-814X.2024.3.41.55.
11. Grohs M., Klessascheck F., Jänicke-Helling A., Pufahl L., Rehse J.-R. Can Conformance Checking Monitor Process Compliance? A Taxonomy of Regulations for Business Processes // *Process Science*. 2026. Vol. 3. Article 11. DOI: 10.1007/s44311-026-00044-w.
12. Pozin B.A., Tsiperman G.N. Proslezhivaemost' trebovanii kak osnova proektirovaniia funktsional'no-logicheskoi arkhitektury programmnoi sistemy // *Trudy Instituta sistemnogo programmirovaniia RAN*. 2022. T. 34. No. 1. S. 23—34. DOI: 10.15514/ISPRAS-2022-34(1)-2.
13. Mucha J., Kaufmann A., Riehle D. A Systematic Literature Review of Pre-Requirements Specification Traceability // *Requirements Engineering*. 2024. Vol. 29. P. 119—141. DOI: 10.1007/s00766-023-00412-z.
14. Svistunov A.V., Mitavskii D.V. Normativno-orientirovannaia arkhitektura skvoznoi proslezhivaemosti trebovanii k informatsionnym sistemam // *Pravovaya informatika*. 2026. No. 2. S. 346—369. DOI: 10.24412/1994-1404-2026-2-346-369.



# ПРИНЦИП ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ТЕОРЕТИКО-ПРАВОВЫЕ АСПЕКТЫ

Дубень А.К.<sup>1</sup>

**Ключевые слова:** цифровизация, информационные технологии, трансформация права, информационное право, вызовы и угрозы, информационная безопасность, принципы права, теория права, философия права.

## Аннотация

**Цель работы** состоит в анализе современных и актуальных проблем правового обеспечения информационной безопасности на национальном и международном уровнях. Обоснование теоретических положений, направленных на определение места и роли принципа достоверности информации как важного элемента по противодействию новых угроз и рисков в системе информационного и международного права.

**Методами исследования** стали следующие общенаучные методы: анализа и синтеза, абстрагирования и моделирования, обобщения, описания, классификации и др. Использовались специальные частноправовые методы познания: сравнительно-правовой, формально-юридический и др.

**Результаты исследования:** в условиях развития информационного общества возрастает роль исследований, рассматривающих принципы правового регулирования общественных отношений на примере отдельной подотрасли права как информационная безопасность. Обоснована необходимость законодательного закрепления принципа достоверности информации в международных нормативно-правовых актах в сфере обеспечения информационной безопасности, а также необходимо выработать подходы к формированию единых стандартов и требований к безопасности в информационной среде, которые позволят определять состояние защищенности информационной инфраструктуры и противодействие распространению недостоверной информации. Констатируя отсутствия специального стратегического регулирования по данному вопросу, важно обратить внимание на принцип достоверности как важного элемента по противодействию новых угроз и рисков. При этом обеспечение достоверности информации следует рассматривать как составную часть состояния защищенности государства, ее информационные ресурсы и технологии. Следовательно, информационная сфера, на сегодняшний день, неизбежно способствует дестабилизации общества и манипулированию общественным и индивидуальным сознанием. Учитывая пребывание информационного пространства в непрерывном состоянии неопределенности и опасности, а также информационный характер любых рисков, для обеспечения информационной безопасности нужен надлежащий государственный механизм, который обеспечит постоянное и бесперебойное противодействие информационным угрозам в современных условиях социально-экономических и геополитических рисков при фундаментальной трансформации мира.

DOI: 10.24412/1994-1404-2026-3-00-28

## Введение

Развитие информационных технологий сопровождается возникновением новых вызовов, угроз и рисков как практического, так и правового характера, в этой связи одной из задач государства является формирование комплексного правового регулирования, способствующего одновременно технологическому развитию общества, а также обеспечению защиты прав граждан. Сегодня в условиях цифровой трансформа-

ции цифровые технологии воздействуют на все сферы социальных и экономических отношений, поэтому технологическая революция меняет привычные парадигмы, заставляя искать решения проблем, с которыми человечество еще никогда не сталкивалось [1, с. 164]. В соответствии со стратегическими нормативно-правовыми актами, одной из угроз государства является использование информационно-коммуникационных технологий для вмеша-

<sup>1</sup> Дубень Андрей Кириллович, кандидат юридических наук, старший научный сотрудник Института государства и права Российской академии наук, г. Москва, Россия.  
E-mail: k.duben@mail.ru

тельства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, а также распространение недостоверной информации, в том числе заведомо ложных сообщений, где основным объектом такого деструктивного воздействия является молодежь.

В этой связи, как справедливо отмечает академик РАН А.Н. Савенков в своих фундаментальных работах, российское государство-цивилизация переживает в своей истории многие события, которые оказывают влияние на внутреннее национальное развитие и определяет пути мировой истории на многие десятилетия, сегодня как никогда остро стоит вопрос о том, чтобы концептуально разработать собранные воедино черты русской цивилизации, охватывающей более чем тысячелетний период истории, ее место в мировых процессах, характер взаимоотношений с другими странами и регионами [2, с. 8]. Таким образом, трансформация права и ее последующая цифровизация, имеет как позитивные, так и негативные аспекты, в частности, новые вызовы и угрозы приводят к деструктивному воздействию, а устоявшиеся правовые конструкции, порождают пробелы и коллизии в законодательстве. Следует обратить внимание, что цифровая трансформация представляет собой «комплексный процесс, который связан с радикальными изменениями в бизнес-процессах, культуре организации, организационной структуре, взаимодействии с партнерами и потребителями, инфраструктуре»<sup>2</sup>. Из этого следует, что наиболее активное воздействие цифровая трансформация оказывает на современное информационное право, что отражается на развитии информационных правоотношений и выделении в рамках них цифровых правоотношений, а также развитии его доктрины [3].

Очевидно, стоит констатировать, что современные цифровые технологии, сочетая в себе конвергентность, сквозной и прорывной характер для развития общества и государства, не только создают безграничные возможности, но и формируют новые вызовы и угрозы безопасности в процессе их внедрения и использования. Считаем, что рассматриваемые проблемы в праве свидетельствуют о том, что внедрение и развитие информационных технологий в определенной части порождают новые угрозы, которые еще более усилились в условиях геополитических изменений, следовательно, информационное общество и цифровизация права, во многом определили позиции информационного права как отдельного направления в отечественной юриспруденции, так и ведущей отрасли права, которая динамично и активно развивается в условиях формирования экономики данных, укреплению цифрового суверенитета и формированию независимой правовой

инфраструктуры, обеспечивающей устойчивость национальной информационной среды.

### **Постановка задачи**

В доктрине информационного права не раз акцентировалось внимание на том, что стратегический характер имеют задачи обеспечения государственного суверенитета в условиях цифровой трансформации; обеспечения безопасности в киберпространстве [4]. Вместе с тем особую значимость придается данной теме в философии права, теории и истории государства и права, А.Н. Савенков отмечает, что «в условиях... усиливающейся динамики развития информационного общества, «электронного государства», цифровой экономики, роста вызовов и угроз информационной безопасности особую роль играет формирование и реализация государственной политики, направленной на учет современных информационных тенденций развития всех сфер жизни общества и государства, выработку научно обоснованных, выверенных, взвешенных подходов регулирования новых информационных отношений» [5, с. 64].

Согласно анализу и обобщению положений Доктрины информационной безопасности Российской Федерации можно констатировать, что к современным угрозам информационной безопасности можно отнести противоправное создание монополий на формирование и распространение достоверной информации, включая создание условий для масштабного манипулирования информацией, дискриминации. Как подтверждение этому, одной из задач обеспечения информационной безопасности является формирование безопасной среды оборота достоверной информации, повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования, а также развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз<sup>3</sup>. Ряд указанных выше информационных угроз в последнее время приобрел особую значимость. Так, угроза создания монополий на формирование и распространение достоверной информации заключается в противоправной фильтрации информации для формирования враждебного по отношению к России информационно-коммуникационного пространства, которое впоследствии влияет на конкурентоспособность и безопасность государства в инновационной и информационной сфере. Современная повестка дня международной информационной безопасности

<sup>2</sup> Цифровая трансформация. Основные принципы, этапы и результаты реализации. URL: <https://roskachestvo.gov.ru/about/competence/digital/docs/standart.pdf> (дата обращения: 20.08.2026).

<sup>3</sup> П. 57 Указа Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

позволяет констатировать, что в отношении России ведется тотальная информационная и гибридная война, включая санкционную агрессию. В связи с этим можно утверждать, что при глобальной цифровой трансформации информация как непосредственный объект правоотношений перешла из разряда ресурсов в разряд средств враждебной деятельности. В связи с этим особое значение приобретает принцип достоверности информации как основа доверия между государствами.

Общепризнанные принципы международного права в исследуемой сфере деятельности нашли отражение и в резолюциях ООН, посвященных проблемам информационной безопасности и научно-техническому прогрессу<sup>4</sup>. Большинство принципов, закрепленных в международно-правовых документах, согласуются с документами стратегического планирования зарубежных государств и подчеркивают важность открытости и транспарентности деятельности государства в информационном пространстве, а также необходимости формирования глобальной культуры информационной безопасности. Рассматривая международно-правовые принципы, следует обратить внимание на принципы, закрепленные в Окинавской хартии глобального информационного общества, включая развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций<sup>5</sup>. Дальнейшее развитие принципов получило отражение в Декларации принципов (2003 г.), включая принцип укрепления доверия и безопасности при использовании цифровых технологий<sup>6</sup>. Из этого следует, что задекларированные принципы влияют на развитие правовых основ государства для цифровой доверительной среды, включая защиту информационно-технологических сетей и противодействие киберугрозам и киберпреступности. Как справедливо отмечает Т.А. Полякова, принципы права, обеспечивающие безопасность в информационной сфере на международном уровне, имеют устойчивый характер, однако необходима структурированная система данных принципов для эффективной реализации норм международного права в данной сфере<sup>7</sup>.

<sup>4</sup> Например, Резолюция 2450 (XXIII) Генеральной Ассамблеи ООН от 19 декабря 1968 г. «Права человека и научно-технический прогресс» // Официальный сайт ООН. URL: <https://undocs.org/ru/A/RES/2450%28XXIII%29> (дата обращения: 28.08.2026).

<sup>5</sup> Окинавская хартия глобального информационного общества (принята на о. Окинава 22 июля 2000 г.) // Дипломатический вестник. 2000. № 8. С. 51—56.

<sup>6</sup> Женевская Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии», принятая 12 декабря 2003 г. // Официальный сайт ООН. URL: [https://www.un.org/ru/events/pastevents/pdf/dec\\_ws1s.pdf](https://www.un.org/ru/events/pastevents/pdf/dec_ws1s.pdf) (дата обращения: 26.08.2026).

<sup>7</sup> Полякова Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3. С. 17.

## Решение поставленной задачи

Можем констатировать, что обеспечение достоверности информации можно рассматривать как составную часть состояния защищенности государства, ее информационные ресурсы и технологии. При этом ряд авторов рассматривает требование по обеспечению достоверности информации как составную часть наряду с конфиденциальностью при обеспечении информационной безопасности, в частности, видный ученый, доктор юридических наук Г.Г. Камалова делает вывод «...предоставление доверителем сведений, составляющих профессиональную тайну, обусловлено наличием доверия личного характера или связанного с особым профессиональным статусом субъекта профессиональной деятельности, что всегда предполагает, что обе стороны правоотношений в сфере профессиональной тайны рассчитывают на достоверность получаемой и сохраняемой информации» [6, с. 284]. Как отмечает О.В. Петровская, для обеспечения эффективного управления достоверность информации можно рассматривать как неотъемлемое условие и меру соблюдения конфиденциальности информации ограниченного доступа [7, с. 143]. В доктрине информационного права констатируется, что актуальность информации определяется ее постоянным обновлением, так называемой актуализацией состояния [8]. В этой связи справедливо ставится вопрос о том, что развитие принципа достоверности требует дополнительных исследований для совершенствования отечественного законодательства, в т. ч. по вопросам государственной тайны, персональных данных, кредитных историй и т. д. [9]. В этой связи полагаем возможным дополнительно закрепить принцип достоверности для обеспечения и проведения экспертизы в целях обеспечения информационной безопасности. В находящейся в процессе постоянной трансформации системе на многие социальные институты влияет постоянно усиливающийся информационный поток, новые способы и особенности сбора и обработки данных, а также отсутствие быстрой адаптивности к происходящим изменениям [10].

Следовательно, обеспечение достоверности информации прямо вытекает из требования обеспечения конфиденциальности сведений, относящихся к государственной тайне, в которых достоверность, рассматривается через категории точности, достаточности и актуальности информации. Следует отметить, важность принципа достоверности при правовом обеспечении информационной безопасности, т.к. он выступает базовым условием для реализации общественных отношений в сфере информационных технологий и обеспечения безопасности.

Из этого следует, что формирование и закрепление единых международных принципов и норм позволит реализовать в Стратегии национальной безопасности Российской Федерации принципы всеобщей, равной и неделимой безопасности, а также отдельные прин-



ципы, к примеру, исследуемый принцип достоверности, согласно которым безопасность отдельного независимого государства самостоятельна, тем самым другое государство не имеет право прямо или косвенно вмешиваться во внутренние или внешние дела, что актуально в сфере обеспечения международной информационной безопасности. Тем самым, обусловленность правовых принципов обеспечения информационной безопасности системой принципов информационного права и законодательства, которые закономерно привлекали внимание исследователей, отмечавших их дальнейшее развитие в связи с изменениями сферы регулируемых общественных отношений и трансформацией права в условиях цифровизации [11].

Таким образом, в условиях цифровизации усиливается зависимость эффективности правовой политики от информационных рисков. В связи с этим Г. Бехманн отмечает характерную для информационного общества фундаментальную дихотомию между стремлением к устойчивому развитию и ростом риска [12]. Российские ученые сходятся во мнении, что вопросы информационной безопасности являются столь же важными, как вопросы ядерной сферы и это делает их ключевым фактором стратегической стабильности государства [13, с. 135]. Следовательно, информационная сфера, на сегодняшний день, неизбежно способствует дестабилизации общества и манипулированию общественным и индивидуальным сознанием. Учитывая пребывание информационного пространства в непрерывном состоянии неопределенности и опасности, а также информационный характер любых рисков, для обеспечения информационной безопасности нужен надлежащий государственный механизм, который обеспечит постоянное и бесперебойное противодействие информационным угрозам в современных условиях социально-экономических и геополитических рисков при фундаментальной трансформации мира.

Считаем, что одной из задач в области обеспечения международной информационной безопасности является развитие обеспечения достоверности с позиции защиты от распространения ложной и недостоверной информации как масштабной и серьезной информационной угрозы не только на национальном (внутригосударственном), но и на международном уровне, в этой связи необходимо принять универсальный документ, закрепляющий в качестве одной из таких основных угроз распространение недостоверной информации, которая приводит к дестабилизации международного мира, безопасности и стабильности. Данные попытки уже осуществлялись, в частности, в Концепции Конвенции ООН об обеспечении международной информационной безопасности, в числе угроз и факторов информационной безопасности были указаны: публичное распространение под видом достоверных сообщений заведомо ложной информации, приводящее к возникновению

угрозы жизни и безопасности граждан или к наступлению тяжких последствий; невозможность точной идентификации источника компьютерных атак или ложной информации, обусловленная технологическими особенностями информационно-коммуникационных технологий, а также отсутствием организационных механизмов обеспечения деанонимизации информационного пространства<sup>8</sup>. Однако в 2024 году была принята Конвенция ООН против киберпреступности, укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, в данном нормативно-правовом акте вышеуказанные угрозы отсутствуют и принцип достоверности не закреплен в качестве универсального положения, который бы определял содержание и направленность правового регулирования общественных отношений, тем самым, отсутствие четкого закрепления принципа достоверности порождает правовые неопределенности в сфере правового обеспечения информационной безопасности и повышает риски распространения недостоверной информации в цифровой среде.

Как справедливо отмечает А.В. Крутских, Россия исторически выступает как государство, которое стремится объединить и укрепить международное сотрудничество в сфере информационной безопасности, в том числе путем выработки правил, норм, принципов ответственного поведения государств, сегодня важно придать нормам об ответственном поведении в киберсреде обязательный характер, поскольку угрозы в информационной среде носят глобальный характер, поэтому поиск решения проблем должен носить универсальный характер<sup>9</sup>.

Юридическое сообщество в лице доктрины информационного и международного права, законодателя и других субъектов права с законодательной инициативой должны выработать подходы к формированию единых стандартов и требований к безопасности в информационной среде, которые, в свою очередь, должны определять состояние защищенности информационной инфраструктуры и противодействие распространению недостоверной информации.

<sup>8</sup> Обновленная Концепция Конвенции ООН об обеспечении международной информационной безопасности // Официальный сайт Совета Безопасности Российской Федерации. URL: <http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAACATW2Rwa3yNK1bNAWI9.pdf> (дата обращения: 26.08.2026).

<sup>9</sup> Крутских А.В. Геополитические аспекты глобального использования ИКТ // Инфофорум. URL: <https://infoforum.live/> (дата обращения: 30.08.2026).

## Выводы

Таким образом, анализ современного состояния правового обеспечения информационной безопасности свидетельствует о том, что отсутствия универсальных международных нормативно-правовых актов, закрепляющих принципы обеспечения кибербезопасности, не позволяет в полной мере развивать правовые средства обеспечения безопасности в информационной среде. Констатируя отсутствия спе-

циального стратегического регулирования по данному вопросу, важно обратить внимание на принцип достоверности как важного элемента по противодействию новых угроз и рисков, поскольку достоверность информации выступает как особое требование в целях обеспечения информационной безопасности, так как одним из условий обеспечения безопасности в информационной среде является гарантия достоверности, в том числе целостности и точности информации.

## Литература

1. Троян Н.А. О некоторых вопросах применения искусственного интеллекта в государственном управлении в условиях цифровой трансформации: правовые аспекты // Правовая информатика. 2026. № 2. С. 164—171.
2. Савенков А.Н. Российское государство-цивилизация и его беспримерный подвиг в обеспечении мира и безопасности человечества: к 80-летию Победы в Великой Отечественной войне // Государство и право. 2025. № 5. С. 7—15.
3. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75—87.
4. Polyakova T.A., Naumov V.B., Minbaleev A.V. Trust in the law during the digital transformation // Государство и право. 2022. № 11. С. 139—147.
5. Савенков А.Н. Философия права и становление российского государства-цивилизации. М., 2024. 739 с.
6. Камалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: дис. ... д-ра юрид. наук. М.: Институт государства и права РАН, 2020. 472 с.
7. Петровская О.В. Принцип достоверности в информационном праве: дис. ... к-та юрид. наук. М.: Институт государства и права РАН, 2022. 204 с.
8. Полякова Т.А., Камалова Г.Г. Концептуальные основания развития института доступа к информации в Российской Федерации при применении цифровых технологий // Мониторинг правоприменения. 2020. № 4 (37). С. 22—27.
9. Полякова Т.А. Влияние цифровой трансформации на развитие информационного права: тенденции, проблемы, перспективы // Мониторинг правоприменения. 2020. № 2 (35). С. 53—58.
10. Петровская О.В. Цифровая трансформация и проблемы обеспечения достоверности информации // Аграрное и земельное право. 2020. № 3 (183). С. 130—132.
11. Чубукова С.Г. Внутриотраслевые принципы обработки генетической информации // Актуальные проблемы российского права. 2019. № 5 (102). С. 98—110.
12. Букалерева Л.А., Лапшин В.Ф., Остроушко А.В. Риск-ориентированный подход в области правового регулирования обеспечения информационной безопасности несовершеннолетних // Вестник Сургутского государственного университета. 2021. № 1 (31). С. 76—83.
13. Савенков А.Н. Государство и право в период кризиса современной цивилизации. М., 2020. 448 с.

SECTION:  
REGULATORY INFORMATICS

## THE PRINCIPLE OF INFORMATION RELIABILITY IN THE FIELD OF INFORMATION SECURITY: THEORETICAL AND LEGAL ASPECTS

Duben A.K.<sup>10</sup>

<sup>10</sup> Andrei K. Duben, Ph.D. (Law), Senior Researcher at the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia. E-mail: k.duben@mail.ru

**Keywords:** digitalization, information technologies, transformation of law, information law, challenges and threats, information security, principles of law, theory of law, philosophy of law.

#### **Abstract**

**The aim of the work** is to analyse modern and pressing issues related to the legal provision of information security at the national and international levels. Justification of theoretical provisions aimed at determining the place and role of the principle of information reliability as an important element in countering new threats and risks in the system of information and international law.

**The following general scientific methods:** analysis and synthesis, abstraction and modelling, generalization, description, classification, etc. Special private-law methods of cognition were also used: comparative legal, formal-legal, etc.

**The results of the study.** In the context of the development of the information society, the role of research examining the principles of legal regulation of social relations — using information security as an example of a specific sub-branch of law — is growing. The necessity of legally enshrining the principle of information reliability in international regulatory legal acts in the field of ensuring information security is substantiated; it is also necessary to develop approaches to forming unified standards and requirements for security in the information environment, which will make it possible to determine the state of protection of information infrastructure and counteract the spread of unreliable information. Noting the absence of special strategic regulation on this issue, it is important to pay attention to the principle of reliability as an important element in countering new threats and risks. At the same time, ensuring the reliability of information should be considered an integral part of the state's security status, along with its information resources and technologies. Consequently, the information sphere today inevitably contributes to the destabilization of society and the manipulation of public and individual consciousness. Given that the information space is in a continuous state of uncertainty and danger, as well as the informational nature of any risks, ensuring information security requires an appropriate state mechanism that will provide continuous and uninterrupted counteraction to information threats in the current context of socio-economic and geopolitical risks amid the fundamental transformation of the world.

#### **References**

1. Troian N.A. O nekotorykh voprosakh primeneniia iskusstvennogo intellekta v gosudarstvennom upravlenii v usloviakh tsifrovoy transformatsii: pravovye aspekty // Pravovaia informatika. 2026. No. 2. S. 164—171.
2. Savenkov A.N. Rossiiskoe gosudarstvo-tsivilizatsiia i ego besprimernyi podvig v obespechenii mira i bezopasnosti chelovechestva: k 80-letiiu Pobedy v Velikoi Otechestvennoi voine // Gosudarstvo i pravo. 2025. No. 5. S. 7—15.
3. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Novye vektory razvitiia informatsionnogo prava v usloviakh tsivilizatsionnogo krizisa i tsifrovoy transformatsii // Gosudarstvo i pravo. 2020. No. 5. S. 75—87.
4. Polyakova T.A., Naumov V.B., Minbaleev A.V. Trust in the law during the digital transformation // Gosudarstvo i pravo. 2022. No. 11. S. 139—147.
5. Savenkov A.N. Filosofia prava i stanovlenie rossiiskogo gosudarstva-tsivilizatsii. M., 2024. 739 s.
6. Kamalova G.G. Pravovoe obespechenie konfidentsial'nosti informatsii v usloviakh razvitiia informatsionnogo obshchestva: dis. ... d-ra iurid. nauk. M. : Institut gosudarstva i prava RAN, 2020. 472 s.
7. Petrovskaia O.V. Printsip dostovernosti v informatsionnom prave: dis. ... k-ta iurid. nauk. M. : Institut gosudarstva i prava RAN, 2022. 204 s.
8. Poliakova T.A., Kamalova G.G. Kontseptual'nye osnovaniia razvitiia instituta dostupa k informatsii v Rossiiskoi Federatsii pri primenении tsifrovyykh tekhnologii // Monitoring pravoprimereniia. 2020. No. 4 (37). S. 22—27.
9. Poliakova T.A. Vliianie tsifrovoy transformatsii na razvitie informatsionnogo prava: tendentsii, problemy, perspektivy // Monitoring pravoprimereniia. 2020. No. 2 (35). S. 53—58.
10. Petrovskaia O.V. Tsifrovaia transformatsiia i problemy obespecheniia dostovernosti informatsii // Agrarnoe i zemel'noe pravo. 2020. No. 3 (183). S. 130—132.
11. Chubukova S.G. Vnutriotraslevye printsipy obrabotki geneticheskoi informatsii // Aktual'nye problemy rossiiskogo prava. 2019. No. 5 (102). S. 98—110.
12. Bukalerovala L.A., Lapshin V.F., Ostroushko A.V. Risk-orientirovannyi podkhod v oblasti pravovogo regulirovaniia obespecheniia informatsionnoi bezopasnosti nesovershennoletnikh // Vestnik Surgutskogo gosudarstvennogo universiteta. 2021. No. 1 (31). S. 76—83.
13. Savenkov A.N. Gosudarstvo i pravo v period krizisa sovremennoi tsivilizatsii. M., 2020. 448 s.



# ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И КРЕДИТНЫХ ОРГАНИЗАЦИЙ

Иванов Н.Ю.<sup>1</sup>

**Ключевые слова:** правовое регулирование, государственные информационные системы, кредитные организации, информационная безопасность, критическая информационная инфраструктура, защита персональных данных, доступ пользователей, экспериментальный правовой режим, частно-государственное партнерство.

## **Аннотация**

**Цель работы.** Состоит в разработке предложений по совершенствованию организационно-правового обеспечения информационной безопасности при взаимодействии государственных ГИС и кредитных организаций на основе научного анализа тенденций развития нормативно-правовой базы.

**Метод исследования.** Методологическую основу исследования составляет комплекс общенаучных и специальных юридических методов. С помощью анализа и синтеза удалось выявить основные тенденции правового регулирования информационной безопасности при взаимодействии ГИС и кредитных организаций. Логический метод послужил инструментом при формулировании выводов и рекомендаций.

**Результаты исследования.** Для дальнейшего совершенствования данного режима предлагается обеспечить унификацию требований к информационной безопасности различных регуляторов (ФСБ, ФСТЭК, Банк России, Роскомнадзор) путем разработки межведомственных и комплексных стандартов и издания совместных нормативных правовых актов, специально предназначенных для правового регулирования деятельности ГИС при взаимодействии с кредитными организациями, а также стимулировать развитие частно-государственного партнерства в области обмена информацией о кибератаках, законодательно закрепив для его участников правовые гарантии конфиденциальности передаваемых данных, упростив порядок подключения частных владельцев объектов критической инфраструктуры к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Доказана необходимость модернизации правового регулирования экспериментальных правовых режимов на финансовом рынке, в том числе в области информационной безопасности путем внесения изменений в Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации».

Установлено, что для усиления информационной безопасности при взаимодействии ГИС и кредитных организаций может потребоваться внести изменения в 28 главу Уголовного кодекса Российской Федерации в части ужесточения уголовной ответственности за неосторожные преступления в сфере компьютерной информации, а также предусмотреть дополнительную административную и дисциплинарную ответственность.

DOI: 10.24412/1994-1404-2026-3-00-29

---

<sup>1</sup> **Иванов Николай Юрьевич**, аспирант кафедры фундаментальной юриспруденции и международного права Российского университета адвокатуры и нотариата имени Г.Б. Мирзоева, г. Москва, Российская Федерация.  
E-mail: nj\_ivanov@mail.ru



## **Введение**

**В** соответствии с национальными целями развития Российской Федерации, определенными Президентом Российской Федерации<sup>2</sup>, перед Правительством Российской Федерации поставлена амбициозная задача: к 2030 году обеспечить «цифровую зрелость» в сфере государственного и муниципального управления, а также в ключевых отраслях экономики и социальной сферы. Для оценки прогресса в решении этой задачи правительство включило в систему индикаторов преимущественно показатели, отражающие долю пользователей различных ГИС<sup>3</sup>. Актуальной проблемой государственного управления остается организация взаимодействия ГИС и кредитных организаций при соблюдении требований информационной безопасности.

В Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»<sup>4</sup> Федеральным законом от 07.04.2025 № 58-ФЗ<sup>5</sup> внесены существенные изменения по совершенствованию правового режима информационной безопасности ГИС прежде всего в банковской деятельности, которые потребовали от регуляторов значительно обновить их нормативную базу в указанной сфере (Банк России, ФСБ, ФСТЭК, Роскомнадзор).

В настоящее время государственные информационные системы (ГИС) активно используются кредитными организациями в целях поиска клиентов, идентификации, проверки, экспертизы клиентов и их бизнеса, мониторинга финансового состояния клиентов, осуществления мероприятий в целях сбора просроченной задолженности, а также во множестве других операций и действий, как предусмотренных законодательством в качестве обязательных, так и выполняемых банками по собственному усмотрению.

1 августа 2026 года на портале «Госуслуги» стартовал эксперимент по получению гражданами социальных льгот через их банковскую карту, сообщил Председатель Правительства Российской Федерации М.В. Мишустин на оперативном совещании со своими заместителями<sup>6</sup>. В сфере предоставления гражданам

различных льгот начинается взаимодействие портала государственных услуг с платежной системой «МИР».

За период в 10—15 лет кредитные организации существенно расширили доступ к необходимой информации — появилась возможность оперативно запрашивать и получать нужные данные из ГИС. Параллельно происходило совершенствование законодательной базы, направленное на повышение прозрачности и открытости данных. Однако внедрение новых правовых норм выявило ряд серьезных проблем: утечки персональных данных и их последующее использование злоумышленниками; злоупотребление режимом коммерческой тайны в целях недобросовестной конкуренции; отмывание денег и финансирование терроризма (ОД/ФТ) как угрозы национальной безопасности; иные формы неправомерного использования информации.

В ответ на эти вызовы государство приняло комплекс мер: были разработаны новые правовые нормы, а действующие положения существенно ужесточены. В результате публичный доступ к ряду категорий информации оказался ограничен. В настоящее время на фоне контрсанкционной политики наблюдаются беспрецедентные шаги государства по ужесточению законодательства в области доступности информации, все новые и новые сведения и правоотношения подпадают под понятие информации ограниченного доступа.

Таким образом, доступность и открытость сведений ГИС, используемых кредитными организациями, с одной стороны, должны сочетаться с необходимостью защиты ГИС в кредитно-финансовой сфере, как объектов критической инфраструктуры. Обозначенные проблемы определяют одновременно сложность и важность указанных правоотношений для развития экономики, вследствие чего представляет научный интерес изучение проблематики перспективных направлений правового регулирования обеспечения информационной безопасности при взаимодействии ГИС и кредитных организаций.

## **Сложный многоуровневый институт**

Эффективное взаимодействие ГИС и кредитных организаций невозможно без создания надежной системы защиты информации. Обеспечение информационной безопасности этих систем является не просто технической задачей, но сложной правовой проблемой. Их правовой режим находится на стыке информационного, административного и финансового права, что порождает специфическую систему регулирования, характеризующуюся высокой степенью императивности, комплексностью и наличием перекрестных требований различных регуляторов.

Правовое регулирование взаимодействия ГИС и кредитных организаций при соблюдении требований информационной безопасности Российской Федерации представляет собой сложный многоуровневый институт. Федеральный закон от 27.07.2006 № 152-ФЗ

<sup>2</sup> Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собрание законодательства РФ. 13.05.2024, № 20, ст. 2584.

<sup>3</sup> Постановление Правительства РФ от 28.01.2025 № 58 «Об утверждении методик расчета показателей для оценки эффективности деятельности высших должностных лиц субъектов Российской Федерации и деятельности исполнительных органов субъектов Российской Федерации» // Собрание законодательства РФ. 17.02.2025, № 7, ст. 605.

<sup>4</sup> Собрание законодательства РФ. 31.07.2017. № 31. (Часть I). Ст. 4736.

<sup>5</sup> Собрание законодательства РФ. 14.04.2025, № 15, ст. 1784.

<sup>6</sup> Правительство утвердило параметры эксперимента по использованию платежных карт «Мир» для предоставления отдельных мер соцзащиты // Портал Правительства России. URL: <http://government.ru/docs/59432> (дата обращения: 15.08.2026).

«О персональных данных»<sup>7</sup> устанавливает императивные требования к конфиденциальности обработки персональных данных, определяя организационные и технические меры, обязательные для реализации операторами, к категории которых в полной мере относятся кредитные организации.

При этом пользователь ГИС, действуя от имени и в интересах оператора персональных данных, становится конечным исполнителем данных требований, и его действия по вводу, просмотру, модификации или передаче персональных данных в рамках взаимодействия с ГИС получают правовую оценку в контексте соблюдения установленных законом процедур.

Не менее значимую роль играет Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»<sup>8</sup>, который возлагает на кредитные организации обязанность по защите информации, связанной с финансовыми операциями клиентов, составляющей предмет банковской тайны. Доступ к таким сведениям через ГИС, например, при взаимодействии с Росфинмониторингом, обуславливает повышенную ответственность пользователя, поскольку утечка или искажение данной информации могут парализовать работу по противодействию противоправным финансовым потокам.

Особый правовой режим устанавливается Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»<sup>9</sup>, который относит банковскую и иную финансовую инфраструктуру к объектам критической информационной инфраструктуры.

Правовой статус банковской тайны, как краеугольного камня доверия в финансовой системе, закреплен в статье 26 Федерального закона «О банках и банковской деятельности»<sup>10</sup>, где раскрывается ее содержание и круг субъектов, обязанных обеспечивать ее конфиденциальность. Пользователь, получая доступ к информации, составляющей банковскую тайну, через ГИС, принимает на себя бремя соблюдения данного режима, и его противоправные действия по разглашению таких сведений подпадают под действие не только административного, но и уголовного законодательства.

Уголовный кодекс Российской Федерации в статье 183 предусматривает санкцию за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. При этом уголовная ответственность может наступить, не только когда мотивом нарушения послужили корыстные цели или в результате хищения документов, но и в результате сбора информации, например, для предоставления в суд, когда такие действия нарушают правовой ре-

жим охраняемой законом тайны<sup>11</sup>, а также требования локальных нормативных актов организации, должностных инструкций<sup>12</sup>.

### Нарушение административного законодательства Российской Федерации в области защиты персональных данных

Законодатель не скрывает свои намерения по усилению мер административного воздействия в рассматриваемой области. Кодекс Российской Федерации об административных правонарушениях<sup>13</sup> содержит отдельный состав, непосредственно касающийся сферы персональных данных — статья 13.11, которая устанавливает административную ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Санкции по данной статье регулярно ужесточаются, а практика их применения расширяется, что свидетельствует о повышенном внимании законодателя и контролирующих органов к данному вопросу.

Примером может служить Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»<sup>14</sup>, который дополнил статью 13.11 КоАП РФ новыми составами административных правонарушений, предусматривающими установление административной ответственности за утечки баз данных, содержащие персональные данные.

Как отмечалось в пояснительной записке к законопроекту, такие меры административного наказания станут существенным стимулом для инвестиций операторов персональных данных в информационную безопасность и окажут превентивное воздействие на операторов, не соблюдающих требования законодательства о персональных данных<sup>15</sup>. Для пользователя информационной системы это означает, что даже техническая ошибка, приведшая к неправомерному распространению персональных данных, может стать основанием для привлечения к административной ответственности с наложением существенного штрафа.

<sup>11</sup> Кассационное определение Четвертого кассационного суда общей юрисдикции от 11.11.2020 № 77-2402/2020 (УИД 23RS0031-01-2019-012379-77) // СПС «КонсультантПлюс».

<sup>12</sup> Определение Восьмого кассационного суда общей юрисдикции от 05.10.2021 по делу № 77-4019/2021 (УИД 42RS0009-01-2020-004129-23) // СПС «КонсультантПлюс».

<sup>13</sup> Собрание законодательства РФ. 07.01.2002, № 1 (ч. 1), ст. 1.

<sup>14</sup> Собрание законодательства РФ. 02.12.2024, № 49 (часть IV), ст. 7411.

<sup>15</sup> Пояснительная записка к проекту Федерального Закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество»). URL: <https://sozd.duma.gov.ru> (дата обращения: 21.10.2025).

<sup>7</sup> Собрание законодательства РФ. 31.07.2006, № 31 (1 ч.), ст. 3451.

<sup>8</sup> Собрание законодательства РФ. 13.08.2001, № 33 (часть I), ст. 3418.

<sup>9</sup> Собрание законодательства РФ. 31.07.2017, № 31 (часть I), ст. 4736.

<sup>10</sup> Собрание законодательства РФ. 05.02.1996, № 6, ст. 492.

### **Нормативное регулирование Банка России**

Наряду с федеральным законодательством, существенную регуляторную нагрузку несут нормативные акты Банка России, которые, обладая силой подзаконных актов, фактически выполняют роль прямых руководящих указаний для кредитных организаций. В частности, Положение Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»<sup>16</sup> детализирует технические и организационные стандарты безопасности.

Стандарт Банка России СТО БР ИББС-1.0-2014<sup>17</sup>, принятые на его основе методические рекомендации Банка России<sup>18</sup> и иные стандарты<sup>19</sup>, хотя и носящие рекомендательный характер, де-факто являются эталоном при построении систем защиты информации в банках. Внутренние (локальные) нормативные акты кредитной организации — Политика информационной безопасности, регламенты доступа в ГИС, должностные инструкции — завершают эту многоуровневую конструкцию. Их юридическое значение заключается в том, что они конкретизируют общие законодательные предписания применительно к специфике конкретного банка и рабочих мест. Ознакомление пользователя с этими документами под подпись является юридически значимым действием, преобразующим общие обязанности, вытекающие из закона, в конкретные трудовые функции. В случае возникновения инцидента именно соответствие или несоответствие действий пользователя положениям внутренних инструкций будет служить первоначальным доказательством при установлении его вины.

### **Структура правового регулирования информационной безопасности при взаимодействии ГИС и кредитных организаций**

Правовое регулирование информационной безопасности при взаимодействии ГИС и кредитных организаций представляет собой сложную, иерархически

организованную систему, которую можно структурировать на четыре основных уровня.

1) Конституционный уровень. Основопологающие принципы, такие как право на тайну частной жизни, личную и семейную тайну (ст. 23 Конституции РФ), право на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 24 Конституции РФ), формируют фундамент для всего последующего регулирования.

2) Уровень федерального законодательства. Данный уровень включает в себя кодифицированные акты и федеральные законы, устанавливающие общие рамки:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: определяет базовые понятия, общие принципы обеспечения информационной безопасности;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: устанавливает обязательные требования к обработке персональных данных, которые в большом объеме обрабатываются в ГИС и информационных системах кредитных организаций;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»: ключевой акт, поскольку большинство ГИС и информационных систем кредитных организаций отнесены к объектам КИИ. Закон вводит особый режим безопасности, включая обязательную категоризацию объектов, их аттестацию и установление особых правил эксплуатации;
- Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»: наделяет Банк России нормотворческими полномочиями по установлению правил осуществления банковских операций, стандартов защиты информации;
- Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»: регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием и защитой, что актуально для некоторых сегментов ГИС финансового блока.

3) Уровень подзаконных нормативных правовых актов. На этом уровне конкретизируются требования законов. Ключевую роль здесь играют акты Банка России (Указания, Положения, Стандарты), ФСБ России, ФСТЭК России, устанавливающие:

- требования к системе защиты информации (СЗИ);
- порядок проведения оценки соответствия и аттестации;
- методики оценки ущерба и категорирования объектов КИИ;

<sup>16</sup> «Вестник Банка России», № 76, 21.12.2023.

<sup>17</sup> «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014» // «Вестник Банка России», № 48-49, 30.05.2014.

<sup>18</sup> Например, «Методические рекомендации Банка России по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка» (утв. Банком России 22.01.2025 № 2-МР) // «Вестник Банка России», № 7, 31.01.2025.

<sup>19</sup> Например, «Стандарт Банка России „Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect. Требования“ СТО БР ФАПИ.СЕК-1.6-2024» (принят и введен в действие приказом Банка России от 07.10.2024 № ОД-1615). URL: <https://cbr.ru> (дата обращения: 23.10.2025).

- технические стандарты и рекомендации по защите (например, серия руководящих документов ФСТЭК<sup>20</sup>).

4) Уровень международных стандартов и лучших практик. Несмотря на национальную специфику, при построении систем защиты активно применяются международные стандарты (ISO/IEC 27001, серия COBIT, PCI DSS), которые адаптируются к требованиям российского законодательства.

### Особенности правового режима информационных систем Банка России

Банк России выступает в этих правоотношениях и как мегарегулятор финансового рынка, устанавливающий обязательные для всех кредитных организаций требования, и как оператор собственных критически важных информационных систем. Эта двойственность определяет особенности правового режима его информационных систем.

Во-первых, информационные системы Банка России обрабатывают информацию, отнесенную к категории конфиденциальной, а в некоторых случаях — и к государственной тайне (например, сведения о золотовалютных резервах, планах по денежной эмиссии). Это влечет необходимость соблюдения не только требований ФЗ-187, но и строгого режима Закона «О государственной тайне», включая лицензирование деятельности по защите сведений и особый порядок допуска сотрудников.

Во-вторых, Банк России обладает нормотворческой автономией в установлении требований к безопасности своих систем. Он издает внутренние нормативные акты (например, Стандарт Банка России СТО БР ИББС-1.0), которые де-факто являются обязательными для исполнения его подразделениями и устанавливают эталон для всей банковской системы.

В-третьих, на Банк России возложены функции национального координатора по защите прав потребителей финансовых услуг и обеспечению стабильности финансового рынка. Сбой в работе его информационных систем (например, системы БЭСП) может привести к системному риску для всей национальной экономики, что предъявляет экстраординарные требования к отказоустойчивости, бесперебойности и доступности этих систем.

### Проблемы правового регулирования информационной безопасности ГИС при взаимодействии с кредитными организациями

Несмотря на развитую нормативную базу, в научной и экспертной среде все чаще обращается внимание на ряд системных проблем в правовом регулировании информационной безопасности ГИС при взаимодействии с кредитными организациями:

Во-первых, это дублирование и пересечение требований. О необходимости ликвидации устаревших положений, пробелов и дублирования норм в законодательстве, которые приводят не только к появлению противоречащих друг другу нормативных правил в области информационной безопасности, но и к пересечению контрольных функций органов власти в своих работах пишут такие крупные ученые, как профессор В.А. Вайпан [1], С.М. Зырянов [2].

Оператор ГИС, являющейся объектом КИИ и обрабатывающей персональные данные, вынужден одновременно выполнять зачастую разнонаправленные требования ФСБ, ФСТЭК, Роскомнадзора и Банка России. Это приводит к значительному росту финансовой и административной нагрузки. В то же время некоторые ученые считают возможным утверждать о наметившейся тенденции по унификации требований информационной безопасности [3].

Второй проблемой можно выделить проблему атрибуции киберинцидентов. Действующее законодательство не в полной мере регулирует процедуру официального установления виновных лиц в случае кибератаки на ГИС, что затрудняет привлечение их к ответственности и применение мер международного правового характера. С учетом повсеместного применения информационных технологий и повышением доступности их использования также повышаются возможности противоправного и злонамеренного их использования, в результате чего проблема атрибуции подобных атак становится наиболее актуальной. В этой связи А.Ж. Мартиросян считает необходимым принцип атрибуции кибератак возвести в специальный принцип новой отрасли права — международного информационного права [4].

В-третьих, жесткие технические требования зачастую не подкреплены адекватными нормами, стимулирующими повышение киберграмотности и личной ответственности сотрудников, имеющих доступ к ГИС. Профессор Е.Н. Клещина считает нехватку квалифицированных кадров в области информационной безопасности одной из проблем предупреждения преступлений, совершаемых работниками банков посредством информационных технологий [5].

Некоторые ученые полагают недостаточной только лишь уголовную ответственность за нарушение требований о безопасности критической информационной инфраструктуры Российской Федерации. Так, в частности, Д.Д. Савенкова в своей диссертации доказывает необходимость введения также административной

<sup>20</sup> Например, приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований по защите информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, дата обращения: 24.09.2025.



и дисциплинарной ответственности субъектов критической информационной инфраструктуры за нарушение порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [6].

Правительство и Банк России уделяют повышенное внимание внедрению правовых актов, посвященных повышению финансовой и инвестиционной грамотности, финансовой киберграмотности, формированию основ финансовой культуры и рационального поведения.

Была принята Стратегия повышения финансовой грамотности и формирования финансовой культуры до 2030 г.<sup>21</sup>, разработаны и одобрены Советом директоров Банка России «Основные направления развития финансового рынка Российской Федерации на 2024 год и период 2025 и 2026 годов»<sup>22</sup>. Однако профессор Н.А. Поветкина [7] отмечает в этих документах разнонаправленный, несистемный способ формирования и закрепления правового категориального аппарата.

Четвертой проблемой является быстрое устаревание нормативной базы. Скорость развития новых цифровых явлений, в том числе киберугроз опережает скорость законодательного процесса [8, 9]. Как отмечает А.К. Дубень [10], «современная национальная система правового обеспечения информационной безопасности в Российской Федерации, включая правовое регулирование, пока не в полной мере соответствует вызовам и рискам современности, в целом развивается недостаточно системно, без учета особенностей деятельности средств и методов защиты информации, включая и экспериментальные правовые режимы в сфере цифровых инноваций». Технические требования, закрепленные в подзаконных актах, могут устаревать к моменту их вступления в силу, что снижает их эффективность. Некоторые ученые отмечают также необходимость своевременного определения в нормативных актах государственных регуляторов вводимых новых терминов для их применения в решении практических задач при использовании современных информационных технологий в обстановке усложнения угроз информационной безопасности [11].

### **Выводы и предложения по правовому регулированию информационной безопасности ГИС при взаимодействии с кредитными организациями**

Правовое регулирование информационной безопасности ГИС при взаимодействии с кредитными организациями представляет собой динамично раз-

вивающуюся, сложносоставную область. Ее ключевой особенностью является формирование специализированного правового режима, основанного на принципах максимальной защищенности, бесперебойности и подчинения строгому государственному контролю.

Для дальнейшего совершенствования данного режима представляется целесообразным следующее.

1) Обеспечить унификацию требований к информационной безопасности различных регуляторов (ФСБ, ФСТЭК, Банк России, Роскомнадзор). Сложность анализа «разнородных нормативных требований» и необходимость их интеграции в единую систему управления рисками информационной безопасности отмечается учеными экономистами, которые предлагают для систематизации законодательных норм внедрить матрицу риск-ориентированной интерпретации нормативных требований [12]. С правовой точки зрения, представляется, что для решения этих задач усилия должны быть направлены на разработку межведомственных и комплексных стандартов и издания совместных нормативных правовых актов, специально предназначенных для правового регулирования деятельности ГИС при взаимодействии с кредитными организациями. Необходимо отметить, что возможность издания нормативных правовых актов совместно несколькими федеральными органами исполнительной власти, а также Банком России совместно с федеральными органами исполнительной власти предусмотрена пунктом 3 «Правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации»<sup>23</sup>, и пунктом 14.1 Положения Банка России от 22.09.2017 № 602-П «О Правилах подготовки нормативных актов Банка России»<sup>24</sup>, однако, представляется, что в отсутствие законодательного требования об обязательности издания совместных нормативных правовых актов при межотраслевом регулировании такое опциональное правило не будет востребовано органами исполнительной власти, так как сопряжено с необходимостью межведомственного взаимодействия, создания рабочих групп, применения согласительных процедур, переговоров и прочих действий, которые сопряжены с риском трудно прогнозируемых результатов и нарушения плановых сроков внедрения нового регулирования.

2) Стимулировать развитие частно-государственного партнерства в области обмена информацией о кибератаках, закрепив для его участников правовые гарантии конфиденциальности передаваемых данных, упростив порядок подключения частных владельцев объектов критической инфраструктуры к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак,

<sup>21</sup> Распоряжение Правительства РФ от 24 октября 2023 г. № 2958-р «Об утверждении Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года» // Собрание законодательства РФ. 2023. № 45. Ст. 8091.

<sup>22</sup> «Вестник Банка России», № 5, 23.01.2024.

<sup>23</sup> Утверждены Постановлением Правительства Российской Федерации от 13.08.1997 № 1009 // Собрание законодательства РФ. 18.08.1997, № 33, ст. 3895.

<sup>24</sup> «Вестник Банка России», № 84, 29.09.2017.

создаваемой в целях предотвращения и устранения последствий компьютерных атак на критическую информационную инфраструктуру Российской Федерации (ГосСОПКА).

Следует отметить, что механизм взаимодействия кредитных организаций с регулирующими органами при выявлении компьютерных инцидентов, инцидентов защиты информации подробно урегулирован. При выявлении инцидентов кредитная организация в соответствии с пунктом 1 части 2 статьи 9 Федерального закона № 187-ФЗ направляет в Банк России с использованием технической инфраструктуры Банка России уведомление, содержащее сведения о выявленном инциденте, по форме и в порядке, установленным СТО БР БФБО-1.5-2023<sup>25</sup>, а также в Национальный координационный центр по компьютерным инцидентам (далее — НКЦКИ) по форме и в порядке, установленным приказом ФСБ России № 282<sup>26</sup>.

При этом в том случае, если кредитной организацией ранее было принято решение направлять информацию об инцидентах в НКЦКИ посредством Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России, дополнительное информирование НКЦКИ о данных событиях не требуется. Однако с учетом постоянно увеличивающегося количества субъектов рассматриваемых правоотношений и роста разнообразия оказываемых ими услуг звучат призывы расширить область применения режима взаимодействия кредитных организаций контролирующими органами.

3) Модернизировать правовое регулирование экспериментальных правовых режимов на финансовом рынке, в том числе в области информационной безопасности путем внесения изменений в Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации»<sup>27</sup> (далее — Закон об ЭПР). На портале Банка России размещена информация о поступлении всего двух инициативных предложений об установлении экспериментального правового режима по направлению «финансовый рынок». Одно из них было от-

клонено, второе рассматривается с мая 2026 года<sup>28</sup>. Банк России все еще только планирует внести изменение в законодательство с тем, чтобы появилась возможность изменять или исключать действие отдельных положений федеральных законов, что необходимо в целях создания правовых условий для пилотирования цифровых финансовых инноваций [13]. Однако, помимо этого, уже также очевидна необходимость дебюрократизации порядка и сокращения установленных Законом об ЭПР сроков рассмотрения инициатив по установлению ЭПР, в том числе в сфере информационной безопасности.

Реализация этих мер будет способствовать повышению устойчивости к современным угрозам информационной безопасности не только ГИС при взаимодействии с кредитными организациями, но и всей национальной финансовой системы.

4) Для укрепления информационной безопасности при взаимодействии ГИС и кредитных организаций необходимо внести изменения в главу 28 Уголовного кодекса Российской Федерации в части ужесточения уголовной ответственности за неосторожные преступления в сфере компьютерной информации, повлекшие значительный ущерб, а также предусмотреть административную и дисциплинарную ответственность, в том числе за нарушение порядка представления информации в систему ГосСОПКА. Безусловно решению современных вызовов информационной безопасности и уязвимостей ГИС могут способствовать такие предлагаемые учеными меры, как принятие новой Доктрины информационной безопасности [14], однако, по нашему мнению, более действенным будет кодификация многочисленных, зачастую разнополярных правовых актов, регулирующих информационные правоотношения и превращение Федерального Закона «Об информации...» № 149-ФЗ с его 70 изменениями и дополнениями в Информационный Кодекс с учетом значительного числа законодательных актов информационного права при взаимном проникновении правовых норм «финтеха» с включением отдельной главы, посвященной ответственности субъектов информационно-правовых отношений.

<sup>25</sup> «Стандарт Банка России «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности». Принят и введен в действие приказом Банка России от 08.02.2023 № ОД-215. URL: <https://cbr.ru> (дата обращения: 16.10.2025).

<sup>26</sup> Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации». URL: <http://pravo.gov.ru> (дата обращения: 16.10.2025).

<sup>27</sup> Собрание законодательства РФ. 03.08.2020, № 31 (часть I), ст. 5017.

<sup>28</sup> Сведения о ходе рассмотрения поступивших инициативных предложений об установлении ЭПР. Портал Банка России. URL: [https://cbr.ru/vfs/fintech/information\\_258-fz.xlsx](https://cbr.ru/vfs/fintech/information_258-fz.xlsx) (дата обращения: 18.08.2026).

## Литература

1. Вайпан В.А. Источники цифрового права // Вестник арбитражной практики. 2024. № 1. С. 3—29.
2. Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере : монография / Н.С. Волкова, А.А. Ефремов, С.М. Зырянов и др.; отв. ред. Л.К. Терещенко. М. : Инфотропик Медиа, 2024. 352 с.
3. Финансовое право в условиях развития цифровой экономики : монография / К.Т. Анисина, Б.Г. Бадмаев, И.В. Бит-Шабо и др.; под ред. И.А. Цинделиани. М. : Проспект, 2019. 320 с.
4. Мартиросян А.Ж. Международно-правовое регулирование обеспечения безопасности в сфере использования информационно-коммуникационных технологий : дис. ... канд. юр. наук. М., 2024. С. 12.
5. Клещина Е.Н. Проблемы предупреждения преступлений, совершаемых посредством информационных технологий работниками банков // Вестник университета им. О.Е. Кутафина (МГЮА). 2025. № 5. С. 187.
6. Савенкова Д.Д. Институт юридической ответственности в системе правового обеспечения информационной безопасности в Российской Федерации : автореф. дис. ... канд. юрид. наук. М., 2019.
7. Поветкина Н.А. Финансово-правовая культура // Финансовое право. 2024. № 12. С. 2—5.
8. Бут Н.Д., Фомичев А.В. Особенности надзора за исполнением законов в кредитно-банковской сфере в условиях цифровой экономики // Право и цифровая экономика. 2024. № 1. С. 5—15.
9. Гулемин А.Н. Цифровые экосистемы в современном праве: анализ национальных и международных подходов // Электронное приложение к «Российскому юридическому журналу». 2024. № 5. С. 27—36.
10. Дубень А.К. Правовое обеспечение информационной безопасности в системе информационного права в Российской Федерации : дис. ... канд. юрид. наук: 5.1.2. М., 2023. 245 с. С. 175.
11. Метельков А.Н. Трансформация объекта защиты в условиях современных угроз безопасности информации // Правовая информатика. 2026. № 1. С. 44—51; с. 45.
12. Козырь Н.С., Бэк В.С. Риск-ориентированная интерпретация требований российского законодательства в сфере кибербезопасности // Правовая информатика. 2026. № 2. С. 52—61; с. 58, 59.
13. Ершова И.В., Тарасенко О.А. Изъятия норм федерального законодательства при установлении экспериментального правового режима // Хозяйство и право. 2025. № 7. С. 25—35.
14. Дубень А.К. Правовое обеспечение информационной безопасности Российской Федерации: нормативно-правовые основы и современные вызовы // Правовая информатика. 2026. № 1. С. 284—288; с. 287.

**SECTION:**  
**REGULATORY INFORMATICS**

# ORGANIZATIONAL AND LEGAL SUPPORT FOR INFORMATION SECURITY IN THE INTERACTION BETWEEN STATE INFORMATION SYSTEMS AND CREDIT ORGANIZATIONS

*Ivanov N. Yu.*<sup>29</sup>

**Keywords:** legal regulation, state information systems, credit organizations, information security, critical information infrastructure, personal data protection, user access, experimental legal regime, public-private partnership.

## Abstract

**Purpose of work.** To develop proposals for improving the organizational and legal framework for information security in the interaction between state information systems and credit organizations, based on a scientific analysis of trends in the development of the regulatory framework.

**Research method.** The methodological basis of the study comprises a set of general scientific and special legal methods. Analysis and synthesis were used to identify the main trends in the legal regulation of information security in the interaction between state information systems and credit organizations. The logical method was applied in formulating conclusions and recommendations.

---

<sup>29</sup> **Nikolai Yu. Ivanov**, Ph.D. student at the Department of Fundamental Jurisprudence and International Law of the Russian University of Advocacy and Notary Services named after G.B. Mirzoev, Moscow, Russian Federation.  
E-mail: [nj\\_ivanov@mail.ru](mailto:nj_ivanov@mail.ru)

**Results of the study.** To further improve this framework, it is proposed to unify information security requirements established by various regulators — the Federal Security Service, the Federal Service for Technical and Export Control, the Bank of Russia, and Roskomnadzor — by developing interagency and comprehensive standards and adopting joint regulatory legal acts specifically designed to regulate the activities of state information systems interacting with credit organizations.

The study also proposes promoting public-private partnerships in the field of information exchange concerning cyberattacks by establishing legal guarantees of confidentiality for the data transmitted by participants and simplifying the procedure for connecting private owners of critical infrastructure facilities to the state system for detecting, preventing, and eliminating the consequences of computer attacks.

The study demonstrates the need to modernize the legal regulation of experimental legal regimes in the financial market, including information security, by amending Federal Law No. 258-FZ of July 31, 2020 “On Experimental Legal Regimes in the Sphere of Digital and Technological Innovations in the Russian Federation”.

It was established that strengthening information security in the interaction between state information systems and credit organizations may require amendments to Chapter 28 of the Criminal Code of the Russian Federation to increase criminal liability for negligent computer-related offenses, as well as to introduce additional administrative and disciplinary liability.

## References

1. Vaipan V.A. Istochniki tsifrovogo prava // Vestnik arbitrazhnoi praktiki. 2024. No. 1. S. 3—29.
2. Gosudarstvo, obshchestvo i lichnost': puti preodoleniia vyzovov i ugroz v informatsionnoi sfere : monografiia / N.S. Volkova, A.A. Efremov, S.M. Zyrianov i dr.; otv. red. L.K. Tereshchenko. M. : Infotropik Media, 2024. 352 s.
3. Finansovoe pravo v usloviakh razvitiia tsifrovoy ekonomiki : monografiia / K.T. Anisina, B.G. Badmaev, I.V. Bit-Shabo i dr.; pod red. I.A. Tsindeliani. M. : Prospekt, 2019. 320 s.
4. Martirosian A.Zh. Mezhdunarodno-pravovoe regulirovanie obespecheniia bezopasnosti v sfere ispol'zovaniia informatsionno-kommunikatsionnykh tekhnologii : dis. ... kand. iur. nauk. M., 2024. S. 12.
5. Kleshchina E.N. Problemy preduprezhdeniia prestuplenii, sovershaemykh posredstvom informatsionnykh tekhnologii rabotnikami bankov // Vestnik universiteta im. O.E. Kutafina (MGlU). 2025. No. 5. S. 187.
6. Savenkova D.D. Institut iuridicheskoi otvetstvennosti v sisteme pravovogo obespecheniia informatsionnoi bezopasnosti v Rossiiskoi Federatsii : avtoref. dis. ... kand. iurid. nauk. M., 2019.
7. Povetkina N.A. Finansovo-pravovaia kul'tura // Finansovoe pravo. 2024. No. 12. S. 2—5.
8. But N.D., Fomichev A.V. Osobennosti nadzora za ispolneniem zakonov v kreditno-bankovskoi sfere v usloviakh tsifrovoy ekonomiki // Pravo i tsifrovaia ekonomika. 2024. No. 1. S. 5—15.
9. Gulemin A.N. Tsifrovye ekosistemy v sovremennom prave: analiz natsional'nykh i mezhdunarodnykh podkhodov // Elektronnoe prilozhenie k “Rossiiskomu iuridicheskomu zhurnalu”. 2024. No. 5. S. 27—36.
10. Duben' A.K. Pravovoe obespechenie informatsionnoi bezopasnosti v sisteme informatsionnogo prava v Rossiiskoi Federatsii : dis. ... kand. iurid. nauk: 5.1.2. M., 2023. 245 s. S. 175.
11. Metel'kov A.N. Transformatsiia ob'ekta zashchity v usloviakh sovremennykh ugroz bezopasnosti informatsii // Pravovaia informatika. 2026. No. 1. S. 44—51; s. 45.
12. Kozyr' N.S., Bek V.S. Risk-orientirovannaia interpretatsiia trebovanii rossiiskogo zakonodatel'stva v sfere kiberbezopasnosti // Pravovaia informatika. 2026. No. 2. S. 52—61; s. 58, 59.
13. Ershova I.V., Tarasenko O.A. Iz'iatii norm federal'nogo zakonodatel'stva pri ustanovlenii eksperimental'nogo pravovogo rezhima // Khoziaistvo i pravo. 2025. No. 7. S. 25—35.
14. Duben' A.K. Pravovoe obespechenie informatsionnoi bezopasnosti Rossiiskoi Federatsii: normativno-pravovye osnovy i sovremennye vyzovy // Pravovaia informatika. 2026. No. 1. S. 284—288; s. 287.





# СТАНОВЛЕНИЕ И РАЗВИТИЕ ЦИФРОВОГО ПРОСТРАНСТВА КАК ОБЪЕКТА ПРАВОВОГО РЕГУЛИРОВАНИЯ<sup>1</sup>

Маскайкина Е.А.<sup>2</sup>

**Ключевые слова:** цифровое пространство, киберпространство, информационное право, государственные информационные системы, объект правоотношения, цифровизация, цифровая трансформация, платформенная экономика, информационная безопасность, суверенитет.

## Аннотация

**Цель:** исследовать процессы становления и эволюции цифрового пространства как объекта правового регулирования, выявить теоретико-правовые основы их формирования, а также определить этапы развития российского законодательства в данной сфере. Рассмотреть трансформацию подходов к регулированию интернет-отношений от фрагментарных норм к системному регулированию платформенной экономики. Заострить внимание на ключевых проблемах, связанных с разграничением понятий «цифровая среда» и «цифровое пространство», а также на противоречии между традиционными методами императивного регулирования и трансграничной природой цифровых сред.

**Методы исследования:** общенаучные методы анализа и синтеза, исторический и формально-юридический методы, а также системный подход, позволивший рассмотреть цифровое пространство как сложный многоаспектный информационный предмет, по поводу которого складываются общественные отношения, требующие правового опосредования.

**Результаты исследования** свидетельствуют, что эволюция цифрового пространства прошла путь от фрагментированной сети Интернет до сложных платформенных экосистем и государственных информационных систем. Обоснована необходимость разграничения понятий «цифровизация» и «цифровая трансформация» как самостоятельных, хотя и взаимосвязанных феноменов. Показано, что классическая методология императивного регулирования, основанная на территориальном принципе, утрачивает свою регулятивную силу в условиях трансграничности цифровых сред. В российском законодательстве прослеживается эволюция от первых актов информатизации (Федеральный закон от 20.02.1995 № 24-ФЗ, Указ Президента РФ от 20.01.1994 № 170) к принятию Федерального закона от 27.07.2006 № 149-ФЗ, заложившего системные основы регулирования, и в последующем — к Федеральному закону от 31.07.2025 № 289-ФЗ, что создало предпосылки для осмысления правовых режимов государственных информационных систем.

**Новизна исследования** состоит в системном анализе становления цифрового пространства как самостоятельного объекта правового регулирования. Обоснована целесообразность применения концепции И.Л. Бачило о замене категории «объект правоотношения» на «предмет отношений» применительно к информационным правоотношениям в цифровой среде. В рамках предложенного подхода выделены и охарактеризованы четыре технологических этапа развития сети Интернет, каждый из которых требовал качественно новых правовых решений. Особое внимание уделено разграничению понятий «цифровая среда» и «цифровое пространство», а также соотношению цифровизации и цифровой трансформации, что позволяет уточнить понятийный аппарат информационного права. Предложена периодизация российского законодательства в сфере регулирования цифровых отношений, включающая переход от косвенного регулирования к специальному регулированию платформенной экономики.

DOI: 10.24412/1994-1404-2026-3-277-284

<sup>1</sup> Статья подготовлена в рамках реализации программы стратегического академического лидерства «Приоритет-2030».

<sup>2</sup> Маскайкина Елена Александровна, руководитель Проектного офиса Центра управления изменениями, аспирант кафедры информационного права и цифровых технологий Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация.

E-mail: [elena.maskaykina@bk.ru](mailto:elena.maskaykina@bk.ru)

## Введение

Исследование процессов становления и эволюции цифрового пространства в качестве объекта правового регулирования объективно требует предварительного уточнения понятийно-категориального аппарата, используемого в рамках настоящей работы. В теории информационного права сохраняется дискуссия относительно структуры правоотношения и места в ней таких фундаментальных категорий, как «объект» и «предмет», от разрешения которой непосредственно зависит методология анализа конкретных форм цифрового пространства и их правовых режимов [1—3]. В юридической доктрине сохраняется дискуссия о структуре правоотношения и разграничении категорий «объект» и «предмет» правового регулирования: не сложилось единого понимания того, что именно выступает объектом правоотношения в цифровой среде: информация, данные, цифровое пространство как таковое или складывающиеся по его поводу общественные отношения, а также как это соотносится с предметом правового регулирования.

Данная теоретическая неопределённость приобретает особую практическую значимость в контексте реализации национального проекта «Экономика данных и цифровая трансформация государства», выступающего одним из ключевых направлений государственной политики Российской Федерации на период до 2030 года и на перспективу до 2036 года. Целевыми ориентирами названного национального проекта определены цифровая трансформация государственного и муниципального управления, экономики и социальной сферы, что предполагает обеспечение кибербезопасности, бесперебойного доступа к сети Интернет, подготовку квалифицированных кадров для ИТ-отрасли, развитие отечественных цифровых платформ и программного обеспечения, внедрение техно-

логий искусственного интеллекта, а также формирование устойчивой системы цифрового государственного управления. Каждое из этих направлений связано с необходимостью определить правовой режим объектов, возникающих в цифровой среде, а также субъектов, осуществляющих деятельность в этой среде, соответственно, требует определенности относительно определения объекта и предмета для соответствующих правоотношений.

В условиях ускорения технологического прогресса и возрастания угроз в киберпространстве вопросы обеспечения цифрового суверенитета приобретают характер приоритетных при решении стратегических задач [4]. В связи с изложенным уточнение понятийного аппарата и выработка единообразных подходов к правовому регулированию цифровых пространств становятся не только доктринальной, но и практико-ориентированной необходимостью, обеспечивающей правовую определённость в условиях формирования экономики данных.

### Теоретические и концептуальные основы исследования цифрового пространства как объекта правового регулирования

В современной теории права сложились две основные концепции понимания объекта правоотношения. Согласно монистической теории, единственным объектом могут выступать лишь действия субъектов, поскольку именно поведение людей подвергается правовому регулированию. Плюралистическая теория, напротив, исходит из многообразия объектов, которые столь же различны, сколь разнообразны сами регулируемые отношения: это могут быть как материальные блага и ценности, так и действия, поведение участников, ради которых субъекты вступают в правоотношения.

Таблица 1

#### Сравнительный анализ классических теорий понимания объекта правоотношений и концепции И.Л. Бачило

| Критерий сравнения              | Монистическая теория                         | Плюралистическая теория                        | Концепция И.Л. Бачило                         |
|---------------------------------|----------------------------------------------|------------------------------------------------|-----------------------------------------------|
| Понимание объекта               | Исключительно действия и поведение субъектов | Многообразие благ: вещи, ценности, действия    | Отказ от объекта; введение предмета отношений |
| Ключевой вопрос                 | На что направлено правовое воздействие?      | Какое благо мотивирует вступление в отношение? | По поводу чего возникло отношение?            |
| Критерий объекта                | Единый: поведение участников отношения       | Отсутствует: открытый перечень благ            | Единый: наличие информационного объекта       |
| Информация как объект           | Не признаётся                                | Признаётся, но без чёткого критерия            | Признаётся предметом информационных отношений |
| Связь с предметом регулирования | Не устанавливается доктриной                 | Не устанавливается доктриной                   | Устанавливается через родовую категорию       |

Традиционный спор между монистической и плюралистической теориями по своей сути является спором о критерии: что именно следует признавать объектом правоотношения. Монистическая теория настаивает на единственном критерии — поведении, но тогда за рамками анализа остаётся информация. Плюралистическая теория отказывается от единого критерия, признавая объектами всё многообразие благ, но тем самым лишает категорию «объект» аналитической строгости. В этой связи особенно значимой представляется концепция, разработанная И.Л. Бачило. Автор обосновывает целесообразность отказа от классического элемента «объект правоотношения» с заменой его категорией «предмет отношений» (материальный или виртуальный), под которым понимаются все виды *информационных объектов*<sup>3</sup>. Данный подход позволяет, во-первых, преодолеть доктринальный спор между монистической и плюралистической концепциями, во-вторых, достичь терминологической унификации путем соотнесения предмета конкретного правоотношения с родовой категорией «предмет правового регулирования».

В рамках предлагаемой концепции элементами информационного правоотношения выступают:

1. субъекты (участники); как отмечает Н.А. Троян, «развитие системы информационных и цифровых отношений сопровождается появлением новых субъектов и объектов информационного права, внедрением наукоемких технологий, формированием новых информационных пространств» [5];
2. предмет отношений — информационный объект (то, по поводу чего возникли отношения);
3. содержание правоотношения — совокупность субъективных прав и юридических обязанностей участников;
4. меры ответственности.

Представляется, что применение данной концепции к исследованию становления и развития цифрового пространства является научно обоснованным и эвристически продуктивным. Именно цифровое пространство (от фрагментированной сети Интернет до государственных информационных систем) является сложным многосоставным информационным предметом, по поводу которого складываются общественные отношения, требующие соответствующего правового регулирования. Развитие экономики данных, снижение значения географических пространств, возможность развития многосторонних связей [6] неизбежно приводят к эволюции цифрового пространства (переход от простых форм к сложным, от централизованных архитектур к децентрализованным, от информационно-коммуникационных систем к иммерсивным виртуальным мирам).

Цифровое пространство определяется в доктрине как «глобальная сфера информационной среды, состоящая из взаимозависимой сети инфраструктур информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры»<sup>4</sup>. Существует широко распространенное мнение о том, что оно не является физически определенным местом, а преодолевает границы, реализуясь в любом физическом или временном измерении. Это сокращенный термин, который относится к среде, созданной слиянием совместных сетей компьютеров, информационных систем и телекоммуникационных инфраструктур.

Цифровое пространство характеризуется доступностью информации, поэтому представляется логичным его отождествление в любых пространственных измерениях, например, на земле, в открытом море, международном воздушном пространстве или космическом пространстве, т. е. возможна его характеристика как общемирового пространства. Все эти аспекты позволяют сделать справедливый вывод о том, что цифровое пространство не находится под исключительным суверенитетом одного государства, но отдельные элементы его инфраструктуры и информационные процессы подчиняются территориальной и государственной юрисдикции. Например, оборудование, составляющее технологическую инфраструктуру, необходимую для функционирования цифрового пространства, находится на территории конкретного государства; принадлежит самому государству или корпорациям; его функционирование обеспечивается национальной электрической сетью<sup>5</sup>. Интеграция физических компонентов технологической инфраструктуры, расположенных на территории того или иного государства, в глобальную среду цифрового пространства не может быть истолкована как отказ от осуществления территориального суверенитета. Кроме того, государства фактически активно развивают в своей контрольно-надзорной деятельности и принцип информационного суверенитета, предполагающий полноту государственной власти по контролю над распространением информации на своей территории.

Таким образом, под цифровым пространством понимается сложный многосоставный информационный объект (предмет отношений), объединяющий технологическую инфраструктуру (сети, информационные системы, технические средства), информационные ресурсы и цифровые процессы, по поводу которых

<sup>3</sup> Бачило И.Л. Информационное право : учебник. М. : Юрайт, 2020. 420 с.

<sup>4</sup> Joint Chiefs of Staff. Joint Publication 1-02: U.S. Department of Defense Dictionary of Military and Associated Terms (Nov. 8, 2010, as amended through February 15, 2016). URL: [https://fas.org/irp/doddir/dod/jp1\\_02.pdf](https://fas.org/irp/doddir/dod/jp1_02.pdf) (дата обращения: 20.06.2018); Schaap A.J. Cyber Warfare Operations: Development and Use under International Law // Air Force Law Review. 2009. № 64. P. 121, 126.

<sup>5</sup> Kastenbergh J.E. Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law // Air Force Law Review. 2009. 64(43). P. 64.; Svantesson J.D.B. Borders on, Border Around — The Future of the Internet // Albany Law Journal of Science & Technology. 2006. Vol. 16. P. 433—435.

складываются общественные отношения, требующие правового опосредования.

### Историко-правовые этапы развития цифрового пространства

Процесс становления цифрового пространства в качестве самостоятельного объекта правового регулирования представляет собой сложную, многоаспектную эволюцию. Ее исходной точкой можно считать возникновение фрагментированной сети интернет, которая впоследствии привела к формированию сложных платформенных экосистем, а на текущем этапе к появлению государственных информационных систем. Указанный процесс зависит от темпов цифровизации, развития платформенной экономики, что закономерно формирует потребность в выработке новых правовых механизмов.

В развитии глобальной сети Интернет традиционно выделяют несколько ключевых этапов, каждый из которых менял характер общественных отношений и ставил новые задачи перед учеными и законодателем.

1) Первый этап (середина XX века) носил экспериментальный характер: формировались базовые протоколы передачи данных, создавались первые информационно-коммуникационные системы (преимущественно для военных нужд). Правовое регулирование на этой стадии отсутствовало, так как технологии не выходили за пределы применения в конкретных сферах, не становились массовыми.

2) Второй этап, приходящийся на 1990-е годы, связан с глобализацией сети Интернет, использованием её для массового применения. Интернет стал значимым фактором социально-экономического развития. Активное формирование трансграничных коммуникации, электронной коммерции обусловило необходимость первоначального правового осмысления необходимости правового регулирования, поскольку предыдущие модели регулирования уже не обеспечивали стабильность и безопасность формирующихся общественных отношений.

3) Третий этап, известный как «Web 2.0», изменил архитектуру сетевого взаимодействия. Распространение социальных платформ и сервисов пользовательского контента привело к тому, что источником формирования, генерации информации стали сами пользователи, а не владельцы ресурсов. Данная трансформация породила новые социальные практики и феномен цифровой идентичности, однако одновременно усложнила процесс решения задач по правовому регулированию в части ответственности за распространяемый контент, защиту персональных данных и установление пределов алгоритмической модерации.

4) Современный, четвёртый этап, ознаменовался принципиальным изменением: цифровая среда перестает быть пассивным полем для коммуникации и превращается в активный инструмент, который сам начинает выступать способом регулирования протека-

ющих в ней отношений [7]. Если ранее сеть выступала преимущественно как коммуникационная инфраструктура, то сегодня она сама становится инструментом нормативного воздействия. Распространение алгоритмического управления, интеграция технологий искусственного интеллекта и развитие децентрализованных архитектур формируют модель, близкую к концепции Л. Лессига «code is law»: программный код и технические стандарты фактически определяют допустимое поведение пользователей, подменяя или дополняя традиционные правовые предписания. В этих условиях закладываются институциональные основания для метавселенных, способных функционировать как квазиавтономные социальные системы с собственными механизмами нормотворчества и разрешения споров.

В научной литературе, как справедливо отмечают Т.А. Полякова, А.В. Минбалеев и Н.В. Кроткова, необходимо различать понятия «цифровизация» и «цифровая трансформация». Цифровизация представляет собой процесс перехода на цифровые технологии, внедрение информационных технологий в отдельные функции и деятельность, ранее выполнявшиеся без их использования. В отличие от этого, цифровая трансформация — более сложный феномен, охватывающий широкий спектр изменений, связанных с применением цифровых технологий, и ориентированный на комплексное, стратегическое преобразование процессов с целью адаптации к изменяющимся условиям и создания новых ценностей [8]. Авторы обоснованно заключают, что цифровизацию необходимо рассматривать как один из важнейших процессов цифровой трансформации, а не как её синоним.

При этом история правового регулирования сети Интернет существенно короче истории самой технологии и насчитывает немногим более 30 лет. Наиболее интенсивное развитие законодательство получило на втором этапе технологической эволюции, когда глобализация сети и её коммерциализация сделали очевидной потребность в унифицированных нормах. Многие государства, в том числе Российская Федерация, с середины 2000-х годов начали последовательно стремиться к выработке всеобъемлющего подхода к регулированию. Однако, классическая методология императивного регулирования, основанная на территориальном принципе и государственном суверенитете, начинает утрачивать свою регулятивную силу в условиях трансграничности платформенных экосистем и виртуальных миров. Возникает объективное противоречие между динамикой технологического развития и статичностью традиционных правовых механизмов.

Существенным фактором, объясняющим позднее появление прямых нормативных предписаний, является исходно низкая степень вовлеченности широких масс субъектов в интернет-отношения и, как следствие, их незначительная экономическая значимость для национальных экономик. Правовое регулирование, как правило, возникает там, где формируется устойчивый массовый интерес, требующий защиты.



В российском контексте следует отметить, что, несмотря на отсутствие прямого законодательного регулирования в 1990-е годы, интернет уже активно использовался в отдельных отраслях экономики и способствовал складыванию самобытной интернет-субкультуры. В этот период отношения регулировались преимущественно стихийно формирующимися локальными нормами интернет-сообществ (так называемыми «нетикетом» и обычкновениями), а также общими конституционными положениями. В частности, статьи 23, 24 и 29 Конституции РФ, закрепляющие права на тайну переписки, неприкосновенность частной жизни и свободу информации, создавали конституционную основу, которая могла быть применена и к отношениям в цифровой среде, хотя и не содержала специальных механизмов реализации.

Точкой отсчета для системного правового регулирования в России, по обоснованному мнению В.Б. Наумова, следует считать принятие Федерального закона от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации»<sup>6</sup>. Данный нормативный акт<sup>7</sup> заложил фундаментальные понятийные основы (такие как «информация», «информационные ресурсы», «информатизация») и определил общие принципы работы с информацией, создав тем самым необходимую базу для будущего отраслевого законодательства. Вместе с тем необходимо подчеркнуть, что указанный закон не содержал прямых норм, регулирующих функционирование сети Интернет как таковой, и не учитывал ее специфики. Дальнейшим шагом в развитии косвенного регулирования стало принятие Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»<sup>8</sup>, который создал технико-юридические предпосылки для признания юридической значимости действий, совершаемых в электронной среде, и стимулировал развитие электронного документооборота. Таким образом, формирование правового режима цифрового пространства происходило постепенно, путем наслоения общих и специальных норм, отражая усложнение самой технологической и социальной реальности.

Учитывая, что право служит своеобразным отражением всех проявлений суверенитета, поскольку право не «привязано» лишь к обществу или государству и способствует обеспечению жизнедеятельности социальных субъектов права [9]: людей, социальных общностей и объединений, логика развития цифрового пространства, пройдя этап становления глобальной сети, закономерно привела к формированию более

сложных образований — платформенных экосистем и, в перспективе, метавселенных. Данная эволюция не могла не отразиться в праве, которое вынуждено адаптироваться к усложняющейся структуре общественных отношений. Важнейшим этапом этого процесса на современном этапе стало принятие Федерального закона от 31 июля 2025 г. № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации»<sup>9</sup>, ознаменовавшего переход от фрагментарного регулирования интернет-отношений к системному осмыслению платформенной экономики как самостоятельного правового феномена. Параллельно с этим возникают вызовы, связанные с внедрением концепции Web3, основанной на децентрализации и распределенных реестрах, а также с развитием метавселенных — иммерсивных виртуальных миров, претендующих на автономную социальную организацию. В этом контексте особую роль играют гибридные модели регулирования, сочетающие императивные государственные предписания с саморегулированием и техническими стандартами.

Показательным примером такой гибридности (в научной литературе выделяется подход, согласно которому уровень информационного или цифрового развития определяется сформированностью рынков информационных объектов, включая рынок информационных систем [10, с. 6]) выступает платформа «ГосТех», которая, не являясь самостоятельной государственной информационной системой, представляет собой «цифровую экосистему создания, развития и эксплуатации государственных информационных систем, включающую единую программно-аппаратную среду, цифровые продукты платформы «ГосТех», информацию, информационные технологии, а также совокупность нормативных правовых, организационных, методологических правил и процедур, обеспечивающих деятельность участников отношений, возникающих в связи с созданием и функционированием платформы «ГосТех»<sup>10</sup>, то есть инфраструктурную среду, объединяющую множество государственных информационных систем и тем самым демонстрирующую новый уровень публично-правового управления цифровым пространством.

Становление правового фундамента для указанных процессов происходило постепенно, начиная с первых актов, заложивших основы государственной политики в сфере информатизации. К числу ключевых документов раннего этапа относится Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государствен-

<sup>6</sup> Наумов В.Б. Развитие интернет-права в России: право в сетях XXI века. СПб., 2016. URL: <http://www.russianlaw.net/files/law/doc/aa71.pdf> (дата обращения: 15.10.2025).

<sup>7</sup> Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» // Собрание законодательства Российской Федерации. 1995. № 8. Ст. 609.

<sup>8</sup> Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» // Собрание законодательства Российской Федерации. 2002. № 2. Ст. 127.

<sup>9</sup> Федеральный закон от 31 июля 2025 г. № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» // Собрание законодательства Российской Федерации. 2025. № 31. Ст. 4643.

<sup>10</sup> Постановление Правительства РФ от 16.12.2022 № 2338 (ред. от 08.09.2025) «Об утверждении Положения о единой цифровой платформе Российской Федерации “ГосТех”...» // Собрание законодательства РФ. 2022. № 52. Ст. 9610.

ной политики в сфере информатизации»<sup>11</sup>. Данный указ, хотя и не содержал прямых упоминаний сети Интернет, сыграл важную роль, впервые на высшем уровне подчеркнув стратегическое значение информатизации для социально-экономического развития Российской Федерации. Он определил приоритеты формирования национальной информационной инфраструктуры, что впоследствии создало концептуальную базу для более детального регулирования. Следующим значимым шагом стало утверждение Доктрины информационной безопасности Российской Федерации (Указом Президента РФ от 9 сентября 2000 г. № Пр-1895). На доктринальном уровне впервые были обозначены угрозы, возникающие в процессе использования сети Интернет, и определен вектор защиты национальных интересов в информационной сфере, включая противодействие киберпреступности и обеспечение безопасности критической информационной инфраструктуры. Понятие «Интернет» начало активно использоваться лишь в начале 2000-х годов, а прецеденты, как известно, не являются источником права в российской правовой системе, указанные акты сформировали необходимые предпосылки для перехода к целенаправленному нормативному регулированию интернет-отношений.

Впервые на доктринальном уровне угрозы, связанные с использованием сети Интернет, были обозначены именно в этих документах. Там же определили и вектор защиты национальных интересов в информационной сфере, включая противодействие киберпреступности и обеспечение безопасности критической информационной инфраструктуры. Понятие «Интернет» начало активно использоваться лишь в начале 2000-х годов. Прецеденты, как известно, источником права в российской правовой системе не являются. Однако перечисленные акты создали необходимые предпосылки для перехода к целенаправленному нормативному регулированию отношений в интернете.

Подлинно переломный момент в развитии российского цифрового законодательства наступил с принятием Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»<sup>12</sup>. Этот закон пришёл на смену устаревшим актам: Федеральному закону № 24-ФЗ «Об информации, информатизации и защите информации» (1995 г.) и Федеральному закону № 85-ФЗ «Об участии в международном информационном обмене» (1996 г.). В нём консолидировали и модернизировали понятийный аппарат. Именно в ФЗ № 149-ФЗ впервые на законодательном уровне закрепили такие ключевые термины, как «информационные технологии», «информационная система», а также упомянули сеть «Интернет». Закон носит межотраслевой характер:

в нём есть и частноправовые нормы (например, регулирующие договоры в электронной форме), и публично-правовые предписания (касающиеся ограничения доступа к информации, обязанностей операторов и т. д.). Принятие ФЗ № 149-ФЗ можно считать моментом зарождения системного цифрового законодательства: он не только урегулировал базовые отношения, но и заложил механизмы для дальнейшего отраслевого нормотворчества.

Параллельно с развитием общего информационного законодательства меняли и смежные институты. Например, в Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» неоднократно вносили изменения. Так устраняли технико-юридические противоречия, уточняли терминологию в части использования усиленных квалифицированных электронных подписей. Эти изменения обеспечили юридическую значимость электронного документооборота и создали доверие к цифровым транзакциям. Ещё один важный шаг — принятие Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платёжной системе». Он ввёл понятия «электронные денежные средства», «перевод электронных денежных средств», заложил правовые основы для функционирования цифровых финансовых сервисов: мобильных банков, онлайн-платежей. Все перечисленные изменения не носили глобального революционного характера, но они последовательно устраняли нормативные лакуны и адаптировали правовую систему к реалиям цифровой экономики.

В итоге формирование нормативных дефиниций, выработка базовых принципов регулирования и настройка смежных институтов подготовили национальную правовую систему к новому этапу цифровизации. Именно этот фундамент позволил перейти к специальному регулированию платформенной экономики, которое воплотилось в ФЗ № 289-ФЗ (2025 г.). Тогда же создались предпосылки для осмысления правовых режимов метавселенных. Дальнейшее развитие, скорее всего, будет связано с поиском баланса между традиционными государственными механизмами и саморегулируемыми протоколами Web3. В этой перспективе роль права может трансформироваться: от прямого предписания — к установлению рамок и стандартов для алгоритмического регулирования.

## Заключение

Проведённый анализ становления цифрового пространства как объекта правового регулирования показал: эволюция прошла путь от фрагментированной сети Интернет до сложных платформенных экосистем и государственных информационных систем. Представляется, что единый универсальный правовой режим, охватывающий всё многообразие форм цифрового пространства, в строгом юридическом смысле вряд ли может быть сформирован в обозримой перспективе ввиду радикальной неоднородности регулируемых

<sup>11</sup> Указ Президента РФ от 20.01.1994 № 170 «Об основах государственной политики в сфере информатизации» // Российская газета. 1994. № 19.

<sup>12</sup> Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

объектов и различий в национальных подходах. Целесообразно говорить о едином типе правового режима цифрового пространства, который реализуется через иерархическую систему «зонтичных» общих норм и специализированных подрежимов для отдельных видов цифровых сред.

При этом государственные информационные системы нуждаются в более глубоком специальном регулировании, чем цифровые платформы. Террито-

риальный принцип стал недостаточным и требует сочетания с трансграничными и экстерриториальными механизмами. Формирование российского цифрового законодательства прошло этапы от первых актов информатизации до принятия отраслевого законодательства о платформенной экономике, что создало предпосылки для системного осмысления публично-правового режима государственных информационных систем.

## Литература

1. Минбалеев А.В. Трансформация регулирования цифровых отношений // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 12 (64). С. 31—36.
2. Новые горизонты развития системы информационного права в условиях цифровой трансформации : монография / Отв. ред.: Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М. : Институт государства и права, 2022. 368 с.
3. Волков Ю.В. Структура информационного отношения и правоотношения // Международный научно-исследовательский журнал. 2024. № 7 (145). С. 1—6.
4. Полякова Т.А., Троян Н.А. Стратегические задачи обеспечения технологического и цифрового суверенитета: правовые аспекты формирования новой информационной среды // Правовая информатика. 2025. № 1. С. 70—78.
5. Троян Н.А. Цифровая трансформация и технологическое развитие как основа инновационного прогресса: стратегические ориентиры для достижения технологического лидерства // Правовая информатика. 2025. № 4. С. 227—234.
6. Минбалеев А.В. Формирование экономики данных в России в условиях многополярного мира: проблемы правового обеспечения // Экономика и управление. 2023. Т. 29. № 8. С. 956—963. DOI: 10.35854/1998-1627-2023-8-956-963.
7. Ладенков Н.Е. Трансформация правовой системы под влиянием цифровизации: причины и тенденции // Философия права. 2021. № 1 (96). С. 164—168.
8. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Цифровая трансформация как правовой феномен и ее влияние на развитие информационного права и законодательства // Государство и право. 2025. № 11. С. 204—219.
9. Трансформация информационного права : монография / Отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М. : Институт государства и права РАН, 2023. 256 с.
10. Акжитов Е.А. Тенденции рынка информационных систем управления транспортной логистикой // Корпоративные информационные системы. 2019. № 2. С. 1—10.

SECTION:  
REGULATORY INFORMATICS

# FORMATION AND DEVELOPMENT OF DIGITAL SPACE AS AN OBJECT OF LEGAL REGULATION<sup>13</sup>

Maskaikina E.A.<sup>14</sup>

**Keywords:** digital space, cyberspace, information law, state information systems, object of legal relations, digitalization, digital transformation, platform economy, information security, sovereignty.

<sup>13</sup> The article was prepared as part of the implementation of the Strategic Academic Leadership Programme "Priority 2030".

<sup>14</sup> **Elena A. Maskaikina**, Head of the Project Office of the Change Management Centre, Ph.D. student at the Department of Information Law and Digital Technologies of the Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation.  
E-mail: [elena.maskaikina@bk.ru](mailto:elena.maskaikina@bk.ru)

### Abstract

**Purpose of work:** to investigate the processes of formation and evolution of digital space as an object of legal regulation, identify the theoretical and legal foundations of their formation, and determine the stages of development of Russian legislation in this area. To examine the transformation of approaches to regulating Internet relations from fragmented rules to the systemic regulation of the platform economy. To focus on the key problems associated with distinguishing between the concepts of “digital environment” and “digital space”, as well as on the contradiction between traditional methods of imperative regulation and the cross-border nature of digital environments.

**Research method:** general scientific methods of analysis and synthesis, historical and formal legal methods, as well as a systemic approach, which made it possible to consider digital space as a complex, multi-component information subject in relation to which social relations arise that require legal mediation.

**Results of the study** indicate that the evolution of digital space has progressed from a fragmented Internet network to complex platform ecosystems and state information systems. The necessity of distinguishing between the concepts of “digitalization” and “digital transformation” as independent, although interrelated, phenomena is substantiated. It is demonstrated that the classical methodology of imperative regulation based on the territorial principle is losing its regulatory force under the conditions of the cross-border nature of digital environments. Russian legislation demonstrates an evolution from the first acts on informatization (Federal Law dated 20.02.1995 № 24-FZ, Decree of the President of the Russian Federation dated 20.01.1994 г. № 170) to the adoption of Federal Law dated 27.07.2006 № 149-FZ, which laid the systemic foundations for regulation, and subsequently to Federal Law dated 31.07.2025 № 289-FZ, thereby creating the prerequisites for understanding the legal regimes of state information systems.

**Novelty of the study** lies in the systemic analysis of the formation of digital space as an independent object of legal regulation. The expediency of applying I. L. Bachilo’s concept of replacing the category “object of legal relations” with “subject matter of relations” with regard to information-related legal relations in the digital environment is substantiated. Within the framework of the proposed approach, four technological stages of Internet development are identified and characterized, each of which required qualitatively new legal solutions. Particular attention is paid to distinguishing between the concepts of “digital environment” and “digital space”, as well as to the relationship between digitalization and digital transformation, which makes it possible to clarify the conceptual framework of information law. A periodization of Russian legislation in the field of regulating digital relations is proposed, including the transition from indirect regulation to special regulation of the platform economy.

### References

1. Minbaleev A.V. Transformatsiia regulirovaniia tsifrovyykh otnoshenii // Vestnik Universiteta imeni O.E. Kutafina (MGlU). 2019. No. 12 (64). S. 31—36.
2. Novye gorizonty razvitiia sistemy informatsionnogo prava v usloviakh tsifrovoy transformatsii : monografiia / Otv. red.: T.A. Poliakova, A.V. Minbaleev, V.B. Naumov. M. : Institut gosudarstva i prava, 2022. 368 s.
3. Volkov Iu.V. Struktura informatsionnogo otnosheniia i pravootnosheniia // Mezhdunarodnyi nauchno-issledovatel’skii zhurnal. 2024. No. 7 (145). S. 1—6.
4. Poliakova T.A., Troian N.A. Strategicheskie zadachi obespecheniia tekhnologicheskogo i tsifrovogo suvereniteta: pravovye aspekty formirovaniia novoi informatsionnoi sredy // Pravovaia informatika. 2025. No. 1. S. 70—78.
5. Troian N.A. Tsifrovaia transformatsiia i tekhnologicheskoe razvitie kak osnova innovatsionnogo progressa: strategicheskie orientiry dlia dostizheniia tekhnologicheskogo liderstva // Pravovaia informatika. 2025. No. 4. S. 227—234.
6. Minbaleev A.V. Formirovanie ekonomiki dannykh v Rossii v usloviakh mnogopoliarnogo mira: problemy pravovogo obespecheniia // Ekonomika i upravlenie. 2023. T. 29. No. 8. S. 956—963. DOI: 10.35854/1998-1627-2023-8-956-963.
7. Ladenkov N.E. Transformatsiia pravovoi sistemy pod vlianiem tsifrovizatsii: prichiny i tendentsii // Filosofiya prava. 2021. No. 1 (96). S. 164—168.
8. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Tsifrovaia transformatsiia kak pravovoi fenomen i ee vlianie na razvitie informatsionnogo prava i zakonodatel’sтва // Gosudarstvo i pravo. 2025. No. 11. S. 204—219.
9. Transformatsiia informatsionnogo prava : monografiia / Otv. red. T.A. Poliakova, A.V. Minbaleev, V.B. Naumov. M. : Institut gosudarstva i prava RAN, 2023. 256 s.
10. Akzhitov E.A. Tendentsii rynka informatsionnykh sistem upravleniia transportnoi logistikoi // Korporativnye informatsionnye sistemy. 2019. No. 2. S. 1—10.





# ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ КАК ОПОРНАЯ ИНФРАСТРУКТУРА НАЦИОНАЛЬНОЙ ПЛАТЁЖНОЙ СИСТЕМЫ: ПРАВОВОЙ РЕЖИМ НЕДОСТУПНОСТИ

Лобанов Н.А.<sup>1</sup>

**Ключевые слова:** противодействие мошенничеству, перевод денежных средств без добровольного согласия, оператор по переводу денежных средств, оператор связи, сертификат безопасности, удостоверяющий центр, обязанности оператора, сроки исполнения обязанностей, ответственность, непрерывность функционирования, публичное обсуждение проектов актов.

## Аннотация

**Цель:** определить, какими нормами установлены последствия недоступности государственных информационных систем для участников национальной платёжной системы, обязанных с 2027 года использовать такие системы, и предложить модель полноты соответствующего правового режима.

**Метод исследования:** формально-юридический анализ Федерального закона от 26 июня 2026 г. № 210-ФЗ и изменённых им законов, а также проектов подзаконных актов, размещённых на федеральном портале проектов нормативных правовых актов в июле и августе 2026 г. Сравнительно-правовым методом рассмотрены подходы к ответственности поставщиков доверенных услуг, а также к распределению рисков третьих сторон в финансовом секторе. В исследовании использованы материалы публичного обсуждения четырёх проектов актов; их анализ позволил оценить полноту правового регулирования по авторской модели правового режима, элементы которой проверяются в тексте закона, в первых редакциях проектов и в позициях разработчиков.

**Результаты:** выделены три государственные информационные системы, обращение к которым становится условием исполнения обязанностей операторами по переводу денежных средств и операторами связи: система противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, единая система учёта платёжных карт и государственная информационная система национального удостоверяющего центра. Показано, что закон в каждом случае устанавливает обязанность участника и последствия её неисполнения, но не устанавливает ни требований к доступности системы, ни порядка действий участника при её недоступности, ни влияния недоступности на течение сроков и наступление ответственности. Предложена модель правового режима опорной государственной информационной системы из восьми элементов и показатель его полноты; рассчитаны значения показателя для трёх систем на уровне закона и проектов подзаконных актов. Установлено, что элементы режима недоступности появляются только на подзаконном уровне и только по итогам публичного обсуждения: по проекту правил возмещения оператором связи разработчик отметил учтённым предложение автора о приостановлении сроков на период недоступности системы. Сформулированы предложения о закреплении режима недоступности на уровне закона.

DOI: 10.24412/1994-1404-2026-3-00-31

## Введение и постановка задачи

Федеральный закон от 26 июня 2026 г. № 210-ФЗ<sup>2</sup> (далее — Закон № 210-ФЗ) завершил формирование правовой конструкции, в которой исполнение обязанностей участниками национальной пла-

тёжной системы поставлено в зависимость от государственных информационных систем. С 1 марта 2027 г. оператор по переводу денежных средств при проверке признаков перевода без добровольного согласия

<sup>2</sup> Федеральный закон от 26 июня 2026 г. № 210-ФЗ «О внесении изменений в Федеральный закон «О связи» и отдельные законода-

тельные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2026. № 26. Ст. 3464.

<sup>1</sup> Лобанов Николай Александрович, независимый эксперт по информационной безопасности и защите критической информационной инфраструктуры, магистрант Института права и национальной безопасности РАНХиГС при Президенте Российской Федерации, г. Москва, Российская Федерация. ORCID: 0009-0006-8187-4528.

E-mail: nlobanov-25@ranepa.ru

клиента обязан использовать сведения, полученные посредством государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий (часть 3.1 статьи 8 Федерального закона «О национальной платёжной системе»<sup>3</sup> в редакции Закона № 210-ФЗ). С 1 сентября 2027 г. тот же оператор до предоставления клиенту платёжной карты обязан запросить сведения в единой системе учёта платёжных карт и обязан отказать в предоставлении карты, если её выдача нарушит установленное количественное ограничение (части 2.3 и 2.4 статьи 9 того же закона). Органы и организации, указанные в части 2.3 статьи 13 Федерального закона «Об информации, информационных технологиях и о защите информации»<sup>4</sup>, обязаны осуществлять электронное взаимодействие с применением сертификатов безопасности национального удостоверяющего центра, а Правительство Российской Федерации вправе установить случаи обязательного использования таких сертификатов в банковской сфере (части 12 и 13 статьи 14.1 Федерального закона «Об электронной подписи»<sup>5</sup> в редакции Закона № 210-ФЗ).

Общая черта этих норм в том, что обязанность участника исполнима только при работоспособности системы, которая ему не принадлежит и им не управляется. При этом последствия неисполнения обязанности закон устанавливает прямо: оператор по переводу денежных средств, исполнивший распоряжение клиента после получения посредством системы сведений об абонентском номере, возмещает клиенту сумму перевода (часть 3.13-1 статьи 8 Федерального закона «О национальной платёжной системе»), оператор связи возмещает сумму перевода при несоблюдении требований о направлении сведений в систему и о приостановлении оказания услуг по полученной из неё информации (часть 11 статьи 1 Федерального закона от 1 апреля 2025 г. № 41-ФЗ<sup>6</sup> в редакции Закона № 210-ФЗ).

В настоящей работе такие системы обозначаются как опорные государственные информационные системы национальной платёжной системы. Термин выбран по функциональному признаку: система является опорной для участника, если обращение к ней составляет условие исполнения его публичной обязанности,

а отказ системы не освобождает участника от последствий неисполнения. Это определение отличает рассматриваемые системы от информационных систем, используемых участниками по собственному усмотрению, и от систем, в которых участник выступает лишь поставщиком сведений.

Постановка задачи. Требуется установить, какими нормами определены последствия недоступности опорной государственной информационной системы для обусловленной ею обязанности участника: течение сроков, наступление ответственности, порядок действий участника в период недоступности, а также доказательственная база для подтверждения факта недоступности. Для этого необходимо: 1) выделить круг опорных систем по тексту Закона № 210-ФЗ; 2) сформировать перечень элементов правового режима, без которых обязанность, обусловленная системой, не может считаться исполнимой; 3) проверить наличие этих элементов в законе и в проектах подзаконных актов; 4) оценить, восполняются ли пробелы закона на подзаконном уровне и какую роль в этом играет публичное обсуждение проектов. Эмпирическую основу составили материалы публичного обсуждения четырёх проектов актов, в котором автор участвовал лично.

Степень разработанности темы. Правовая модель информационной системы и статус её оператора исследованы в работах А.Н. Метелькова, который показал, что законодательная конструкция понятия «информационная система» не включает субъекта права как элемент [1] и что термин «оператор» в законодательстве и стандартах многозначен, а требования регуляторов должны строго соответствовать субъектам, наделённым обязанностью их исполнять [2]. Развитие государственных информационных систем как платформ и экосистем государственных услуг рассмотрено Н.А. Троян [3], этапы правовой информатизации и задачи цифрового суверенитета исследованы Т.А. Поляковой и Н.А. Троян [4]. А.К. Дубень обосновывает необходимость единого правового режима защиты государственных информационных систем, систем персональных данных и объектов критической информационной инфраструктуры [5]; Д.А. Ловцов и А.С. Бурый рассматривают киберустойчивость как целевой фактор обеспечения кибербезопасности критически важных объектов [6]. Правовые основы противодействия мошенничеству на финансовом рынке систематизированы М.В. Хадеевой и Е.К. Овчинниковым, которые выделяют институциональные, организационные и функциональные основы национальной антифрод-системы и приводят архитектуру её финансового сегмента [7]; эволюция законодательства о противодействии кибермошенничеству вплоть до создания единого информационного пространства безопасности описана В.А. Гаужаевой и Е.В. Прокофьевой [8]. Распределение ответственности между банком и клиентом при дистанционном обслуживании исследовано П.С. Шуваловым и Н.В. Огановой [9]. Ответственность лиц, оказывающих доверенные услуги, как фактор доверия к цифровому

<sup>3</sup> Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платёжной системе» // Собрание законодательства Российской Федерации. 2011. № 27. Ст. 3872.

<sup>4</sup> Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

<sup>5</sup> Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // Собрание законодательства Российской Федерации. 2011. № 15. Ст. 2036.

<sup>6</sup> Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2025. № 14. Ст. 1574.

взаимодействию рассмотрена Н.И. Соловяненко [10]. Зарубежные исследования затрагивают смежные вопросы: состояние механизмов отзыва сертификатов в веб-инфраструктуре открытых ключей [11], последствия нормативного включения сертификатов, выпущенных по правилам публичного регулирования, в программы для доступа к сайтам [12], распределение ответственности за риски третьих сторон между банками, регуляторами и поставщиками технологий по регламенту Европейского союза об операционной устойчивости [13, 14], системный риск концентрации облачных услуг [15] и устойчивость инфраструктуры доменных имён, обслуживающей государственные сервисы [16].

Вместе с тем в известной автору литературе не рассматривался вопрос о правовых последствиях недоступности государственной информационной системы для обязанностей частных лиц, обусловленных обращением к ней. Настоящая работа восполняет этот пробел на материале Закона № 210-ФЗ.

Научная новизна состоит в предложенной модели правового режима опорной государственной информационной системы, в расчёте показателя полноты режима для трёх систем и в эмпирическом установлении того, на каком уровне регулирования и в результате какой процедуры элементов режима недоступности являются в тексте актов.

## **РЕШЕНИЕ ЗАДАЧИ**

### **Круг опорных систем по Закону № 210-ФЗ**

Анализ Закона № 210-ФЗ позволяет выделить три государственные информационные системы, обращение к которым обуславливает обязанности участников национальной платёжной системы.

Первая система создана Федеральным законом от 1 апреля 2025 г. № 41-ФЗ. Закон № 210-ФЗ расширяет обязанности её пользователей: они обязаны принимать меры, направленные на предотвращение и пресечение противоправных действий, и передавать в систему сведения о выявленных признаках таких действий (часть 6 статьи 1 Федерального закона № 41-ФЗ). Для оператора связи установлены обязанности выявлять по критериям, утверждаемым Правительством Российской Федерации, абонентские номера, используемые для противоправных вызовов и сообщений, направлять сведения о них в систему и приостанавливать оказание услуг по номерам, сведения о которых получены посредством системы (часть 10 той же статьи). Для оператора по переводу денежных средств установлены обязанность использовать сведения системы при проверке признаков перевода без добровольного согласия (часть 3.1 статьи 8 Федерального закона «О национальной платёжной системе»), учёт таких сведений при выявлении операций с признаками перевода без добровольного согласия (пункт 6 части 3.5 той же статьи), а также обязанность направить оператору связи через систему обращение клиента о возмещении (часть

3.13-5 той же статьи, часть 13 статьи 1 Федерального закона № 41-ФЗ). Обязанность возмещения при неисполнении этих требований возложена на оператора по переводу денежных средств (части 3.13-1, 3.13-2 статьи 8) и на оператора связи (части 11 и 14 статьи 1 Федерального закона № 41-ФЗ). Порядок взаимодействия операторов при возмещении устанавливается Правительством Российской Федерации по согласованию с Банком России (часть 13 статьи 1 Федерального закона № 41-ФЗ); соответствующий проект постановления размещён на федеральном портале проектов нормативных правовых актов под идентификатором 02/07/07-26/00169315<sup>7</sup> (далее — проект правил возмещения), проект критериев абонентских номеров под идентификатором 02/07/07-26/00169312<sup>8</sup>.

Вторая система, единая система учёта платёжных карт, введена статьёй 9.2 Федерального закона «О национальной платёжной системе» в редакции Закона № 210-ФЗ. Её оператором является оператор национальной системы платёжных карт, пользователями являются Банк России и операторы по переводу денежных средств (части 2 и 4 статьи 9.2). Оператор системы обязан обеспечивать её функционирование, защиту содержащейся в ней информации и предоставление операторам по переводу денежных средств сведений о количестве карт, предоставленных клиенту (часть 6 той же статьи). Оператор по переводу денежных средств обязан направлять в систему сведения о предоставленных картах (часть 7), обязан запросить сведения до предоставления карты и обязан отказать в предоставлении карты при превышении ограничения в двадцать карт (части 2.2 и 2.4 статьи 9). Порядок формирования и ведения системы и правила предоставления сведений устанавливаются нормативными актами Банка России (части 3 и 8 статьи 9.2); этот уровень регулирования в настоящей статье не анализируется.

Третья система, государственная информационная система национального удостоверяющего центра, введена статьёй 13.1 Федерального закона «Об электронной подписи» в редакции Закона № 210-ФЗ. Национальный удостоверяющий центр является федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

<sup>7</sup> Проект постановления Правительства Российской Федерации «Об утверждении правил взаимодействия оператора по переводу денежных средств и оператора связи при возмещении суммы перевода денежных средств, осуществленного без добровольного согласия физического лица» (ID 02/07/07-26/00169315) // Федеральный портал проектов нормативных правовых актов. URL: <https://regulation.gov.ru/projects/169315> (дата обращения: 03.09.2026).

<sup>8</sup> Проект постановления Правительства Российской Федерации «Об утверждении критериев абонентских номеров, которые используются в целях совершения телефонных вызовов и (или) направления коротких текстовых сообщений, имеющих признаки совершения противоправных действий, и абонентских номеров, на которые совершаются телефонные вызовы и (или) направляются короткие текстовые сообщения, имеющие признаки совершения противоправных действий» (ID 02/07/07-26/00169312) // Федеральный портал проектов нормативных правовых актов. URL: <https://regulation.gov.ru/projects/169312> (дата обращения: 03.09.2026).

он создаёт сертификаты безопасности, прекращает их действие, подтверждает владение ключом идентификации, ведёт реестр сертификатов безопасности и обеспечивает доступ к нему любым лицам (часть 1 статьи 13.1). Создание, выдача и прекращение действия сертификатов осуществляются с использованием государственной информационной системы национального удостоверяющего центра, оператор которой определяется Правительством Российской Федерации (части 5 и 7 той же статьи). Сертификат безопасности удостоверяет присвоение ключа аутентификации информационной системе или сайту и используется для обеспечения устойчивого и защищённого взаимодействия с ними (часть 1 статьи 14.1). Обязательность применения сертификатов установлена для органов и организаций по части 2.3 статьи 13 Федерального закона «Об информации, информационных технологиях и о защите информации» (часть 12 статьи 14.1), а для банковской сферы может быть установлена Правительством Российской Федерации по согласованию с Банком России (часть 13 той же статьи). Случаи прекращения действия сертификата помимо трёх законных устанавливаются Правительством Российской Федерации (пункт 4 части 7 статьи 14.1); соответствующий проект размещён под идентификатором 02/07/08-26/00170134<sup>9</sup>. Требования к сертификатам и к порядку их создания, выдачи, использования и прекращения действия устанавливаются уполномоченным органом (подпункт «а» пункта 9 части 4 статьи 8 Федерального закона «Об электронной подписи»); проект приказа размещён под идентификатором 02/08/08-26/00170667<sup>10</sup>.

Три системы различаются по субъекту оператора (федеральный орган исполнительной власти, оператор национальной системы платёжных карт, орган или организация, определяемые Правительством Российской Федерации), по кругу пользователей и по характеру обязанности участника. Общим для них является то, что обязанность участника не может быть исполнена без работоспособной системы: оператор по переводу денежных средств не может использовать сведения, которые система не передала, не может запросить систему учёта карт, если она не отвечает, и не может организовать защищённое взаимодействие с применением сертификата, если реестр сертификатов недоступен для проверки его статуса.

<sup>9</sup> Проект постановления Правительства Российской Федерации «О случаях, при которых сертификат безопасности национального удостоверяющего центра прекращает свое действие» (ID 02/07/08-26/00170134, размещён 10.08.2026) // Федеральный портал проектов нормативных правовых актов. URL: <https://regulation.gov.ru/projects/170134> (дата обращения: 03.09.2026).

<sup>10</sup> Проект приказа Минцифры России «Об утверждении требований к сертификатам безопасности национального удостоверяющего центра, порядку создания, выдачи, использования и прекращения действия таких сертификатов» (ID 02/08/08-26/00170667, размещён 28.08.2026) // Федеральный портал проектов нормативных правовых актов. URL: <https://regulation.gov.ru/projects/170667> (дата обращения: 03.09.2026).

## Модель правового режима опорной государственной информационной системы

Для проверки полноты регулирования предлагается описывать правовой режим опорной государственной информационной системы как множество из восьми элементов  $R = \{r1, ..., r8\}$ , каждый из которых отвечает на один вопрос, возникающий у обязанного лица при отказе системы.

r1. Определённость оператора системы и его обязанности обеспечивать её функционирование.

r2. Обусловленность обязанности участника обращением к системе: норма прямо связывает исполнение обязанности с получением сведений из системы или с передачей сведений в неё.

r3. Последствия неисполнения обусловленной обязанности для участника: возмещение, отказ в совершении операции, иная ответственность.

r4. Требования к доступности системы: показатель доступности, предельное время восстановления, порядок плановых работ.

r5. Порядок действий участника при недоступности системы: допустимый альтернативный способ исполнения обязанности либо прямое указание на её приостановление.

r6. Влияние недоступности на течение сроков и наступление ответственности: приостановление сроков, исчисляемых от событий в системе, и освобождение участника от последствий неисполнения за период недоступности.

r7. Фиксация периодов недоступности оператором системы и уведомление участников: доказательственная база, на которую участник может сослаться.

r8. Возможность участника проверить состояние сведений системы на заданный момент: выписка, реестр, журнал, доступный участнику.

Элементы r1, r2, r3 описывают, как система встроена в обязанность участника; элементы r4, r5, r6, r7, r8 описывают режим её недоступности. Для каждой системы и каждого уровня регулирования элемент оценивается как присутствующий (1), присутствующий частично (0,5) или отсутствующий (0). Показатель полноты режима K определяется как отношение суммы оценок к числу элементов; отдельно рассчитывается показатель полноты режима недоступности Kн по элементам r4 — r8. Модель не претендует на измерение качества нормы; она фиксирует, на какие из восьми вопросов текст акта даёт ответ.

Уровни регулирования: L1, федеральный закон в редакции Закона № 210-ФЗ; L2, проект подзаконного акта в первой опубликованной редакции; L3, позиция разработчика по итогам публичного обсуждения, зафиксированная в сводке предложений или в ответе на странице обсуждения. Уровень L3 отражает письменное намерение разработчика; доработанные редакции рассмотренных проектов на момент подготовки статьи не опубликованы, поэтому текстом акта этот уровень не подтверждён.



## **Применение модели**

Система противодействия правонарушениям. На уровне закона элемент r1 присутствует частично: пользователи системы и их обязанности определены, обязанность оператора системы обеспечивать её функционирование и его ответственность перед пользователями в анализируемых нормах не конкретизированы. Элементы r2 и r3 присутствуют полностью: обязанность использовать сведения системы и возмещение при её неисполнении установлены прямо. Элементы r4 — r8 в законе отсутствуют. Проект правил возмещения в первой редакции связывает каждый срок процедуры с событием в системе: датой получения документа считается дата формирования системой уведомления о его доставке (пункт 3 правил), оператор связи клиента определяется оператором системы в срок не более трёх рабочих дней (пункт 8), обращение доставляется системой (пункт 9), сведения о возмещении вносятся в систему (пункт 30), контрольная сверка проводится оператором системы по её неизменяемым журналам (пункты 31 и 32). Проект предусматривает выписки из системы по состоянию на заданный момент времени и неизменяемые журналы (пункт 3 постановления, пункт 7 правил), что даёт элемент r8 и частично элемент r7. Элементы r4, r5 и r6 в первой редакции отсутствуют: текст не отвечает на вопрос, что происходит со сроками, если система не формирует уведомление о доставке.

Автором в ходе публичного обсуждения проекта правил возмещения было направлено предложение о дополнении правил положением, по которому при недоступности системы течение всех сроков, установленных правилами, приостанавливается, периоды недоступности фиксируются в неизменяемых журналах и учитываются при контрольной сверке, а также предложения об увеличении интервала сверки и о сроке перенаправления обращения надлежащему оператору связи. Согласно сводке предложений, сформированной разработчиком 29 июля 2026 г., позиция автора отмечена как частично учтённая: первое и третье предложения отмечены учтёнными, интервал сверки увеличен с четырёх до шести часов вместо предложенных двадцати четырёх с мотивировкой синхронизации с признаками перевода без добровольного согласия, установленными Банком России. Таким образом, на уровне L3 элемент r6 присутствует, а элемент r7 усиливается за счёт фиксации периодов недоступности. Из двух других участников обсуждения позиция одной кредитной организации отмечена как не учтённая, позиция другой как частично учтённая. По проекту критериев абонентских номеров предложения автора, направленные на защиту от внесения в систему номеров добросовестных абонентов и на закрепление порядка исключения сведений, отмечены частично учтёнными, но по существу не приняты: разработчик сообщил, что возможность исключения номера будет реализована технически на едином портале государственных услуг. Для режима недоступности этот результат значе-

ния не имеет, но он показывает, что элемент r8 в части исправления сведений системы разработчик относит к организационному, а не к нормативному уровню.

Единая система учёта платёжных карт. На уровне закона элемент r1 присутствует полностью: оператор назван, обязанность обеспечивать функционирование системы установлена (пункт 1 части 6 статьи 9.2). Элемент r2 присутствует: запрос в систему до предоставления карты обязателен. Элемент r3 присутствует частично: закон устанавливает обязанность отказать в предоставлении карты, но не устанавливает специальных последствий выдачи карты без запроса. Элемент r8 присутствует частично: оператор системы обязан предоставлять сведения, однако форма подтверждения состояния сведений на момент запроса законом не определена. Элементы r4 — r7 отсутствуют. Поскольку подзаконное регулирование отнесено к нормативным актам Банка России, уровни L2 и L3 для этой системы в настоящей работе не оцениваются.

Государственная информационная система национального удостоверяющего центра. На уровне закона элемент r1 присутствует полностью: национальный удостоверяющий центр является федеральным органом, его функции и обязанности перечислены, установлена его ответственность (части 1, 2 и 9 статьи 13.1). Элемент r2 присутствует: обязательность применения сертификатов установлена для определённого круга органов и организаций и может быть распространена на банковскую сферу. Элемент r3 присутствует частично: последствия неприменения сертификата для обязанного лица в рассматриваемых нормах не конкретизированы. Элемент r8 присутствует полностью: реестр сертификатов безопасности с датами и основаниями прекращения действия доступен любым лицам (пункты 4 и 5 части 1 статьи 13.1). Элемент r7 присутствует частично: срок внесения сведений о прекращении действия в реестр установлен только для прекращения по заявлению и по соглашению (часть 8 статьи 14.1) и не установлен для случаев, определяемых Правительством Российской Федерации. Элементы r4, r5 и r6 отсутствуют.

Проект постановления о случаях прекращения действия сертификата в первой редакции содержит четыре случая, текстуально воспроизводящие основания прекращения действия и аннулирования сертификата ключа проверки электронной подписи из частей 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи»: решение суда о недостоверности сведений, прекращение деятельности центра без перехода функций, отсутствие у владельца ключа идентификации, наличие ключа аутентификации в ранее созданном сертификате. Для случаев, описанных безличной конструкцией «если установлено», проект не определяет ни субъекта установления, ни момента прекращения действия. Проект приказа о требованиях к сертификатам в части порядка их создания, выдачи, использования и прекращения действия ограничивается перечнем разделов порядка, который затем утверждает сам

национальный удостоверяющий центр; требований к периодичности издания списков прекративших действие сертификатов, к доступности сервисов проверки статуса и к действиям при недоступности системы центра проект не содержит. Иными словами, на уровне L2 для этой системы элементы r4 — r6 отсутствуют, а элемент r7 остаётся частичным. Предложения автора по обоим проектам, направленные 2 сентября 2026 г. и включающие момент прекращения действия сертификата со дня записи в реестре, срок такой записи, уведомление владельца и порядок действий при недоступности инфраструктуры центра, на момент подготовки статьи результатами рассмотрения не подтверждены: публичное обсуждение первого проекта завершено 7 сентября 2026 г., второго продолжается до 25 сентября 2026 г.

Результаты применения модели сведены в таблицу (табл. 1).

Обозначения: СПП, система противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий; ЕСУПК, единая система учёта платёжных карт; ГИС НУЦ, государственная информационная система национального удостоверяющего центра; L1, L2, L3, уровни регулирования по разделу о модели правового режима. Источник: составлено автором по текстам Закона № 210-ФЗ и изменённых им законов, первых редакций проектов 02/07/07-26/00169315, 02/07/08-26/00170134 и 02/08/08-26/00170667, сводки предложений по проекту 02/07/07-26/00169315 от 29 июля 2026 г.

### Интерпретация

Из значений (табл. 1) следуют три наблюдения.

Первое. На уровне закона показатель полноты режима недоступности не превышает 0,3 ни для одной из трёх систем; для системы противодействия правонарушениям он равен нулю. Закон подробно описывает,

что участник обязан сделать с использованием системы и что произойдёт, если он этого не сделает, но не описывает, что происходит с обязанностью, если система недоступна. Такая асимметрия объяснима генезисом норм: они писались как нормы об обязанностях частных лиц, а система рассматривалась как средство исполнения, надёжность которого презюмируется. В терминах модели А.Н. Метелькова, где информационная система в законодательной конструкции лишена субъекта [1], а требования регулятора должны адресоваться субъекту, обязанному их исполнять [2], можно сказать, что режим недоступности не имеет адресата: обязанность обеспечивать функционирование системы либо вовсе не выражена (система противодействия правонарушениям), либо выражена без показателей и без последствий для участников (единая система учёта платёжных карт, система национального удостоверяющего центра).

Второе. Элементы режима недоступности появляются на подзаконном уровне, причём в наиболее полном виде только по итогам публичного обсуждения. Проект правил возмещения в первой редакции дал элементы r7 и r8, потому что сама процедура сверки требует неизменяемых журналов и выписок; элемент r6 появился в позиции разработчика после предложения участника обсуждения. Для системы национального удостоверяющего центра проекты подзаконных актов элементов r4 — r6 не добавили; порядок, в котором такие элементы могли бы появиться, отнесён к документу самого центра, не проходящему публичное обсуждение. Это согласуется с выводом Н.И. Соловяненко о том, что отсутствие ясности в распределении ответственности является одним из главных факторов, препятствующих доверию к электронным услугам [10]: для сертификата, применение которого обязательно, неопределённость момента прекращения его действия и порядка действий при недоступности реестра прямо влияет на исполнимость обязанности пользователя.

Таблица 1

#### Полнота правового режима опорных государственных информационных систем национальной платёжной системы по уровням регулирования

| Элемент режима                                              | СПП, L1 | СПП, L2 | СПП, L3 | ЕСУПК, L1 | ГИС НУЦ, L1 | ГИС НУЦ, L2 |
|-------------------------------------------------------------|---------|---------|---------|-----------|-------------|-------------|
| r1 оператор и его обязанность обеспечивать функционирование | 0,5     | 0,5     | 0,5     | 1         | 1           | 1           |
| r2 обусловленность обязанности участника                    | 1       | 1       | 1       | 1         | 1           | 1           |
| r3 последствия неисполнения для участника                   | 1       | 1       | 1       | 0,5       | 0,5         | 0,5         |
| r4 требования к доступности                                 | 0       | 0       | 0       | 0         | 0           | 0           |
| r5 порядок действий при недоступности                       | 0       | 0       | 0       | 0         | 0           | 0           |
| r6 влияние недоступности на сроки и ответственность         | 0       | 0       | 1       | 0         | 0           | 0           |
| r7 фиксация недоступности и уведомление                     | 0       | 0,5     | 1       | 0         | 0,5         | 0,5         |
| r8 проверка состояния сведений                              | 0       | 1       | 1       | 0,5       | 1           | 1           |
| <b>К, полнота режима</b>                                    | 0,31    | 0,50    | 0,69    | 0,38      | 0,50        | 0,50        |
| <b>Кн, полнота режима недоступности</b>                     | 0,00    | 0,30    | 0,60    | 0,10      | 0,30        | 0,30        |

Третье. Между тремя системами обнаруживается различие в исходной полноте, объясняемое не значимостью системы, а способом её появления в законе. Единая система учёта платёжных карт и система национального удостоверяющего центра введены статьями, посвящёнными самим системам, поэтому оператор и его обязанности названы ( $r1$  равен единице). Система противодействия правонарушениям введена отдельным законом, а Закон № 210-ФЗ добавляет к нему обязанности пользователей; поэтому в анализируемых нормах обязанность оператора системы перед пользователями остаётся невыраженной. При этом именно для этой системы последствия неисполнения обязанности участника наиболее тяжёлые: возмещение суммы перевода.

### Сравнительно-правовой контекст

Зарубежный опыт показывает, что вопрос о последствиях отказа опорной инфраструктуры для обязанных лиц решается в двух плоскостях. В отношении инфраструктуры открытых ключей Д. Бербекару и А. Лиой показывают, что механизмы отзыва сертификатов реализованы неполно и по-разному в разных программах, отчего статус сертификата остаётся неопределённым для проверяющей стороны [11]. Дискуссия о квалифицированных сертификатах аутентификации сайтов по регламенту Европейского союза показала, что предписание включать определённые сертификаты в программы для доступа к сайтам сталкивается с техническими правилами самих разработчиков программ [12]. Для Российской Федерации эти выводы означают, что обязанность применять сертификаты безопасности национального удостоверяющего центра (часть 12 статьи 14.1) и обязанность обеспечивать их предварительную установку в средствах доступа к сайтам (части 10 и 11 той же статьи) требуют, чтобы статус сертификата был проверяем в любой момент, то есть требуют элементов  $r4$ ,  $r7$  и  $r8$  на нормативном уровне.

В отношении рисков третьих сторон в финансовом секторе регламент Европейского союза об операционной цифровой устойчивости распределяет ответственность за надзор над поставщиками информационно-коммуникационных услуг между финансовыми организациями, регуляторами и самими поставщиками, и в литературе обсуждается, насколько это распределение сбалансировано [13, 14]. Российская конструкция иная: поставщиком опорной услуги выступает государство или уполномоченная им организация, и требования к поставщику устанавливаются не договором с участником, а публично-правовыми нормами. Тем важнее, чтобы эти нормы содержали те элементы, которые в договорной модели обеспечиваются соглашением об уровне обслуживания: показатели доступности, порядок уведомления и последствия простоя. Работы о системном риске концентрации облачных услуг [15] и об устойчивости инфраструктуры доменных имён государственных сервисов [16] подтверждают,

что отказ единого для многих участников узла имеет последствия для всех одновременно; для опорной государственной информационной системы это означает, что режим её недоступности должен быть единым для всех участников и установлен заранее.

### Предложения

С учётом изложенного предлагается следующее.

1. Закрепить на уровне федерального закона общее правило о последствиях недоступности государственной информационной системы для обязанностей, исполнение которых обусловлено обращением к ней: течение сроков, исчисляемых от событий в системе, приостанавливается на период её недоступности; участник не несёт последствий неисполнения обязанности, если неисполнение вызвано недоступностью системы, подтверждённой её оператором. Такое правило может быть включено в Федеральный закон «Об информации, информационных технологиях и о защите информации» применительно ко всем государственным информационным системам либо в каждый из рассмотренных законов отдельно. Первый вариант предпочтительнее: он отвечает предложению о едином правовом режиме защиты таких систем [5] и исключает расхождения между ними.

2. Установить обязанность оператора опорной государственной информационной системы фиксировать периоды недоступности в неизменяемых журналах, информировать пользователей о плановых и нештатных периодах недоступности и выдавать по обращению пользователя подтверждение периода недоступности. Для системы противодействия правонарушениям такой подход уже отражён в позиции разработчика проекта правил возмещения; его следует перенести с уровня правил взаимодействия операторов на уровень акта о самой системе.

3. Для государственной информационной системы национального удостоверяющего центра определить в постановлении о случаях прекращения действия сертификатов момент прекращения действия для случаев, установленных Правительством Российской Федерации, со дня внесения сведений в реестр, срок такого внесения и обязанность уведомления владельца, а в требованиях к порядку создания, выдачи, использования и прекращения действия сертификатов установить периодичность издания списков прекративших действие сертификатов, требования к доступности сервисов проверки статуса и порядок действий при недоступности инфраструктуры центра. Без этого обязанность по части 12 статьи 14.1 остаётся обусловленной системой, режим недоступности которой не определён.

4. Для единой системы учёта платёжных карт предусмотреть в нормативных актах Банка России форму подтверждения состояния сведений системы на момент запроса и порядок действий оператора по переводу денежных средств при отсутствии ответа системы

в установленный срок. Поскольку закон обязывает отказать в предоставлении карты при превышении ограничения, отсутствие ответа системы в его нынешней редакции означает невозможность предоставить карту любому клиенту, что несоразмерно цели нормы.

5. При подготовке подзаконных актов к Закону № 210-ФЗ использовать предложенную модель как перечень контрольных вопросов: акт, вводящий обязанность, обусловленную системой, должен содержать ответы по элементам r4 — r8 либо отсылку к акту, где они содержатся.

### Результаты и выводы

1. Закон № 210-ФЗ ставит исполнение обязанностей операторами по переводу денежных средств и операторами связи в зависимость от трёх государственных информационных систем: системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, единой системы учёта платёжных карт и государственной информационной системы национального удостоверяющего центра. Для каждой из них закон устанавливает обязанность участника и последствия её неисполнения, но не устанавливает режим недоступности системы.

2. Предложенная модель правового режима опорной государственной информационной системы из восьми элементов позволяет измерять полноту регулирования. На уровне закона показатель полноты

режима недоступности составляет от 0 до 0,3 для трёх систем; на уровне проектов подзаконных актов он повышается до 0,3; на уровне позиции разработчика по итогам публичного обсуждения проекта правил возмещения достигает 0,6.

3. Элементы режима недоступности отсутствуют в законе и в первой редакции подзаконного акта и появляются только в результате публичного обсуждения, причём лишь там, где процедура обсуждения предусматривает письменную позицию разработчика. Это делает полноту режима зависимой от участия адресатов регулирования в обсуждении, то есть от фактора, который сам по себе нормативно не гарантирован.

4. Устранение выявленного пробела возможно введением общего правила о последствиях недоступности государственной информационной системы для обусловленных ею обязанностей на уровне федерального закона и конкретизацией элементов r4 — r8 в актах о каждой системе.

Практическое подтверждение и достоверность результатов. Значения показателя рассчитаны по опубликованным текстам актов и проектов и могут быть воспроизведены по указанным в сносках идентификаторам. Результативность предложения о приостановлении сроков подтверждена сводкой предложений разработчика, сформированной 29 июля 2026 г. Ограничение работы состоит в том, что уровень L3 отражает намерение разработчика, а не текст акта; после опубликования доработанных редакций проектов значения показателя подлежат пересчёту.

### Литература

1. Метельков А.Н. Понятие информационной системы: технические и нормативно-правовые аспекты // Правовая информатика. 2025. № 2. С. 112—118.
2. Метельков А.Н. Оператор: многозначность в подходах и функциях в обеспечении информационной безопасности // Правовая информатика. 2026. № 1. С. 43—51. DOI: 10.24412/1994-1404-2026-1-00-04.
3. Троян Н.А. Правовое регулирование цифровых платформ и экосистемы государственных услуг: вектор развития экономики данных в цифровую эпоху // Правовая информатика. 2026. № 1. С. 145—152. DOI: 10.24412/1994-1404-2026-1-00-15.
4. Полякова Т.А., Троян Н.А. Трансформация государственного управления в Российской Федерации: от кибернетики, информатики к цифровизации // Правовая информатика. 2025. № 4. С. 215—226.
5. Дубень А.К. Правовое обеспечение информационной безопасности Российской Федерации: нормативно-правовые основы и современные вызовы // Правовая информатика. 2026. № 1. С. 284—288. DOI: 10.24412/1994-1404-2026-1-00-31.
6. Ловцов Д.А., Бурый А.С. Кибербезопасность: основные тенденции в обеспечении // Правовая информатика. 2024. № 2. С. 23—34.
7. Хадеева М.В., Овчинников Е.К. Правовые основы функционирования антифрод-системы на финансовом рынке // Вестник Университета им. О.Е. Кутафина (МГЮА). 2025. № 8 (132). С. 164—172. DOI: 10.17803/2311-5998.2025.132.8.164-172.
8. Гаужаева В.А., Прокофьева Е.В. Отдельные аспекты эволюции противодействия кибермошенничеству // Право и управление. 2026. № 4. С. 470—474.
9. Шувалов П.С., Оганова Н.В. Развитие правового механизма дистанционного банковского обслуживания в условиях цифровизации // Юридическая наука. 2023. № 4. С. 187—191.
10. Соловяненко Н.И. Юридические функции и ответственность лиц, оказывающих доверенные услуги в цифровой бизнес-среде // Право и практика. 2021. № 4. С. 138—144. DOI: 10.24412/2411-2275-2021-4-138-144.



11. Berbecaru D.G., Liyo A. An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem // IEEE Access. 2023. Vol. 11. P. 79156—79175. DOI: 10.1109/ACCESS.2023.3299357.
12. Entschew E., Hall K., Bailey C., Nguyen K. A New eIDAS Beginning for QWACs // Datenschutz und Datensicherheit — DuD. 2022. Vol. 46. No. 4. P. 217—224. DOI: 10.1007/s11623-022-1591-x.
13. Wittlin J., Ossowska A., Sawicka K. Is DORA an opportunity for more balanced distribution of third-party risk management assurance responsibilities between banks, regulators and technology providers? // Information & Communications Technology Law. 2025. Vol. 35. No. 1. P. 109—116. DOI: 10.1080/13600834.2025.2514385.
14. Pierides M., Mulligan J. Key themes of resiliency, outsourcing and third-party risk management regimes // Journal of Securities Operations & Custody. 2025. Vol. 17. No. 2. P. 102. DOI: 10.69554/AUIQ5402.
15. Harmon R.L., Vytelingum P., Babaie-Harmon J. Cloud concentration risk: A framework agent-based model for systemic risk analysis // Journal of Financial Compliance. 2021. Vol. 4. No. 3. P. 232. DOI: 10.69554/SGUT4817.
16. Septiadi A., Lyu M., Habibi Gharakheili H., Sivaraman V. Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2026. Vol. 10. No. 2. P. 1—30. DOI: 10.1145/3805629.

**SECTION**  
**REGULATORY INFORMATICS**

## STATE INFORMATION SYSTEMS AS THE SUPPORTING INFRASTRUCTURE OF THE NATIONAL PAYMENT SYSTEM: THE LEGAL REGIME OF UNAVAILABILITY

*Lobanov N.A.*<sup>11</sup>

**Keywords:** fraud prevention, funds transfer without the client's voluntary consent, money transfer operator, telecommunications operator, security certificate, certification authority, operator duties, time limits for performance of duties, liability, continuity of operation, public consultation on draft regulations.

### **Abstract**

**Purpose:** to establish which provisions govern the consequences of unavailability of state information systems for participants required, from 2027, to use such systems, and to propose a model of the completeness of that legal regime.

**Research method:** formal legal analysis of Federal Law No. 210-FZ of 26 June 2026, the laws it amends and the related draft regulations of July and August 2026. The comparative method covers trust service liability and the allocation of third-party risk in the financial sector. The study draws on materials of the public consultation on four drafts; their analysis makes it possible to assess the completeness of the regulation against an author's model applied to the statute, the drafts and developers' recorded positions.

**Results:** three state information systems are identified whose use is a condition for the duties of money transfer and telecommunications operators: the system for countering offences committed with the use of information and communication technologies, the unified payment card register and the state information system of the national certification authority. For each the law imposes a duty and prescribes the consequences of non-performance, but sets no availability requirements, no procedure during downtime and no rule on how downtime affects time limits and liability. An eight-element model of the regime and a completeness index are proposed and calculated. Elements of the unavailability regime emerge only at the secondary level and only through public consultation: the developer of the draft compensation rules marked the proposal to suspend time limits during unavailability as accepted. Enshrining the regime in federal law is proposed.

---

<sup>11</sup> **Nikolay A. Lobanov**, independent expert in information security and critical information infrastructure protection; master's student at the Institute of Law and National Security, Russian Presidential Academy of National Economy and Public Administration, Moscow, Russian Federation. ORCID: 0009-0006-8187-4528.

E-mail: [nlobanov-25@ranepa.ru](mailto:nlobanov-25@ranepa.ru)

## References

1. Metel'kov A.N. Poniatie informatsionnoi sistemy: tekhnicheskie i normativno-pravovye aspekty // Pravovaia informatika. 2025. No. 2. S. 112—118.
2. Metel'kov A.N. Operator: mnogoznachnost' v podkhodakh i funktsiiakh v obespechenii informatsionnoi bezopasnosti // Pravovaia informatika. 2026. No. 1. S. 43—51. DOI: 10.24412/1994-1404-2026-1-00-04.
3. Troian N.A. Pravovoe regulirovanie tsifrovyykh platform i ekosistemy gosudarstvennykh uslug: vektor razvitiia ekonomiki dannykh v tsifrovuiu epokhu // Pravovaia informatika. 2026. No. 1. S. 145—152. DOI: 10.24412/1994-1404-2026-1-00-15.
4. Poliakova T.A., Troian N.A. Transformatsiia gosudarstvennogo upravleniia v Rossiiskoi Federatsii: ot kibernetiki, informatiki k tsifrovizatsii // Pravovaia informatika. 2025. No. 4. S. 215—226.
5. Duben' A.K. Pravovoe obespechenie informatsionnoi bezopasnosti Rossiiskoi Federatsii: normativno-pravovye osnovy i sovremennye vyzovy // Pravovaia informatika. 2026. No. 1. S. 284—288. DOI: 10.24412/1994-1404-2026-1-00-31.
6. Lovtsov D.A., Buryi A.S. Kiberbezopasnost': osnovnye tendentsii v obespechenii // Pravovaia informatika. 2024. No. 2. S. 23—34.
7. Khadeeva M.V., Ovchinnikov E.K. Pravovye osnovy funktsionirovaniia antifrod-sistemy na finansovom rynke // Vestnik Universiteta im. O.E. Kutafina (MGLU). 2025. No. 8 (132). S. 164—172. DOI: 10.17803/2311-5998.2025.132.8.164-172.
8. Gauzhaeva V.A., Prokof'eva E.V. Otdel'nye aspekty evoliutsii protivodeistviia kibermoshennichestvu // Pravo i upravlenie. 2026. No. 4. S. 470—474.
9. Shuvalov P.S., Oganova N.V. Razvitie pravovogo mekhanizma distantsionnogo bankovskogo obsluzhivaniia v usloviakh tsifrovizatsii // Iuridicheskaya nauka. 2023. No. 4. S. 187—191.
10. Solovianenko N.I. Iuridicheskie funktsii i otvetstvennost' lits, okazyvaiushchikh doverennye uslugi v tsifrovoi biznes-srede // Pravo i praktika. 2021. No. 4. S. 138—144. DOI: 10.24412/2411-2275-2021-4-138-144.
11. Berbecaru D.G., Liou A. An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem // IEEE Access. 2023. Vol. 11. P. 79156—79175. DOI: 10.1109/ACCESS.2023.3299357.
12. Entschew E., Hall K., Bailey C., Nguyen K. A New eIDAS Beginning for QWACs // Datenschutz und Datensicherheit — DuD. 2022. Vol. 46. No. 4. P. 217—224. DOI: 10.1007/s11623-022-1591-x.
13. Wittlin J., Ossowska A., Sawicka K. Is DORA an opportunity for more balanced distribution of third-party risk management assurance responsibilities between banks, regulators and technology providers? // Information & Communications Technology Law. 2025. Vol. 35. No. 1. P. 109—116. DOI: 10.1080/13600834.2025.2514385.
14. Pierides M., Mulligan J. Key themes of resiliency, outsourcing and third-party risk management regimes // Journal of Securities Operations & Custody. 2025. Vol. 17. No. 2. P. 102. DOI: 10.69554/AUIQ5402.
15. Harmon R.L., Vytelingum P., Babaie-Harmon J. Cloud concentration risk: A framework agent-based model for systemic risk analysis // Journal of Financial Compliance. 2021. Vol. 4. No. 3. P. 232. DOI: 10.69554/SGUT4817.
16. Septiadi A., Lyu M., Habibi Gharakheili H., Sivaraman V. Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2026. Vol. 10. No. 2. P. 1—30. DOI: 10.1145/3805629.



# ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ПОЖАРНОЙ БЕЗОПАСНОСТИ

Попова С.В.<sup>1</sup>

**Ключевые слова:** сверточные нейронные сети, видеонаблюдение, машинное обучение, автоматические системы, ложное срабатывание, модель, пожар, обнаружение пожара, технологии.

## Аннотация

**Цель работы:** состоит в обосновании применения искусственного интеллекта в области обеспечения пожарной безопасности на объектах защиты.

**Метод исследования:** методологическую основу составили анализ научных источников по проблематике обеспечения пожарной безопасности с внедрением интеллектуальных систем, а также обобщение результатов исследований, посвященных применению технологий искусственного интеллекта для раннего обнаружения возгораний и его тушения.

**Результаты исследования:** установлено, что искусственный интеллект позволяет автоматизировать обработку данных с датчиков, камер видеонаблюдения, обеспечивая обнаружения возгорания на ранней стадии его развития. Наибольшую эффективность показывают комплексные системы, объединяющие компьютерное зрение, сенсорные данные и прогнозные модели. Предложена функциональная схема, разделяющая сбор и проверку данных, аналитическую обработку, представление информации оператору и взаимодействие с противопожарной автоматикой. Показано, что практическую пригодность модели необходимо оценивать не только по точности классификации, но и по времени обнаружения, частоте ложных тревог, доле пропущенных событий и устойчивости к изменению условий наблюдения. Обоснована целесообразность объединения визуальных и физических признаков с учетом качества каждого источника.

**Практическая значимость:** заключается во внедрении интеллектуальных систем на различных объектах защиты. Применение искусственного интеллекта способствует сокращению времени обнаружения пожара, снижению ложных вызовов. Для большей эффективности данные технологии должны дополнять, а не заменять сертифицированные средства противопожарной защиты.

DOI: 10.24412/1994-1404-2026-3-295-301

## Введение

Ежегодно на территории Российской Федерации происходят сотни тысяч пожаров, последствия от которых выражаются в огромных показателях гибели и травмировании людей, а также значительных материальных потерь как для общества, так и государства в целом. Согласно статистическим данным МЧС России, только за 2025 год произошло 317 482 случая возгораний, на которых зафиксирована гибель людей в количестве 6571 человека и 7986 случаев получения травм. Материальные потери составили свыше 29,2 млрд рублей, а основными причинами пожаров стали неосторожное обращение с огнем и нарушение

правил устройства и эксплуатации электрического оборудования<sup>2</sup>.

Несмотря на то, что наблюдается положительная динамика снижения общего числа пожаров, показатели имеют высокие значения и необходимо продолжать работу в области предупреждения пожаров, а в случае их возникновения — совершенствования мероприятий по их ликвидации [1], поэтому своевременное обнаружение пожара остается одной из важных задач по защите людей и материальных ценностей.

Традиционные автоматические системы обнаружения пожара основываются на применении тепловых,

<sup>2</sup> Пожары и пожарная безопасность в 2025 году. Статистика пожаров и их последствий: информационно-аналитический сборник. Балашиха : ФГБУ ВНИИПО МЧС России, 2026. 113 с.

<sup>1</sup> **Попова Светлана Вячеславовна**, старший преподаватель кафедры пожаротушения и аварийно-спасательных работ Уральского института ГПС МЧС России, г. Екатеринбург, Российская Федерация.  
E-mail: vip.sveta79@bk.ru

дымовых, газовых, оптических и комбинированных извещателей<sup>3</sup>. Данные устройства обеспечивают обнаружение определенных факторов пожара, которые могут давать ложные сигналы срабатывания из-за появления пыли, пара или других факторов. При этом обычные извещатели срабатывают как один показатель, например при повышении температуры или появления высокой концентрации продуктов горения (дыма), при этом они не всегда способны выявить признаки возгорания на начальном этапе развития пожара.

На сегодняшний день, одним из важных направлений является применение искусственного интеллекта, позволяющего оперативно получать и обрабатывать данные, выявлять признаки возгораний и снижать время реагирования экстренных служб [2].

Искусственный интеллект представляет интерес там, где необходимо обработать большой объем неоднородных данных и выявить сочетания признаков, которые трудно описать небольшим набором фиксированных правил. К таким задачам относятся анализ видеопотока, распознавание нестандартных режимов работы оборудования и сопоставление информации от пространственно распределенных датчиков.

Вместе с тем результат распознавания не равнозначен доказанной надежности всей системы. Алгоритм может успешно работать на подготовленной выборке и допускать ошибки после изменения освещения, положения камеры либо состава наблюдаемых объектов. Снижение количества ложных срабатываний в лабораторном эксперименте не гарантирует такого же эффекта на производственной площадке. Следовательно, оценивать применение искусственного интеллекта следует не только с позиции возможностей модели, но и с учетом места этой модели в общей организации противопожарной защиты.

Развитие технологий искусственного интеллекта создает условия для перехода от простого контроля пороговых значений к комплексному анализу данных. Алгоритмы машинного обучения способны выявлять скрытые зависимости, классифицировать наблюдаемые события, прогнозировать развитие опасной ситуации и оперативно передавать информацию для реагирования экстренным службам, а также сократить количество ложных тревог [2—4].

Проблема исследования заключается в определении условий, при которых интеллектуальная обработка данных дает практически полезную информацию, не создавая при этом новых недопустимых зависимостей. Для ее рассмотрения необходимо разграничить обнаружение события, прогнозирование его развития и выдачу команд исполнительным устройствам. Эти функции связаны между собой, но различаются

по исходным данным, последствиям ошибок и требованиям к подтверждению результатов.

### Основная часть

На сегодняшний день одним из перспективным направлением является автоматический анализ изображений с камер видеонаблюдения. Алгоритмы компьютерного зрения распознают дым и открытое пламя по цветовым, текстурным, геометрическим и динамическим характеристикам. Сверточные нейронные сети (СНС) способны автоматически выделять информативные признаки изображения, что позволяет обнаруживать возгорания на открытых территориях, складах, производственных объектах и в помещениях с высокими потолками, где традиционный дымовой извещатель может сработать с задержкой [5].

Видеонаблюдение позволяет контролировать пространство на расстоянии и получать изображение участка, где предположительно развивается пожар. Это представляет интерес для открытых площадок, протяженных производственных зон и помещений, в которых движение дыма до установленного извещателя зависит от высоты, вентиляции и расположения оборудования. Вместе с тем видеокамера фиксирует только доступные ей визуальные признаки. Если очаг закрыт конструкциями, находится вне поля зрения или не создает различимых изменений изображения, алгоритм не получает достаточной информации для обнаружения.

Для практического использования важен анализ последовательности кадров. Отдельное изображение не всегда позволяет отличить дым от облака пыли или пламя от отражения. Временные признаки дают дополнительную информацию о появлении, перемещении и изменении наблюдаемой области. Однако требование подтвердить событие на нескольких последовательных кадрах создает задержку. Чем продолжительнее интервал подтверждения, тем выше риск потерять часть выигрыша от раннего обнаружения. Поэтому его выбор должен проверяться совместно с оценкой ложных тревог.

Условия получения изображения способны влиять на результат не меньше, чем архитектура модели. Существенны положение камеры, размер предполагаемого очага в кадре, контраст с фоном, засветка, степень сжатия видео и загрязнение защитного стекла. Один и тот же алгоритм может давать различные результаты на двух внешне сходных площадках. По этой причине приемочные испытания должны включать реальные положения камер и характерные режимы освещения, а не ограничиваться воспроизведением демонстрационных видеозаписей.

Важное значение приобретает и состав отрицательных примеров — ситуаций, в которых пожара нет. Для промышленного объекта к ним могут относиться сварочные работы, выброс пара, движение запыленного транспорта и изменение освещения при открытии ворот. Для общественного здания набор помех будет

<sup>3</sup> Тенденции развития автоматических пожарных извещателей / А.В. Федоров, Т.А. Буцынская, А.А. Лукьянченко, Ч.Д. Хынг // Пожары и чрезвычайные ситуации: предотвращение, ликвидация. 2009. № 2. С. 111—114. EDN: NTRBGX.



другим. Если такие сцены отсутствовали при подготовке и проверке модели, ее работа в условиях объекта остается неопределенной, даже когда общая точность на исходной выборке высока.

Алгоритмы машинного обучения могут использоваться не только для фиксации возникшего пожара, но и для прогнозирования условий его появления. Источниками таких данных выступают различные сведения в том числе об оборудовании, вентиляции, температуре, пожарной нагрузке и выявленные ранее нарушения. Это позволяет произвести моделирование развития пожара и выявить угрозу для людей в процессе их эвакуации из здания [6, 7]. Кроме того, интеллектуальная система может анализировать данные камер, извещателей и систем контроля доступа, после чего рекомендовать наиболее безопасные маршруты.

Следует различать обнаружение признаков горения и выявление предпосылок его возникновения. В первом случае система анализирует уже появившиеся проявления опасного процесса. Во втором — рассматривает отклонения, которые могут предшествовать пожару, но не обязательно приведут к нему. Например, необычный температурный режим электрического оборудования служит основанием для проверки технического состояния, однако сам по себе не подтверждает наличие горения. Объединение этих двух задач без соответствующих пояснений способно вызвать ненужную тревогу и привести к неправильному выбору действий.

Отдельную группу составляет поддержка принятия решений после подтверждения события. Здесь требуется не столько классифицировать изображение, сколько представить сведения о месте возникновения пожара, доступности помещений, состоянии инженерных систем и возможных направлениях распространения опасных факторов. Полезность аналитического модуля определяется тем, сокращает ли он время поиска значимой информации и помогает ли оператору понять ситуацию. Избыточное количество уведомлений может дать противоположный результат.

Также необходимо подчеркнуть, что не всякая задача нуждается в машинном обучении. Если опасное состояние надежно определяется по известному физическому критерию и условия наблюдения устойчивы, применение формализованного алгоритма может быть более прозрачным и экономически оправданным. Интеллектуальная модель имеет смысл тогда, когда ее вклад можно установить сравнением с таким исходным решением. Поэтому необходимость внедрения следует подтверждать не общим интересом к технологии, а выявленным недостатком существующего информационного процесса.

Интеллектуальный анализ повышает эффективность профилактической работы, поскольку позволяет переходить от планового обслуживания к обслуживанию по фактическому техническому состоянию. При этом прогноз модели не должен рассматриваться как достаточное основание для отмены обязательных регламентных мероприятий.

Помимо профилактики, искусственный интеллект применяется непосредственно при возникновении пожара, в частности в робототехнических системах для разведки и работы в опасных для человека условиях. Подобный подход представлен в исследовании А.У. Актаевой, Т.Д. Жаксылыка и Ж.И. Сарсенбаевой, рассматривающих искусственный интеллект как средство повышения эффективности управления пожаротушением и противопожарного надзора [8]. Авторы также отмечают необходимость дальнейшей доработки и детального изучения интеллектуальных платформ пожарной безопасности.

Пожарные роботы могут применяться для разведки, передачи изображения, измерения температуры и концентрации токсичных веществ. Использование автономных устройств особенно актуально на химических предприятиях, складах горючих материалов, энергетических объектах и в помещениях с риском обрушения. Алгоритмы искусственного интеллекта обеспечивают распознавание препятствий, построение карты помещения, выбор маршрута и идентификацию очага. Однако полностью автономное принятие решений ограничивается возможными ошибками навигации и распознавания. Поэтому предпочтительным является режим, при котором робот выполняет отдельные операции самостоятельно, но сохраняет связь с оператором [9]. Это позволяет использовать автоматизацию для отдельных операций, не передавая системе неопределенный круг решений с потенциально тяжелыми последствиями.

Кроме того, необходима заранее установленная логика поведения при потере связи. Универсального решения здесь нет: остановка может быть приемлемой в одной ситуации и создавать препятствие в другой, а возвращение по прежнему маршруту может оказаться невозможным после изменения обстановки. Следовательно, режим отказа должен определяться с учетом конструкции комплекса и условий применения. Его работоспособность следует проверять отдельно от качества распознавания объектов. Сведения, полученные робототехническим комплексом, полезны лишь при возможности связать их с местом и временем наблюдения. Изображение высокой температуры без понятной пространственной привязки ограничено пригодно для принятия решений. Поэтому в информационном интерфейсе необходимо указывать положение комплекса, направление наблюдения, актуальность данных и статус связи. Роботизированная разведка в таком случае становится дополнительным источником проверяемой информации, а не изолированной демонстрацией автономности.

Таким образом, робототехнические системы являются одним из перспективных инструментов повышения эффективности и безопасности действий при пожаре. Однако применение искусственного интеллекта не ограничивается роботизированной разведкой и тушением, а охватывает широкий круг задач — от раннего обнаружения возгорания до прогнозирования рисков и управления эвакуацией (табл. 1).

Основные направления применения искусственного интеллекта

| НАПРАВЛЕНИЕ                  | ИСХОДНЫЕ ДАННЫЕ                               | ПРИМЕНЯЕМЫЕ МЕТОДЫ                            | ОЖИДАЕМЫЙ РЕЗУЛЬТАТ                         |
|------------------------------|-----------------------------------------------|-----------------------------------------------|---------------------------------------------|
| Обнаружение дыма и пламени   | Изображения и видеопотоки                     | Сверточные нейронные сети, детекторы объектов | Раннее визуальное обнаружение пожара        |
| Анализ показаний извещателей | Температура, дым, газы, влажность             | Классификация, анализ временных рядов         | Снижение количества ложных тревог           |
| Прогнозирование риска        | История эксплуатации и состояние оборудования | Регрессия, деревья решений, нейронные сети    | Выявление потенциально опасных участков     |
| Контроль оборудования        | Телеметрия и журналы обслуживания             | Поиск аномалий, предиктивная аналитика        | Прогнозирование отказов                     |
| Поддержка эвакуации          | Камеры, извещатели, системы доступа           | Компьютерное зрение, оптимизация маршрутов    | Выбор безопасных путей движения             |
| Мониторинг территорий        | Спутниковые снимки, данные БПЛА               | Сегментация изображений, прогнозные модели    | Обнаружение и оценка распространения пожара |
| Пожарная разведка            | Данные роботов и тепловизоров                 | Навигация, распознавание объектов             | Снижение риска для личного состава          |

Таблица 2

Архитектура интеллектуальной системы пожарной безопасности

| УРОВЕНЬ АРХИТЕКТУРЫ        | КОМПОНЕНТЫ                                                   | ОСНОВНЫЕ ФУНКЦИИ                                                                                        |
|----------------------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 1. Сбор данных             | Датчики, видеокамеры, тепловизоры, системы диспетчеризации   | Получение информации о состоянии объекта и возможных признаках пожара                                   |
| 2. Обработка данных        | Модули фильтрации, синхронизации и предварительной обработки | Устранение помех, согласование и подготовка данных для анализа                                          |
| 3. Интеллектуальный анализ | Модели искусственного интеллекта                             | Оценка вероятности пожара, проверка тревожных сигналов, ранжирование рисков и прогнозирование сценариев |
| 4. Управление и оповещение | Интерфейс оператора, противопожарная автоматика              | Передача предупреждений оператору и взаимодействие с системами противопожарной защиты                   |

Приведенные результаты являются возможными направлениями полезного применения, а не гарантированными эффектами внедрения. Для каждого объекта необходимо установить, какая информация отсутствует в действующей системе и может ли предлагаемый модуль восполнить этот недостаток. Такой порядок позволяет избежать установки аналитики, которая дублирует существующие функции и увеличивает нагрузку на персонал без подтвержденной пользы.

Архитектура интеллектуальной системы пожарной безопасности должна включать несколько взаимосвязанных уровней (табл. 2), где ключевым принципом является разделение функций. Искусственный интеллект может выполнять прогнозирование, ранжирование рисков и проверку тревожных сигналов, однако критически важные команды должны обрабатываться сертифицированными техническими средствами и резервироваться детерминированными алгоритмами. Для

сохранения работоспособности при потере связи целесообразно применять периферийные вычисления. В этом случае обработка данных осуществляется непосредственно на объекте, а не только на удаленном сервере.

Предлагаемая архитектура состоит не в закреплении единственной технической реализации, а в обозначении границ ответственности компонентов. Эти границы необходимы для проверки, обслуживания и анализа причин ошибочных сообщений.

На первом уровне выполняются получение измерений и контроль доступности источников. Помимо полезного сигнала фиксируются сведения об исправности устройства, временной отметке и состоянии связи. На втором уровне данные согласуются и подготавливаются к обработке. Здесь выявляются пропуски, задержки и очевидные нарушения формата. Предварительная обработка должна сохранять информацию о проблеме

мах источника, а не скрывать ее за технически удобным заполнением отсутствующих значений. Третий уровень включает модели распознавания и правила объединения результатов. Целесообразно, чтобы выход этого уровня содержал описание события, пространственную привязку и указание на недостаточность либо противоречивость данных. Четвертый уровень предназначен для оператора: он представляет информацию в понятной форме, позволяет просмотреть исходные материалы и фиксирует действия персонала.

Взаимодействие с противопожарной автоматикой рассматривается отдельно. В предлагаемой схеме интеллектуальный модуль не блокирует штатное обнаружение и выполнение предусмотренных защитных функций. Если его результаты предполагается использовать для управления, соответствующая логика должна быть выделена, документирована и проверена. Нельзя считать безопасной схему, в которой отказ аналитического сервера незаметно прекращает выполнение базовых функций.

Интеллектуальная система зависит от программного обеспечения, каналов передачи и качества исходной информации. Искажение временных отметок, подмена видеопотока или несанкционированное изменение параметров способны повлиять на результат без физического повреждения датчиков. Поэтому разграничение доступа, регистрация изменений и контроль целостности конфигурации необходимо рассматривать как часть надежности мониторинга.

При объединении с другими инженерными системами следует ограничивать объем доступных команд. Если аналитическому модулю требуется только получать состояние оборудования, предоставление ему широких прав управления создает ненужный риск. Интерфейсы должны соответствовать фактической функции. Такой подход упрощает проверку и уменьшает вероятность распространения отказа из вспомогательного программного компонента на другие элементы объекта.

Журналирование необходимо не только для последующего расследования инцидента. Оно позволяет оценить повторяемость помех, выявить проблемные камеры и проверить, что происходило между обнаружением признака и действием оператора. В журнале полезно связывать исходное сообщение, версию модели, состояние каналов и ответ персонала. Без этой связи причины ошибки могут остаться неясными, а корректирующие действия — свестись к необоснованной настройке порога.

Человеческий фактор проявляется в двух противоположных формах. Частые ложные предупреждения приводят к снижению внимания, тогда как длительная безошибочная работа способна вызвать чрезмерное доверие к автоматике. В обоих случаях оператор перестает критически оценивать сообщения. Поэтому обучение должно включать не только штатный порядок работы, но и примеры неопределенных, противоречивых и ошибочных результатов.

Интерфейс должен помогать проверять сообщение, а не создавать впечатление безусловной достоверности. Полезны изображение контролируемого участка, состояние источников и краткое объяснение выявленных признаков. Формулировки следует выбирать с учетом фактической функции: «обнаружены признаки дыма» точнее передает результат видеоклассификатора, чем категоричное заключение о характере и масштабе пожара.

К ограничениям внедрения искусственного интеллекта в систему обеспечения пожарной безопасности можно отнести следующие.

- Недостаток репрезентативных данных. Реальные записи пожаров получить сложно, а проведение натурных испытаний требует значительных ресурсов. Использование преимущественно лабораторных данных может привести к снижению качества модели в реальных условиях.
- Изменение условий эксплуатации. Камера может быть перемещена, ее объектив — загрязнен, а освещение — изменено. В результате распределение входных данных будет отличаться от использованного при обучении модели.

Основными рисками являются: ложные срабатывания и пропуск опасного события; недостаточная интерпретируемость решения; зависимость от качества и доступности связи; возможность несанкционированного доступа; подмена или искажение информации от датчиков и др.

Важно отметить, что применение только видеокамеры или отдельного интеллектуального датчика не обеспечивает необходимой надежности во всех возможных условиях. Более устойчивым является мультимодальный подход, при котором решение формируется на основании независимых физических признаков.

Внедрение искусственного интеллекта не должно приводить к исключению традиционных средств пожарной защиты. Нейросетевая модель может ошибаться при появлении ранее неизвестных объектов или условий. Поэтому рациональным является гибридный подход, объединяющий возможности машинного обучения с формализованными правилами и сертифицированной противопожарной автоматикой.

### Заключение

Таким образом, искусственный интеллект в обеспечении пожарной безопасности является перспективным инструментом ее развития. Его применение способствует обнаружению пожара на ранней стадии его развития с последующей минимизацией последствий от него. Основным преимуществом внедрения таких технологий является проведение анализа большого объема получаемых данных и выявление сложных зависимостей, которые трудно учесть с помощью традиционных пороговых алгоритмов.

## Литература

1. Дьяков В.Ф. Анализ основных показателей по пожарам в Российской Федерации в период с 2021 по 2025 год // Российский научный вестник. 2026. № 2. С. 69—73. DOI: 10.24412/2782-3830-2026-2-69-73. EDN: DSCIOG.
2. Соклаков Р.А. Возможности применения ИИ в сфере обеспечения пожарной безопасности // Вестник науки. 2024. Т. 1. № 12 (81). С. 1558—1561. EDN: VJNWZW.
3. Хабибрахманов Э.И., Аксенов С.Г., Харисова З.И. Использование возможностей искусственного интеллекта в области пожарной безопасности // Человек. Социум. Общество. 2022. № 14. С. 37—42. EDN: ZUSEKX.
4. Щенина С.В., Губайдуллина И.Н. Искусственный интеллект и пожарная безопасность // Экономика и безопасность. 2025. № 7. С. 158—160. EDN: IPFUXO.
5. Калиев Д.И., Швеиц О.Я. Свёрточные нейронные сети для решения задач обнаружения пожаров по данным аэрофотосъемки // Программные системы: теория и приложения. 2022. Т. 13. № 1 (52). С. 195—213. DOI: 10.25209/2079-3316-2022-13-1-195. EDN: MEPMJM.
6. Мураев Н.П., Карапузиков А.А. Компьютерное моделирование развития пожара и эвакуации в зданиях массового пребывания людей // Правовая информатика. 2025. № 4. С. 127—134. DOI: 10.24412/1994-1404-2025-4-127-134. EDN: NRUOVD.
7. Мельников Г.О., Турсенев С.А. Интеграция технологии искусственного интеллекта для повышения эффективности эвакуации людей при пожаре // Природные и техногенные риски (физико-математические и прикладные аспекты). 2023. № 4 (48). С. 30—36. DOI: 10.61260/2307-7476-2024-2023-4-30-36. EDN: DDHLPZ.
8. Актаева А.У., Жаксылык Т.Д., Сарсенбаева Ж.И. Искусственный интеллект и пожарная безопасность // НИР. 2023. № 1 (13). С. 133—137.
9. Щепетов Н.С., Кропотова Н.А. Искусственный интеллект и пожарная безопасность: роль и практические разработки // Актуальные вопросы совершенствования инженерных систем обеспечения пожарной безопасности объектов : сб. мат. XII Всерос. науч.-практ. конф., Иваново, 22 апреля 2025 г. Иваново : Ивановская пожарно-спасательная академия ГПС МЧС России, 2025. С. 462—468. EDN: VKSCJB.

SECTION:  
REGULATORY INFORMATICS

# THE USE OF ARTIFICIAL INTELLIGENCE IN ENSURING FIRE SAFETY

Popova S. V.<sup>4</sup>

**Keywords:** *convolutional neural networks, video surveillance, machine learning, automatic systems, false alarm, model, fire, fire detection, technologies.*

## Abstract

**Purpose of work:** *to substantiate the application of artificial intelligence in fire safety at protected facilities.*

**Research method:** *The methodological basis of the study included an analysis of scientific sources on fire safety provision through the implementation of intelligent systems, as well as a generalization of research findings on the use of artificial intelligence technologies for the early detection and suppression of fires.*

**Results of the study:** *It was established that artificial intelligence makes it possible to automate the processing of data from sensors and video surveillance cameras, thereby ensuring the detection of fires at an early stage of their development. Integrated systems combining computer vision, sensor data, and predictive models demonstrate the highest efficiency. A functional scheme was proposed that separates data collection and verification, analytical processing, information presentation to the operator, and interaction with fire protection automation systems. It was shown that the practical applicability of a model should be evaluated not only by classification accuracy, but also by detection time, false alarm frequency, the proportion of missed events, and resilience to changing observation conditions. The feasibility of combining visual and physical features while considering the quality of each data source was substantiated.*

---

<sup>4</sup> **Svetlana V. Popova**, Senior Lecturer, Department of Firefighting and Emergency Rescue Operations, Ural Institute of the State Fire Service of the Ministry of Emergency Situations of Russia, Ekaterinburg, Russian Federation.  
E-mail: [vip.sveta79@bk.ru](mailto:vip.sveta79@bk.ru)



**Practical value:** The results can be applied to the implementation of intelligent systems at various protected facilities. The use of artificial intelligence contributes to reducing fire detection time and the number of false alarms. To ensure greater effectiveness, these technologies should complement, rather than replace, certified fire protection systems.

## References

1. D'iakov V.F. Analiz osnovnykh pokazatelei po pozharam v Rossiiskoi Federatsii v period s 2021 po 2025 god // Rossiiskii nauchnyi vestnik. 2026. No. 2. S. 69—73. DOI: 10.24412/2782-3830-2026-2-69-73. EDN: DSCIOG.
2. Soklakov R.A. Vozmozhnosti primeneniia II v sfere obespecheniia pozharnoi bezopasnosti // Vestnik nauki. 2024. T. 1. No. 12 (81). S. 1558—1561. EDN: VJNWZW.
3. Khabibrakhmanov E.I., Aksenov S.G., Kharisova Z.I. Ispol'zovanie vozmozhnostei iskusstvennogo intellekta v oblasti pozharnoi bezopasnosti // Chelovek. Sotsium. Obshchestvo. 2022. No. 14. S. 37—42. EDN: ZUSEKX.
4. Shchenina S.V., Gubaidullina I.N. Iskusstvennyi intellekt i pozharnaia bezopasnost' // Ekonomika i bezopasnost'. 2025. No. 7. S. 158—160. EDN: IPFUXO.
5. Kaliev D.I., Shvets O.Ia. Svertochnye neironnye seti dlia resheniia zadach obnaruzheniia pozharov po dannym aerofotos'emki // Programmnye sistemy: teoriia i prilozheniia. 2022. T. 13. No. 1 (52). S. 195—213. DOI: 10.25209/2079-3316-2022-13-1-195. EDN: MEPXJM.
6. Muraev N.P., Karapuzikov A.A. Komp'iuternoe modelirovanie razvitiia pozhara i evakuatsii v zdaniakh massovogo prebyvaniia liudei // Pravovaia informatika. 2025. No. 4. S. 127—134. DOI: 10.24412/1994-1404-2025-4-127-134. EDN: NRUOVD.
7. Mel'nikov G.O., Tursenev S.A. Integratsiia tekhnologii iskusstvennogo intellekta dlia povysheniia effektivnosti evakuatsii liudei pri pozhare // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty). 2023. No. 4 (48). S. 30—36. DOI: 10.61260/2307-7476-2024-2023-4-30-36. EDN: DDHLPZ.
8. Aktaeva A.U., Zhaksylyk T.D., Sarsenbaeva Zh.I. Iskusstvennyi intellekt i pozharnaia bezopasnost' // NIR. 2023. No. 1 (13). S. 133—137.
9. Shchepetov N.S., Kropotova N.A. Iskusstvennyi intellekt i pozharnaia bezopasnost': rol' i prakticheskie razrabotki // Aktual'nye voprosy sovershenstvovaniia inzhenernykh sistem obespecheniia pozharnoi bezopasnosti ob'ektov : sb. mat. XII Vseros. nauch.-prakt. konf., Ivanovo, 22 apreliia 2025 g. Ivanovo : Ivanovskaia pozharно-spasatel'naia akademiia GPS MChS Rossii, 2025. S. 462—468. EDN: VKSCJB.



# ПРАВОВЫЕ МЕХАНИЗМЫ СНИЖЕНИЯ РИСКОВ НЕКАЧЕСТВЕННОЙ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Олифиренко А.А.<sup>1</sup>

**Ключевые слова:** информационная безопасность, публичная функция, целостность информации, юридически значимое решение, происхождение данных, версионность, межведомственный обмен, компьютерный инцидент, достоверность сведений, восстановление прав.

## Аннотация

**Цель работы.** Цель работы состоит в определении правовых механизмов снижения рисков распространения некачественной информации в государственных информационных системах и устранения последствий ее использования при осуществлении публичных функций.

**Метод исследования.** Формально-юридический метод применен для толкования требований к качеству информации, ее защите и исправлению. Системно-структурный анализ использован для восстановления связи между исходной версией записи, ее преобразованиями и юридически значимыми результатами. Функциональный подход позволил соотнести оценку качества информации с назначением информационного ресурса и содержанием публичной функции.

**Результаты исследования.** Установлено, что некачественное состояние информации определяется нарушением требования, существенного для конкретной публичной функции; нарушение защищаемого состояния информации или функционирования ГИС образует самостоятельное основание для применения мер информационной безопасности. Предложен порядок реагирования, охватывающий переданные сведения, производные результаты и решения, фактически связанные со спорной версией. Компетентный субъект выбирает актуализацию, повторную оценку, временное ограничение использования либо пересмотр решения в установленной процедуре. Техническое восстановление версии записи не удостоверяет ее содержательную пригодность, поэтому возврат в обработку требует проверки по источнику и назначению ресурса. При признаках компьютерного инцидента порядок дополняется регистрацией событий, техническим расследованием и восстановлением защищенного состояния информации и ГИС. Применимость подхода подтверждена позициями Конституционного Суда Российской Федерации по исправлению ошибок публичного органа и исправлению реестровых записей.

DOI: 10.24412/1994-1404-2026-3-302-311

## Введение и постановка задачи

В государственной информационной системе (далее — ГИС) одна запись может последовательно воспроизводиться, сопоставляться с другими сведениями и преобразовываться в результаты, используемые при подготовке административных решений. Для целей настоящей статьи информационный ресурс рассматривается как организованная совокупность информации в ГИС, предназначенная для использования при осуществлении одной или нескольких публичных функций. В составе такого ресурса выделяются информационные объекты — функцио-

нально обособленные единицы информации, имеющие самостоятельное назначение и способные повлиять на юридически значимый результат. Информационным объектом может выступать реестровая запись, электронный документ, сообщение межведомственного обмена или иной результат фиксации и обработки сведений, имеющий самостоятельное значение для осуществления публичной функции. Запись в настоящем исследовании рассматривается как один из видов информационного объекта и обозначает зафиксированную в ГИС совокупность сведений, используемую как

<sup>1</sup> Олифиренко Артем Алексеевич, ведущий специалист по защите систем искусственного интеллекта, ответственный за безопасность ИИ-систем, руководитель суб-команды мониторинга информационной безопасности ООО «Экосистема недвижимости „Метр квадратный“», Москва, Россия; аспирант кафедры информационного права и цифровых технологий ФГБОУ ВО «Саратовская государственная юридическая академия», Саратов, Россия. ORCID 0000-0002-2186-281X.

E-mail: [artemolifirenko@yandex.ru](mailto:artemolifirenko@yandex.ru)

единицу хранения и обработки, а версия записи — состояние этой совокупности сведений в определенный момент времени. Разграничение имеет правовое значение, поскольку решение оценивается по той версии записи, которой орган располагал в момент совершения соответствующего действия. Исправление исходного значения изменяет дальнейшую обработку, но не устраняет последствия прежнего использования записи. Для их выявления требуется восстановить последовательность операций с конкретной версией.

Качество информации представляет собой интегральную характеристику степени ее пригодности для совершения действий и принятия решений, отвечающих целям, задачам и интересам субъекта. Для целей статьи конкретная публичная функция понимается как предусмотренное законодательством направление деятельности или полномочие публичного органа, при осуществлении которого информация используется для совершения юридически значимого действия или принятия решения. В ГИС информация признается некачественной, если несоответствие требованию, существенному для такой функции, снижает пригодность сведений для ее выполнения.

Проблема качества информации входит в предмет обеспечения информационной безопасности, если расхождение обусловлено воздействием на защищаемые свойства информации либо нарушением функционирования информационной системы. Под защищаемым состоянием далее понимается состояние информации и ГИС, при котором сохраняются свойства информации и условия функционирования системы, подлежащие защите в соответствии с требованиями информационной безопасности. Приказом ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» утверждены требования, предусматривающие предотвращение несанкционированного доступа и специальных воздействий, направленных в том числе на уничтожение и искажение информации<sup>2</sup>. Методический документ ФСТЭК России «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержденный 12 апреля 2026 г., предусматривает регистрацию и последующий анализ событий безопасности<sup>3</sup>. Содержательная ошибка, содержащаяся в исходных сведениях либо возникшая при применении некоррект-

ной методики, может сделать информацию некачественной без нарушения ее защищаемого состояния. Этим обусловлено разграничение предмета технической и содержательной проверок.

Цель исследования — определить правовые механизмы снижения рисков распространения некачественной информации в ГИС и устранения последствий ее использования при осуществлении публичных функций.

### **Научно-теоретические подходы к исследованию**

В настоящем исследовании юридическая значимость качества записи определяется той функцией, которую она выполняет в механизме правоприменения. Р.В. Амелин указывает, что «неотъемлемой частью механизма правового регулирования является система фиксации и удостоверения юридических фактов» [1, с. 445]. Тем самым официальная фиксация сведений приобретает самостоятельное правовое значение, поскольку сформированная в установленном порядке запись используется для удостоверения обстоятельств, с которыми связываются юридические последствия. С.Е. Чаннов конкретизирует эту связь применительно к публичным информационным системам (так в работе он называет ГИСы), отмечая, что «указанные реестры служат для фиксации определенных юридических фактов, как правило, непосредственно порождающих, изменяющих либо прекращающих обязанности различных субъектов. В этом и заключается их юридическое значение» [2, с. 421]. Значение информационной системы как элемента правового механизма получает дальнейшее развитие в совместной монографии Р.В. Амелина и С.Е. Чаннова, где отмечается, что «публичная информационная система де факто может выступать в качестве формы (источника) права, если закон устанавливает обязательность использования такой системы» [3, с. 10]. Из приведенных положений следует, что *правовое значение записи определяется одновременно ее официальным происхождением, установленной процедурой формирования и ролью в осуществлении публичной функции. Совокупность этих признаков создает основание юридического доверия к записи и позволяет использовать ее в соответствующей правоприменительной процедуре. Юридическая достоверность в данном контексте характеризует возможность руководствоваться официальной записью в установленной процедуре, тогда как фактическая истинность характеризует соответствие содержащихся в ней сведений реальному положению дел.* Такое разграничение позволяет далее оценивать качество информации с учетом как правового статуса записи, так и содержательной пригодности сведений для конкретной публичной функции [4].

Требования к достоверности и своевременности обращения информации закреплены на уровне общих принципов информационного законодательства и конкретизируются применительно

<sup>2</sup> Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». Зарегистрирован в Минюсте России 16 июня 2025 г. № 82619 // СПС «КонсультантПлюс». П. 1.

<sup>3</sup> Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах : методический документ. Утвержден ФСТЭК России 12 апреля 2026 г. // СПС «КонсультантПлюс».

к публичной сфере. Пункт 6 ст. 3 Федерального закона № 149-ФЗ относит к принципам правового регулирования «достоверность информации и своевременность ее предоставления»<sup>4</sup>. Тем самым достоверность закрепляется как общий нормативный стандарт обращения информации. Федеральный закон № 8-ФЗ дополняет его применительно к публичной сфере, закрепляя принцип достоверности информации о деятельности публичных органов и право пользователя получать достоверную информацию<sup>5</sup>. Эти положения связывают общий стандарт достоверности с правом адресата полагаться на официальные сведения и проверять их содержание. *Нормативное требование достоверности охватывает процедурное основание доверия к официальной записи и возможность проверки ее фактического содержания.*

*Составляющая качества информации обозначает оцениваемый аспект ее пригодности, метрика — способ измерения такой составляющей, требование — целевое ожидание к значению метрики, порог — граничное значение, отделяющее допустимое состояние информации от недопустимого.* Выбор этих элементов определяется назначением сведений. Ф. Серра, В. Перальта, А. Маротта и П. Марсель, обобщая исследования контекстного управления качеством данных, исходят из положения о том, что «DQ must be considered in the context of the task carried out by the data users» («качество данных должно рассматриваться в контексте задачи, выполняемой пользователями данных»; перевод автора) [5, р. 2]. Эта позиция придает выполняемой задаче значение критерия отбора показателей качества данных. Применительно к ГИС такой задачей выступает конкретная публичная функция, поэтому существенным является отклонение от требования, влияющего на ее выполнение.

Разграничение содержательной и технической проверки имеет самостоятельное основание в моделях качества данных. В обзоре Б.М.В. Бернардо, Х.С. Мамеде, Ж.М.П. Баррозу и В.М.П.Д. Сантоса точность характеризуется как степень, в которой значения данных «correctly represent the actual value of a given concept» («правильно представляют фактическое значение соответствующего понятия»; перевод автора), тогда как восстанавливаемость понимается как способность «recover and preserve data and quality in the event of failure, data loss, or corruption» («восстановить и сохранить данные и их качество при сбое, утрате или повреждении»; перевод автора) [6, р. 20]. Сопоставление этих определений показывает различие предметов проверки. Точность требует сопоставления содержания с фак-

тическим состоянием объекта, а восстанавливаемость характеризует способность системы вернуть информационный объект после технического нарушения. Поэтому техническое восстановление версии и проверка ее содержательной пригодности образуют самостоятельные этапы.

А.И. Костогрызов и А.А. Нистратов рассматривают качество функционирования информационной системы как системную характеристику и связывают общую цель ее функционирования с надежностью и своевременностью предоставления информации, полнотой, достоверностью и безопасностью используемой информации; для подсистемы информационной безопасности отдельно выделяется целостность защищаемой информации [7, с. 15]. Такое разграничение показывает различие трех объектов оценки: качества функционирования ГИС, качества используемой в ней информации и целостности защищаемой информации. В настоящем исследовании центральным объектом выступает качество информации, а качество функционирования ГИС и целостность информации учитываются в той мере, в какой их нарушение влияет на пригодность сведений для конкретной публичной функции.

*Правовая оценка должна связывать исходную запись и ее версии с межсистемной передачей, результатами обработки и юридически значимыми решениями.*

### **Решение поставленной задачи: правовые механизмы выявления и устранения последствий некачественной информации в ГИС**

#### **Критерии признания информации в ГИС некачественной и границы ее проверки**

*Информация в ГИС признается некачественной при несоответствии требованию, существенному для конкретной публичной функции.* Законодательное определение информационной системы как совокупности, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, предполагает ее оценку как на содержательном, так и на технологическом уровне<sup>6</sup>.

Если расхождение затрагивает защищаемые свойства информации либо нарушает функционирование ГИС, его последствия входят в предмет обеспечения информационной безопасности. Статья 16 Федерального закона № 149-ФЗ связывает защиту информации с предотвращением неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения сведений<sup>7</sup>. *Проверка устанавливает причину и стадию возникновения расхождения, возможное воздействие на систему и влияние спорной версии на выполнение публичной функции.* Оператор ГИС обеспечивает защиту инфор-

<sup>4</sup> Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31. Ч. I. Ст. 3448. П. 6 ст. 3.

<sup>5</sup> Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства Российской Федерации. 2009. № 7. Ст. 776. П. 2 ст. 4, п. 1 ст. 8.

<sup>6</sup> Федеральный закон № 149-ФЗ, ст. 2.

<sup>7</sup> Федеральный закон № 149-ФЗ, ст. 16.



мации «на всех стадиях (этапах) обработки и хранения информации», а также в течение жизненного цикла системы<sup>8</sup>.

Границы проверки определяются содержанием и назначением информации, что согласуется с подпунктами «г», «д» пункта 2(1) постановления Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации», предусматривающими определение состава размещаемых сведений, функций системы, ее архитектуры и критериев достижения целей создания<sup>9</sup>. Профиль качества информации представляет собой документированный набор применимых составляющих качества информации и их целевых значений (метрики, требований и порогов), используемый для оценки пригодности информации в конкретной публично-правовой процедуре. Он определяет применимые требования и допустимые пределы их значений; источник подтверждения, компетенция субъектов и порядок проверки устанавливаются нормативными и организационными правилами соответствующей процедуры [6; 8; 9].

Р. Миллер, С.Х.М. Чан, Х. Уилан и Ж. Грегорио, сопоставив регулирование и стандартизированные рамки качества данных, установили, что «accuracy, completeness, consistency, and timeliness are equally and well represented across all frameworks» («точность, полнота, согласованность и своевременность одинаково широко представлены во всех рассмотренных рамках»; перевод автора) [8, р. 1]. Результат сопоставления показывает устойчивость этих характеристик независимо от специфики конкретной рамки. Поэтому точность, полнота, согласованность и своевременность образуют ядро профиля качества информации, которое дополняется требованиями, обусловленными назначением конкретного ресурса.

### **Целостность версии информационного объекта как защищаемое состояние и составляющая качества информации**

Целостность версии информационного объекта в правовом контексте характеризует сохранность объема, структуры и связей конкретной версии информационного объекта, непротиворечивость и отсутствие несанкционированных искажений. Она рассматривается двояко: как защищаемое состояние конкретной версии информационного объекта и как специальная составляющая качества информации,

когда пригодность зависит от сохранения состава, структуры и связей конкретной версии. Федеральный закон № 149-ФЗ и приказ ФСТЭК России № 117 связывают защиту целостности информации с предотвращением неправомерного уничтожения и модифицирования, а также с восстановлением сведений<sup>10</sup>.

Технический контроль целостности версии информационного объекта устанавливает сохранность либо изменение защищаемого состояния версии. Оценка целостности информации как составляющей качества информации определяет, повлияло ли изменение состава, структуры или связей на пригодность информации для публичной функции; истинность, достоверность, полнота и актуальность проверяются как самостоятельные содержательные составляющие. При обнаружении воздействия восстанавливаются обстоятельства изменения и подтвержденная версия, после чего оценивается ее пригодность.

### **Распространение ошибочной версии записи по стадиям обработки и возникновение правового риска**

Правовой риск возникает, если использование спорной версии способно повлиять на осуществление публичного полномочия или правовое положение адресата, в частности повлечь необоснованное ограничение, возложение обязанности или отказ в предоставлении положенного блага. Проверка устанавливает причину и стадию расхождения, а также фактическое влияние спорной версии на результат<sup>11</sup>. Пункт 29 приказа ФСТЭК России № 117 требует устанавливать события, которые могут нарушить цели защиты, определять объекты возможного воздействия и учитывать угрозы, реализация которых может привести к негативным последствиям<sup>12</sup>.

Связь между состоянием сведений и результатом осуществления публичного полномочия учитывается в Методическом документе ФСТЭК России, в котором отмечается «критическая зависимость реализуемых полномочий (функций)» от устойчивости информационных систем и защищенности содержащейся в них информации<sup>13</sup>. При оценке события учитывается состояние системы и публичная функция, выполнение которой связано с затронутыми сведениями.

Корректность программно заданной операции подтверждает соблюдение алгоритма, а не качество использованных сведений. Проверке подлежат результаты, на формирование которых фактически повлияла спорная версия; пока они сохраняют юридическое значение, исправления исходной записи недостаточно.

<sup>8</sup> Приказ ФСТЭК России № 117, п. 9.

<sup>9</sup> Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Собрание законодательства Российской Федерации. 2015. № 28. Ст. 4241. П. 2(1), пп. «г», «д».

<sup>10</sup> Федеральный закон № 149-ФЗ, ст. 16; приказ ФСТЭК России № 117, прил., п. 2, п. 30.

<sup>11</sup> Приказ ФСТЭК России № 117; Методический документ ФСТЭК России.

<sup>12</sup> Приказ ФСТЭК России № 117, п. 29.

<sup>13</sup> Методический документ ФСТЭК России, п. 2.1.

### Проверка качества сведений до их включения в ГИС и фиксация происхождения версии

Предупредительная проверка начинается с определения назначения сведений и требований, существенных для выполнения публичной функции. Профиль качества информации закрепляет применимые составляющие и их целевые значения (метрики, требования и пороги), тогда как допустимый источник, способ подтверждения записи и компетенция субъекта определяются нормативными и организационными правилами процедуры<sup>14</sup>.

В широком правовом значении информация охватывает содержание, форму представления и порядок обращения; данные характеризуют формальную сторону материально зафиксированной информации. Для разграничения данные понимаются как записи, показатели или значения, пригодные для хранения, передачи и автоматизированной обработки. Качество данных — интегральная характеристика их пригодности для автоматизированной обработки и формирования осмысленной информации; качество информации — интегральная характеристика пригодности для действий и решений, отвечающих целям, задачам и интересам субъекта. Такое разграничение отделяет оценку формы данных от оценки юридически значимого содержания.

Требования к качеству государственных данных закреплены приказом Минцифры России от 16 июня 2025 г. № 533 «Об утверждении Порядка управления качеством государственных данных с использованием федеральной государственной информационной системы «Единая информационная платформа национальной системы управления данными»». Пункт 2 определяет полноту через «степень заполненности представляемых государственных данных на уровне записей и полей», достоверность — через соответствие «формату и ограничениям», точность — посредством сопоставления со значениями регистров, справочников и классификаторов, а консистентность — как «непротиворечивость и связанность государственных данных»<sup>15</sup>. Пункт 3 связывает оценку этих характеристик с контролем данных на витринах и при передаче через систему межведомственного электронного взаимодействия, относя выявленные отклонения к инцидентам качества государственных данных<sup>16</sup>.

<sup>14</sup> Приказ Минцифры России от 16 июня 2025 г. № 533 «Об утверждении Порядка управления качеством государственных данных с использованием федеральной государственной информационной системы «Единая информационная платформа национальной системы управления данными»». Зарегистрирован в Минюсте России 3 декабря 2025 г. № 84423 // СПС «КонсультантПлюс»; Федеральный закон № 149-ФЗ; Федеральный закон № 152-ФЗ; Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» // Собрание законодательства Российской Федерации. 2007. № 49. Ст. 6043; Федеральный закон № 8-ФЗ.

<sup>15</sup> Приказ Минцифры России № 533, п. 2.

<sup>16</sup> Приказ Минцифры России № 533, п. 3.

Используемая в приказе «достоверность» означает соответствие формату и ограничениям и относится к формальной проверке государственных данных; она не тождественна истинности или содержательной достоверности информации, подтверждаемой надежными и верифицируемыми источниками. Фактическое основание, происхождение и порядок формирования записи устанавливаются отдельно.

Метаданные — это сведения, описывающие данные и операции с ними. В. Кумар, Чандраппа и Н.С. Харинараяна по результатам обзора 55 исследований установили, что «completeness, accuracy, consistency, accessibility, conformance, provenance, and timeliness are commonly used dimensions in metadata quality assessment» («при оценке качества метаданных обычно используются полнота, точность, согласованность, доступность, соответствие требованиям, происхождение и своевременность»; перевод автора) [10, p. 661]. Включение происхождения в этот ряд придает происхождению статус самостоятельной характеристики метаданных и позволяет связывать конкретную версию записи с последующими объектами обработки. По метаданным определяется момент появления расхождения и устанавливаются объекты, в которых использовалась спорная версия.

Необходимость сохранять эту связь во времени получает дополнительное обоснование в работе Л. Эрлингер и В. Вёсса. Рассматривая задачи автоматизированного мониторинга качества данных, авторы указывают: «The continuous measurement, storage, and usage of the collected metadata should be possible» («для результатов профилирования данных и измерений качества данных должна быть предусмотрена возможность непрерывного измерения, хранения и использования собранных метаданных»; перевод автора) [9, p. 11]. Непрерывное измерение и хранение метаданных создают временную связь между состояниями записи и позволяют восстановить путь спорной версии. Результат контроля связывается с конкретной версией и сохраняется вместе со сведениями о проведенной проверке, фиксирующими момент появления расхождения и пределы его дальнейшего распространения.

### Временное ограничение использования спорной версии записи до завершения проверки

Спорная версия сохраняется в истории изменений для установления обстоятельств ее появления и последующего использования. Одновременно она исключается из операций, при которых может возникнуть правовой риск.

Если запись влияет на возникновение права, назначение выплаты, установление статуса или возложение обязанности, соответствующая операция приостанавливается до завершения проверки либо проводится на основе подтвержденного источника. Порядок ограничения использования спорной записи должен закрепляться во внутренних регламентах с разграничением компетенции подразделений.

Мера РСБ.2 Методического документа ФСТЭК России предусматривает «своевременное выявление признаков компьютерных атак и инцидентов безопасности», а при их обнаружении требует проведения мероприятий по реагированию<sup>17</sup>. При углубленной проверке сведения из разных журналов сопоставляются с результатами анализа уязвимостей и обнаружения вторжений, после чего устанавливается связь расхождения с действиями пользователя либо изменениями в работе системы<sup>18</sup>. Для ГИС на платформе «ГосТех» дополнительная организационная основа предусмотрена п. 22 Положения о платформе, по нему оператор «обеспечивает централизованную реализацию мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак, а также реагированию на компьютерные инциденты»<sup>19</sup>. *Эти положения применимы, когда некачественное состояние информации связано с компьютерной атакой, техническим воздействием или нарушением функционирования компонентов платформы.*

### **Установление пригодности версии записи и восстановление информационного объекта**

Техническая проверка устанавливает способ воздействия и восстанавливает последовательность операций, после чего сведения сопоставляются с источником и документами, положенными в основу записи<sup>20</sup>. Возможность подтверждения зависит от сохранности сведений о событиях безопасности. Мера РСБ.1 предусматривает «определение событий безопасности и данных о них, подлежащих регистрации», мера РСБ.3 требует обеспечить «формирование надежных меток времени и (или) синхронизацию системного времени», а мера РСБ.4 направлена на «обеспечение хранения и защиты данных о событиях безопасности от несанкционированного доступа»<sup>21</sup>. По совокупности этих сведений устанавливаются момент изменения, использованная учетная запись и последовательность межсистемной передачи конкретной версии.

Для восстановления цепочки зависимости используется происхождение данных. Под происхождением данных в настоящей статье понимаются сведения

об источнике конкретной версии и последовательности ее преобразований. Б. Главич указывает, что «The provenance of a data item provides a record of how the data item was derived from other data items by a set of transformations» («происхождение элемента данных содержит запись о том, каким образом этот элемент был получен из других элементов данных посредством совокупности преобразований»; перевод автора) [11, р. 211]. Это определение задает критерий фактической зависимости, при котором производный объект включается в область проверки при подтвержденной цепочке преобразований от спорной версии. В той же работе показано, что при диагностике ошибки происхождения данных позволяет выделить входные данные и преобразования, фактически участвовавшие в формировании результата [11, р. 214—215]. *По истории операций устанавливаются момент появления расхождения, последующее использование спорной версии, а также документы, расчеты и решения, в которых она получила отражение.*

Восстановление предыдущей версии решает техническую часть задачи. Такая версия могла быть ошибочной, утратить актуальность или быть сформирована по неверной методике. *Поэтому перед возвратом в обработку версия повторно оценивается по первичным источникам, назначению ресурса и применимому профилю качества информации.*

Предлагаемая последовательность соответствует пункту 22 приказа Минцифры России № 533, согласно которому при выявлении несоответствия требованиям к качеству государственных данных или фактическим данным обладатель вносит изменения «в государственные данные, содержащиеся в источнике государственных данных»<sup>22</sup>. Автоматический инцидент закрывается после «успешного выполнения механизма контроля качества государственных данных»<sup>23</sup>. *Возвращение записи в обработку требует подтверждения ее пригодности, а не только технического восстановления прежнего значения.*

### **Исправление сведений в зависимых ресурсах и прекращение использования ошибочной версии при межсистемном обмене**

После исправления сведений и подтверждения их пригодности запись возвращается в обработку, однако прежняя версия могла сохраниться у получателей либо повлиять на производные объекты. Область исправления устанавливается по истории использования версии, времени операций и направлениям передачи. Для этого сведения технической документации о программных интерфейсах, алгоритмах, электронных моделях процессов, архитектуре и базе данных систем<sup>24</sup> сопоставляются с журналами операций. Область

<sup>17</sup> Методический документ ФСТЭК России, мера РСБ.2.

<sup>18</sup> Методический документ ФСТЭК России, усиление меры РСБ.2.

<sup>19</sup> Постановление Правительства Российской Федерации от 16 декабря 2022 г. № 2338 «Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех», о внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 и признании утратившим силу пункта 6 изменений, которые вносятся в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Собрание законодательства Российской Федерации. 2022. № 52. Ст. 9610. П. 22.

<sup>20</sup> Приказ ФСТЭК России № 117; Методический документ ФСТЭК России.

<sup>21</sup> Методический документ ФСТЭК России, меры РСБ.1, РСБ.3, РСБ.4.

<sup>22</sup> Приказ Минцифры России № 533, п. 22.

<sup>23</sup> Приказ Минцифры России № 533, п. 23.

<sup>24</sup> Постановление Правительства РФ № 676, п. 5(1).



исправления образуют зависимые объекты, на содержание которых повлияла ошибочная версия.

Когда распространение спорной версии связано с неправомерным действием или реализацией угрозы, выявление затронутых ресурсов и восстановление информации входят в процессы защиты, предусмотренные статьей 16 Федерального закона № 149-ФЗ и пунктом 30 приказа ФСТЭК России № 117<sup>25</sup>. Исправление сведений в исходной записи и актуализация зависимых результатов относятся к управлению качеством информации. Получателю передается подтвержденная версия вместе со сведениями о периоде использования прежнего значения, после чего принимающая сторона актуализирует зависимый объект либо временно исключает его из обработки до завершения собственной проверки. До подтверждения исправления прежняя версия исключается получателем из новых операций. Завершение межсистемного обновления подтверждается получателем после прекращения использования прежней версии.

Обновлению зависимых ресурсов предшествует установление причины расхождения и исключение условий его повторного появления. Пункт 66 приказа ФСТЭК России № 117 связывает контроль уровня защищенности с «оценкой возможностей нарушения безопасности информации и (или) нарушения функционирования информационных систем внешними и внутренними нарушителями»<sup>26</sup>. Если расхождение вызвано компьютерным инцидентом, контроль проводится вне установленного периодического графика: пункт 67 предусматривает его осуществление «не реже одного раза в три года или после компьютерного инцидента»<sup>27</sup>. Реагирование завершается после устранения причины изменения, обновления зависимых сведений и подтверждения того, что спорная версия больше не воспроизводится в информационных системах.

### Проверка юридически значимых решений после исправления записи и восстановление правового положения адресата

С.Е. Чаннов связывает функционирование публичной информационной системы непосредственно с осуществлением публичного управления, указывая, что «реальное осуществление действий в сфере публичного управления оказывается в зависимости [...] от функционала используемой публичной информационной системы» [2, с. 420]. Эта зависимость означает, что свойства и сбои информационной системы способны влиять на результат реализации публичного полномочия. Также, по мнению С.Е. Чаннова, «любые сбои и ошибки в публичной информационной системе становятся фактами, имеющими юридическое значение» [2, с. 419].

*Для целей настоящего исследования это означает необходимость проверки уже возникших юридических последствий после исправления записи. Исправление записи не устраняет автоматически правовые последствия ее прежнего использования. В связи с этим необходимо установить, при принятии каких решений использовалась прежняя версия записи и какое влияние она оказала на правовое положение адресата.*

Если причиной некачественного состояния стало нарушение целостности информации либо функционирования ГИС и информация была использована при принятии юридически значимого решения, устранение технических последствий предшествует проверке правовых последствий использования спорной версии. Требования ФСТЭК России связывают защиту информации с предупреждением негативных последствий нарушения ее защищаемых свойств и реализации угроз безопасности<sup>28</sup>. В предлагаемом механизме восстановление подтвержденного состояния информации сопровождается проверкой решения, проводимой принявшим его органом в пределах своей компетенции и с соблюдением установленной законом процедуры.

Принципиальное значение имеет ситуация, при которой ошибка допущена самим публичным органом и длительное время определяла правовое положение гражданина. В Постановлении Конституционного Суда Российской Федерации от 14 января 2016 г. № 1-П Суд указал, что исправление ошибки, допущенной пенсионным органом, относится к праву и обязанности государства, однако механизм ее исправления должен обеспечивать баланс публичных и частных интересов, учитывать отсутствие нарушений со стороны гражданина и исключать его чрезмерное обременение. При распределении неблагоприятных последствий должны учитываться особенности жизненной ситуации, продолжительность периода, в течение которого гражданин полагался на официально признанный государством статус, и другие значимые обстоятельства<sup>29</sup>. Для целей настоящего исследования эта позиция означает, что исправление ошибочной официальной записи или результата ее обработки требует оценки последствий, возникших у добросовестного адресата вследствие доверия к действиям государственного органа.

Иная ситуация возникает, когда ошибочная запись в ЕГРН уже стала основанием возникновения и государственной регистрации права. В Постановлении Конституционного Суда Российской Федерации от 28 января 2025 г. № 3-П указано, что требование

<sup>28</sup> Приказ ФСТЭК России № 117, п. 10.

<sup>29</sup> Постановление Конституционного Суда Российской Федерации от 14 января 2016 г. № 1-П «По делу о проверке конституционности части первой статьи 13 Закона Российской Федерации “О пенсионном обеспечении лиц, проходивших военную службу, службу в органах внутренних дел, Государственной противопожарной службе, органах по контролю за оборотом наркотических средств и психотропных веществ, учреждениях и органах уголовно-исполнительной системы, и их семей” в связи с жалобой гражданина С.В. Иванова» // Собрание законодательства Российской Федерации. 2016. № 4. Ст. 551. П. 5 мотивировочной части.

<sup>25</sup> Федеральный закон № 149-ФЗ, ст. 16; приказ ФСТЭК России № 117, п. 30.

<sup>26</sup> Приказ ФСТЭК России № 117, п. 66.

<sup>27</sup> Приказ ФСТЭК России № 117, п. 67.



о признании зарегистрированного права отсутствующим направлено на обеспечение «достоверности, непротиворечивости содержащихся в ЕГРН публичных сведений о существовании, принадлежности и правовом режиме объектов недвижимости». Вместе с тем ошибки, вызванные несогласованностью действий государственных органов при ведении реестров, «не могут быть поставлены в вину» гражданам, которые рассчитывали на законность действий публичной власти<sup>30</sup>. *Исправление реестровой записи должно учитывать судьбу возникшего на ее основе права и необходимость защиты добросовестного доверия лица к действиям государства.*

Рассмотренные позиции показывают, что проверке подлежит юридически значимый результат, на формирование которого фактически повлияла некачественная информация. Пределы проверки определяются характером изменений правового положения адресата и полномочиями органа, принявшего соответствующий акт. *Негативные последствия организационных и межведомственных ошибок не должны автоматически возлагаться на добросовестное лицо, доверившееся официальной информации.* Вопрос о пересмотре акта, восстановлении права и компенсации разрешается в порядке, установленном для соответствующего вида правоотношений [2, с. 419—428; 11]<sup>31</sup>.

### **Выводы о правовых механизмах снижения рисков некачественной информации в ГИС**

Результаты подтверждают функциональную природу качества информации: применимые требования определяются назначением ресурса, публичной функцией и возможными правовыми последствиями.

*Некачественной информацией в ГИС следует признавать сведения, несоответствие которых существенному для конкретной публичной функции требованию снижает их пригодность и создает риск искажения юридически значимого результата.* Расхождение может возникнуть в исходных сведениях, при фиксации, преобразовании либо воздействии на информационный объект. Причина и стадия определяют предмет проверки и распределение обязанностей по восстановлению версии и оценке связанных результатов.

*Исправление исходной записи открывает проверку связанных результатов, которая в зависимости от их характера выражается в актуализации сведений, повторной оценке, ограничении использования либо пересмотре публично-властного решения в установленном порядке.*

Выбор последствия учитывает правовое положение адресата, фактическую зависимость решения от ошибочной версии и защиту добросовестного доверия к официальной информации. *Организационные и межведомственные риски распределяются между публичными субъектами с учетом их компетенции и контроля над соответствующим участком информационного процесса и не должны перекладываться на добросовестного адресата.*

При признаках угрозы или нарушения функционирования ГИС процедура дополняется регистрацией события безопасности, техническим расследованием и восстановлением защищенного состояния информации и ГИС. Содержательная оценка устанавливает пригодность сведений и последствия их использования. *Разграничение этих направлений связывает управление качеством информации с информационной безопасностью, не смешивая их предмет.*

*Исследование выполнено за счет гранта Российского научного фонда № 26-18-00420, <https://rscf.ru/project/26-18-00420/>, финансирование осуществляется через организацию ФГБОУ ВО «Саратовская государственная юридическая академия».*

<sup>30</sup> Постановление Конституционного Суда Российской Федерации от 28 января 2025 г. № 3-П «По делу о проверке конституционности статей 12, 209 и 304 Гражданского кодекса Российской Федерации и части 5 статьи 1 Федерального закона “О государственной регистрации недвижимости” в связи с жалобами граждан Н.И. Гришиной, Н.З. Гулордавы и других» // Собрание законодательства Российской Федерации. 2025. № 6. Ст. 538.

<sup>31</sup> Постановления КС РФ № 1-П и № 3-П.

## Литература

1. Амелин Р.В. Информационные системы как правовой инструмент воздействия на общественные отношения: анализ российской и мировой практики // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2021. Т. 21, вып. 4. С. 445—452. DOI: 10.18500/1994-2540-2021-21-4-445-452.
2. Чаннов С.Е. Использование цифровых технологий в сфере публичного управления // Известия Саратовского университета. Новая серия. Серия «Экономика. Управление. Право». 2021. Т. 21. Вып. 4. С. 419—428. DOI: 10.18500/1994-2540-2021-21-4-419-428.
3. Амелин Р.В., Чаннов С.Е. Тенденции и перспективы использования государственных информационных систем в государственном управлении: правовые аспекты : монография. М. : ИНФРА-М, 2023. 171 с. ISBN 978-5-16-112170-2.
4. Амелин Р.В., Чаннов С.Е. Эволюция правовых методов под воздействием цифровых технологий // Вестник Поволжского института управления. 2021. Т. 21. № 5. С. 4—12.
5. Serra F., Peralta V., Marotta A., Marcel P. Use of Context in Data Quality Management: A Systematic Literature Review // Journal of Data and Information Quality. 2024. Vol. 16. No. 3. Art. 19. P. 1—41. DOI: 10.1145/3672082.
6. Bernardo B.M.V., São Mamede H., Barroso J.M.P., Santos V.M.P.D. Data Governance & Quality Management: Innovation and Breakthroughs Across Different Fields // Journal of Innovation & Knowledge. 2024. Vol. 9. No. 4. Art. 100598. DOI: 10.1016/j.jik.2024.100598.
7. Костокрызов А.И., Нистратов А.А. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 1. Общий подход // Правовая информатика. 2024. № 3. С. 13—31. DOI: 10.24682/1994-1404-2024-3-13-31.
8. Miller R., Chan S.H.M., Whelan H., Gregório J. A Comparison of Data Quality Frameworks: A Review // Big Data and Cognitive Computing. 2025. Vol. 9. No. 4. Art. 93. DOI: 10.3390/bdcc9040093.
9. Ehrlinger L., Wöß W. A Survey of Data Quality Measurement and Monitoring Tools // Frontiers in Big Data. 2022. Vol. 5. Art. 850611. DOI: 10.3389/fdata.2022.850611.
10. Kumar V., Chandrappa, Harinarayana N.S. Exploring Dimensions of Metadata Quality Assessment: A Scoping Review // Journal of Librarianship and Information Science. 2025. Vol. 57. No. 3. P. 661—673. DOI: 10.1177/09610006241239080.
11. Glavic B. Data Provenance: Origins, Applications, Algorithms, and Models // Foundations and Trends in Databases. 2021. Vol. 9. No. 3—4. P. 209—441. DOI: 10.1561/19000000068.

## SECTION:

## REGULATORY INFORMATICS

## LEGAL MECHANISMS FOR REDUCING RISKS OF LOW-QUALITY INFORMATION IN GOVERNMENT INFORMATION SYSTEMS

Olifirenko A.A.<sup>32</sup>

**Keywords:** information security, public function, information integrity, legally significant decision, data provenance, version management, inter-agency exchange, computer incident, data accuracy, restoration of rights.

### Abstract

**Purpose of work.** The purpose of the study is to determine legal mechanisms for reducing the risks associated with the dissemination of low-quality information in government information systems and for addressing the consequences of its use in the exercise of public functions.

**Research method.** The formal legal method is used to interpret requirements governing information quality, protection, and correction. System-structural analysis is applied to reconstruct dependencies between an original record, subsequent

<sup>32</sup> **Artem A. Olifirenko**, Lead Specialist in Artificial Intelligence Systems Security, responsible for AI systems security, Head of the Information Security Monitoring Sub-Team, LLC "Real Estate Ecosystem 'Metr Kvadratny'", Moscow, Russia; Ph.D. student, Department of Information Law and Digital Technologies, Saratov State Law Academy, Saratov, Russia. ORCID: 0000-0002-2186-281X.

E-mail: [artemolifirenko@yandex.ru](mailto:artemolifirenko@yandex.ru)

transformations, and legally significant outputs. A functional approach relates quality assessment to the intended use of an information resource and the public function performed with its support.

**Results of the study.** The study shows that low-quality information is identified by breach of a requirement material to a particular public function, while interference with the protected state of information independently triggers information-security measures. The proposed response procedure covers transmitted data, derived outputs, and public-authority decisions actually linked to the disputed record version. The competent authority selects the applicable measure according to the dependency and governing procedure: updating the data, reassessing the output, temporarily restricting its use, or reviewing the decision. Restoring a technically verified record version does not establish its substantive fitness; return to processing therefore requires review against the source and intended use. Where a computer incident is suspected, the procedure is supplemented by security-event logging, technical investigation, and restoration of the protected state of information and the GIS. The approach is supported by Constitutional Court cases concerning correction of errors by public authorities and registry corrections.

## References

1. Amelin R.V. Informatsionnye sistemy kak pravovoi instrument vozdeistviia na obshchestvennye otnosheniia: analiz rossiiskoi i mirovoi praktiki // Izvestiia Saratovskogo universiteta. Novaia seriia. Seriia: Ekonomika. Upravlenie. Pravo. 2021. T. 21, vyp. 4. S. 445—452. DOI: 10.18500/1994-2540-2021-21-4-445-452.
2. Channov S.E. Ispol'zovanie tsifrovyykh tekhnologii v sfere publichnogo upravleniia // Izvestiia Saratovskogo universiteta. Novaia seriia. Seriia "Ekonomika. Upravlenie. Pravo". 2021. T. 21. Vyp. 4. S. 419—428. DOI: 10.18500/1994-2540-2021-21-4-419-428.
3. Amelin R.V., Channov S.E. Tendentsii i perspektivy ispol'zovaniia gosudarstvennykh informatsionnykh sistem v gosudarstvennom upravlenii: pravovye aspekty : monografiia. M. : INFRA-M, 2023. 171 s. ISBN 978-5-16-112170-2.
4. Amelin R.V., Channov S.E. Evoliutsiia pravovykh metodov pod vozdeistviem tsifrovyykh tekhnologii // Vestnik Povolzhskogo instituta upravleniia. 2021. T. 21. No. 5. S. 4—12.
5. Serra F., Peralta V., Marotta A., Marcel P. Use of Context in Data Quality Management: A Systematic Literature Review // Journal of Data and Information Quality. 2024. Vol. 16. No. 3. Art. 19. P. 1—41. DOI: 10.1145/3672082.
6. Bernardo B.M.V., São Mamede H., Barroso J.M.P., Santos V.M.P.D. Data Governance & Quality Management: Innovation and Breakthroughs Across Different Fields // Journal of Innovation & Knowledge. 2024. Vol. 9. No. 4. Art. 100598. DOI: 10.1016/j.jik.2024.100598.
7. Kostogryzov A.I., Nistratov A.A. Metodicheskie polozheniia po veroiatnostnomu prognozirovaniiu kachestva funktsionirovaniia informatsionnykh sistem. Chast' 1. Obshchii podkhod // Pravovaia informatika. 2024. No. 3. S. 13—31. DOI: 10.24682/1994-1404-2024-3-13-31.
8. Miller R., Chan S.H.M., Whelan H., Gregório J. A Comparison of Data Quality Frameworks: A Review // Big Data and Cognitive Computing. 2025. Vol. 9. No. 4. Art. 93. DOI: 10.3390/bdcc9040093.
9. Ehrlinger L., Wöß W. A Survey of Data Quality Measurement and Monitoring Tools // Frontiers in Big Data. 2022. Vol. 5. Art. 850611. DOI: 10.3389/fdata.2022.850611.
10. Kumar V., Chandrappa, Harinarayana N.S. Exploring Dimensions of Metadata Quality Assessment: A Scoping Review // Journal of Librarianship and Information Science. 2025. Vol. 57. No. 3. P. 661—673. DOI: 10.1177/09610006241239080.
11. Glavic B. Data Provenance: Origins, Applications, Algorithms, and Models // Foundations and Trends in Databases. 2021. Vol. 9. No. 3—4. P. 209—441. DOI: 10.1561/19000000068.



# ИНТЕЛЛЕКТУАЛЬНЫЙ ПОМОЩНИК ДЛЯ ОБУЧЕНИЯ НАСЕЛЕНИЯ АЛГОРИТМАМ ОКАЗАНИЯ ПЕРВОЙ ПОМОЩИ

Васильев Р.В.<sup>1</sup>

**Ключевые слова:** искусственный интеллект, сценарный тренажер, обратная связь, адаптация учебного маршрута, цифровая поддержка, персонализация, доступность, модуль, интерфейс.

## Аннотация

**Цель работы:** обосновать структуру интеллектуального помощника для обучения населения первой помощи и определить критерии оценивания такого учебного средства.

**Метод исследования:** проанализированы научные труды, посвященные использованию искусственного интеллекта и цифровых технологий в процессе подготовки населения.

**Результаты исследования:** предложена архитектура интеллектуального помощника, которая включает в себя базу знаний, учебные сценарии, диалоговый интерфейс, модель освоения материала каждым пользователем и средства контроля знаний. В основу данной архитектуры положено разграничение содержания и способа его подачи. При этом требования безопасности остаются неизменными, тогда как объяснения и форма представления материала могут адаптироваться к уровню подготовки обучающегося. Предложен подход к оценке знаний, при котором критические ошибки фиксируются отдельно. Правильные ответы на второстепенные вопросы не компенсируют ошибок, влияющих на безопасность действий. Определены показатели для оценки технического качества помощника, усвоения последовательности оказания первой помощи и переноса полученных знаний в практическую деятельность.

**Практическая значимость:** предложенная концепция может служить основой для подготовки технического задания на цифровое учебное средство и разработки сценарных тренажеров. Помощник также может быть использован для самостоятельного повторения материала между очными занятиями. Основное назначение помощника — дополнять практическое обучение под руководством инструктора, а не заменять его.

DOI: 10.24412/1994-1404-2026-3-312-319

## Введение

Подготовка населения по вопросам оказания первой помощи направлена не только на освоение отдельных приемов, но и формирование умения выбирать последовательность действий в условиях дефицита времени, недостаточной информации и высокого эмоционального напряжения [1, 2]. Это говорит о том, что знание приемов само по себе не гарантирует готовности к их применению в конкретной ситуации. Даже при успешном воспроизведении учебного материала обучающийся может испытывать затруднения при оценке обстановки и определении первоочередных действий. Поэтому образовательный результат необходимо рассматривать не только как объем усвоенной информации, но и как способность распознать значимые признаки ситуации, определить приоритеты и избежать опасных действий [3].

Очные занятия позволяют отрабатывать практические приемы и получать обратную связь от ин-

структора. Вместе с тем возможности регулярного повторения ограничиваются расписанием, доступностью оборудования и организационными ресурсами. Между занятиями человек нередко обращается к открытым интернет-источникам, содержание которых различается по полноте, достоверности и соответствию уровню подготовки читателя. Возникает потребность в доступном инструменте самостоятельной работы, который не только предоставляет сведения, но и помогает обнаруживать ошибки в понимании материала [4].

Технологии искусственного интеллекта позволяют организовать взаимодействие на естественном языке, уточнять смысл ответа и подбирать дополнительные задания. Однако применительно к первой помощи удобство общения не может служить достаточным основанием для использования системы. Связное объяснение способно содержать пропуск обязательного действия,

<sup>1</sup> **Васильев Роман Викторович**, старший преподаватель кафедры безопасности в ЧС Уральского института ГПС МЧС России, г. Екатеринбург, Российская Федерация.  
E-mail: [roman\\_vasilev\\_1972@mail.ru](mailto:roman_vasilev_1972@mail.ru)



неверное условие его выполнения или неподтвержденное утверждение.

В связи с этим, проблема настоящего исследования заключается в определении условий, при которых интеллектуальный помощник способен поддерживать индивидуальную подготовку, не подменяя проверенные правила свободно сформированными рекомендациями.

### Основная часть

Функциональное назначение помощника не следует сводить к ответам на вопросы. Обычный справочник также предоставляет информацию, но, как правило, не устанавливает, почему пользователь ошибается и какое упражнение ему необходимо выполнить следующим.

По мнению Н.П. Ивановой, проектирование интеллектуального ассистента предполагает определение границ предметной области и структурирование составляющих ее ситуаций, а их отбор требует педагогической экспертизы [5]. В контексте нашего исследования данный подход служит методологическим основанием для представления учебных ситуаций по оказанию первой помощи в виде формализованных сценариев с заданными условиями и последовательностью действий. Его применение также обосновывает необходимость экспертной проверки содержания сценариев и организации диалога, объясняющего обучающемуся основания принимаемых решений.

И.А. Аксененко, С.А. Бронов, В.В. Калитина, Е.А. Степанова обосновывают целесообразность применения интеллектуальных помощников для индивидуализации образовательного взаимодействия. Исследователи подчеркивают, что отдельный ответ не всегда устраи-

ет затруднения обучающегося, а для выявления причин непонимания и уточнения запроса может потребоваться диалог [6]. Данное положение может лечь в основу разработки диалогового помощника, адаптирующего учебное взаимодействие к ошибкам, возникающим при освоении алгоритмов оказания первой помощи. Такая адаптация предполагает использование уточняющих вопросов, объяснение причин выбора конкретных действий и повторное включение ситуационных заданий, вызвавших затруднения. При этом индивидуализация должна касаться способов объяснения материала и последовательности заданий, сохраняя неизменным содержание установленных алгоритмов. Диалоговый помощник следует рассматривать как дополнение к практической подготовке, а не как замену отработке навыков под руководством инструктора.

Индивидуализация подготовки предполагает различение затруднений, обусловленных незнанием необходимого действия, неверным пониманием условий его выполнения, нарушением последовательности или устойчивым воспроизведением ошибочного правила. При этом одинаковые ответы обучающихся могут быть связаны с разными причинами ошибок.

Так, пропуск оценки безопасности места происшествия может объясняться как непониманием ее значения, так и привычкой сразу переходить к помощи пострадавшему. В первом случае целесообразно разъяснить необходимость предварительной оценки безопасности, во втором — предложить ситуационные задания, требующие осознанного выбора безопасного поведения до начала оказания помощи. Таким образом, обратная связь должна учитывать выявленную причину затруднения, а не сводиться к указанию на неверный ответ.

Таблица 1

**Требования к интеллектуальному помощнику**

| НАПРАВЛЕНИЕ              | ПРОЕКТНОЕ РЕШЕНИЕ                                                                | КРИТЕРИЙ ПРОВЕРКИ                                                            |
|--------------------------|----------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Достоверность содержания | Использование экспертно- проверенных материалов с указанием источника и версии   | Прослеживаемость каждого значимого правила до основания                      |
| Контекстность оценки     | Проверка действия с учетом состояния сценария                                    | Отсутствие оценки действия вне условий его применимости                      |
| Персонализация           | Выбор заданий по выявленным затруднениям                                         | Связь следующего задания с конкретной учебной потребностью                   |
| Обратная связь           | Объяснение ошибки и предоставление возможности повторного решения                | Понимание пользователем причины коррекции                                    |
| Безопасность             | Разделение генерации текста и проверки допустимости действий                     | Блокирование непроверенных инструкций                                        |
| Доступность              | Краткие формулировки, управление сложностью текста, альтернативные способы ввода | Возможность выполнения заданий пользователями с разной цифровой грамотностью |
| Сопровождение            | Версионирование материалов и повторное тестирование после обновления             | Воспроизводимость оценки для конкретной версии системы                       |

Функциональная структура системы

| КОМПОНЕНТ               | ОСНОВНЫЕ ДАННЫЕ                                                          | ФУНКЦИИ                                                        |
|-------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------|
| Проверенная база знаний | Учебные материалы, правила, условия применимости, сведения об источниках | Хранение содержания и управление версиями                      |
| Сценарный модуль        | Начальные условия, наблюдаемые признаки, действия, переходы              | Развитие учебной ситуации и проверка последовательности        |
| Модель обучающегося     | Ответы, ошибки, обращения к подсказкам, повторные попытки                | Описание текущих затруднений и самостоятельности               |
| Модуль адаптации        | Учебные цели и сведения об освоении                                      | Подбор сложности, повторения и объема поддержки                |
| Диалоговый интерфейс    | Ответ пользователя и релевантные фрагменты базы знаний                   | Уточнение смысла, формулирование вопросов и объяснений         |
| Контроль безопасности   | Ограничения, критические ошибки, правила отказа от оценки                | Проверка выходных сообщений и остановка недостоверного диалога |
| Аналитический модуль    | Журнал событий учебной сессии                                            | Подготовка отчета для пользователя и преподавателя             |

Реализация такого подхода требует определения состава интеллектуального помощника и функций его компонентов. Выделение модулей представления учебного материала, моделирования ситуаций, оценки действий обучающегося и формирования обратной связи позволяет описать порядок их взаимодействия и установить требования к результатам работы каждого из них. Основные требования к интеллектуальному помощнику и критерии проверки их реализации представлены в таблице 1.

Предлагаемые требования означают, что качество помощника нельзя свести к естественности речи. Убедительно сформулированное, но предметно ошибочное объяснение представляет больший риск, чем стилистически простой ответ, основанный на проверенном правиле.

В основу структуры интеллектуального помощника положено разделение предметного, педагогического и языкового компонентов (табл. 2). Предметный компонент определяет допустимость действия. Педагогический выбирает способ дальнейшей работы с обучающимся. Языковой обеспечивает понятную форму взаимодействия, не изменяя содержание обязательных требований.

Адаптация учебного маршрута осуществляется на основании типа ошибки, повторяемости затруднения и объема использованной поддержки. Выбор учебного задания зависит от того, в чем именно затрудняется обучающийся. Если ему не хватает знаний, помощник кратко поясняет правило, а затем предлагает определить, в какой ситуации оно применяется. Если ошибка связана с порядком действий, упражнение должно помочь разобраться, почему один этап предшествует другому. Устойчивое повторение одной и той же ошибки требует более подробного разбора: обучающемуся предлагают сравнить ситуации, в которых внешне

сходные условия предполагают разные действия. При этом правильный ответ, полученный с подсказкой, еще не свидетельствует о самостоятельном освоении материала. Чтобы проверить понимание, соответствующее действие необходимо повторно оценить в другом сценарии и уже без помощи. Работа над выявленными затруднениями не отменяет возвращения к ранее изученным темам.

Роль языковой модели в такой системе следует разделить от функции оценки. Модель может помогать разбирать ответы, сформулированные в свободной форме, подбирать доступное объяснение и кратко комментировать допущенную ошибку. Однако решение о правильности действия должно определяться формализованными правилами сценария, а не только выводом модели.

Особого внимания требуют неоднозначные ответы. Прежде чем оценивать такую формулировку, помощник должен уточнить, какое действие имел в виду обучающийся. Иначе возникает риск, что система сама выберет наиболее вероятное толкование и оценит собственную интерпретацию вместо исходного ответа. Если уточнение не позволяет надежно определить смысл, пользователю следует предложить выбрать действие из заданных вариантов.

Для подготовки объяснений можно предварительно извлекать относящиеся к задаче сведения из проверенной базы знаний. Это дает модели опору на отобранные материалы, но не исключает ошибок: найденный фрагмент может не подходить к конкретной ситуации, а его связь с условиями задачи может быть истолкована неверно. Поэтому проверять необходимо не только достоверность используемых сведений, но и применимость сформированного ответа к текущему этапу сценария.

Д.Е. Пальчунов, А.А. Якобсон предлагают прецедентный подход, при котором для решения новых задач используются знания, полученные в предыдущих диалогах. Прецеденты представлены в виде частичных моделей; их сходство и возможные преобразования описываются с помощью онтологических гомоморфизмов. Особое внимание авторы уделяют аргументации в диалоге. Задача системы не ограничивается выдачей решения: ей необходимо уточнить потребности пользователя, рассмотреть его доводы и объяснить, на чем основан ответ [7].

И.В. Смирнов и соавторы рассматривают интеллектуального ассистента как средство ответа на типовые вопросы по учебному курсу и подготовки подсказок преподавателю с учетом реакции аудитории [8]. Для нашего исследования эти положения важны при определении функций помощника по обучению первой помощи. Прецедентный подход может быть полезен для организации работы с учебными диалогами, а предложенные функции ассистента — для информационной поддержки обучающихся. При этом адаптация подсказок к индивидуальному уровню подготовки требует отдельной проработки.

При разработке сценарной модели важно предусмотреть, что одна и та же задача может допускать несколько правильных вариантов решения. Обучающийся не обязан дословно воспроизводить заданный ответ или во всех случаях следовать единственной последовательности действий. Генеративный компонент в такой системе нужен прежде всего для интерпретации ответов, выраженных в свободной форме. Решение о том, допустимо ли предложенное действие, должно приниматься на основе правил, заранее определенных экспертами для соответствующего этапа сценария.

Если сценарий построен как жесткая линейная цепочка, любое отступление от авторского решения может ошибочно оцениваться как нарушение. Поэтому при экспертной разметке необходимо обозначить, какие действия и переходы обязательны, где возможны альтернативы, а какие ответы не соответствуют текущей задаче. Это позволяет отделить содержательную ошибку от различий в формулировках или допустимом порядке выполнения действий.

Рассмотрим учебный сценарий оказания помощи пострадавшему, который не реагирует на обращение. В нем могут отрабатываться оценка безопасности места происшествия, проверка реакции пострадавшего, привлечение окружающих и обращение в экстренные службы. Конкретный порядок действий и критерии их оценки должны соответствовать принятому алгоритму первой помощи и условиям задания. Если обучающийся пропускает этап, обозначенный экспертами как обязательный для безопасного продолжения, правильные ответы на последующие вопросы не должны компенсировать этот пропуск. Система фиксирует критическую ошибку и направляет обучающегося на повторную отработку соответствующего действия.

Обратная связь при этом не должна ограничиваться сообщением о неверном ответе. Помощнику следует объяснить, с каким риском связан допущенный пропуск, а затем предложить сходную задачу с другими исходными условиями. Повторное выполнение позволит проверить, понял ли обучающийся основание выбранного порядка действий или лишь запомнил ответ из предыдущей попытки.

Следовательно, основанием для изменения учебного маршрута должно служить не только число ошибок. Не менее важны их характер, этапы, на которых они возникают, повторяемость и возможные последствия для пострадавшего. Такая оценка позволяет направлять обучающегося на отработку конкретных затруднений, а не просто увеличивать количество заданий.

С.Г. Тополян отмечает возможности генеративных моделей в создании качественных текстов, изображений, видео и аудиоматериалов. При этом автор обращает внимание на ограничения таких технологий: модели могут выдавать недостоверные сведения, а их использование сопряжено с рисками нарушения авторских прав. К числу проблем также относятся сложность моделей, трудности интерпретации их работы и возможность применения в злонамеренных целях [9]. В учебной практике эти ограничения требуют проверки создаваемых материалов. Важно оценивать не только точность содержащихся в них сведений, но и то, насколько содержание отвечает задачам обучения и требованиям безопасности.

Основным риском применения генеративной модели связан с возможностью формирования правдоподобных, но непроверенных указаний. Поэтому свободное порождение текста допустимо прежде всего на уровне языка объяснения. Правила выбора действий, обязательные ограничения и признаки критических ошибок должны поступать из контролируемого содержания. Отдельный риск связан с несогласованностью целей ИИ с целями и ценностями человека, что может приводить к манипулятивному или обманному поведению системы и требует контроля ее применения в обучении [10].

Перед публикацией новой версии необходимо проверять не только правильные ответы, но и реакции на неполные, противоречивые и провокационные запросы. Существенное значение имеют ситуации, когда пользователь просит проигнорировать правила тренажера, предлагает опасное действие или описывает состояние, не предусмотренное сценарием. В таких случаях система должна ограничивать оценку, уточнять условия либо завершать неподдерживаемую ветвь диалога.

В системе необходимо предусмотреть четкую границу между тренировкой и помощью при реальном происшествии. Сообщение пользователя о чрезвычайной ситуации, которая происходит в данный момент, должно прерывать занятие. Вместо следующего задания интерфейс должен выводить краткое сообщение о необходимости связаться с экстренными службами

Показатели апробации

| ПОКАЗАТЕЛЬ                      | СПОСОБ ОПРЕДЕЛЕНИЯ                                                                         | НАЗНАЧЕНИЕ                                  |
|---------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------|
| Доля критических ошибок         | Отношение числа критических ошибок к числу заранее определенных возможностей их совершения | Оценка безопасности решений                 |
| Корректность последовательности | Проверка обязательных действий и зависимостей между ними                                   | Оценка процедурного компонента              |
| Самостоятельность               | Учет выполнения без подсказок при сопоставимой сложности                                   | Выявление зависимости от поддержки          |
| Перенос знаний                  | Решение нового сценария на ранее изученный принцип                                         | Различение понимания и запоминания          |
| Сохранение результата           | Повторное оценивание после фиксированного интервала                                        | Оценка устойчивости освоения                |
| Практическое выполнение         | Наблюдение инструктора по стандартизированному чек-листу                                   | Проверка действий вне текстового интерфейса |
| Согласованность оценивания      | Сопоставление автоматизированных заключений и экспертной разметки                          | Проверка оценочного модуля                  |
| Небезопасные ответы системы     | Экспертная проверка сообщений на контрольном наборе                                        | Выявление рисков генерации                  |

по номеру 112 и следовать указаниям диспетчера. При этом пользователь должен понимать назначение помощника: он служит для обучения, но не заменяет экстренную связь и не гарантирует правильность индивидуальных решений в условиях реального происшествия.

Отдельного внимания заслуживают пределы оценки практических навыков. Текстовый ответ позволяет проверить, понимает ли обучающийся порядок действий, однако не показывает, способен ли он правильно выполнить их. Знание последовательности приема и владение самим приемом — разные результаты подготовки. По этой причине итог цифрового занятия должен отражать успешность решения учебных задач. Рассматривать его как подтверждение полной готовности к оказанию первой помощи было бы необоснованно.

Объем данных в учебном журнале следует определять исходя из задач анализа обучения. Для работы сценарного тренажера сведения о реальных пострадавших не нужны. Преподавателю достаточно видеть обезличенные идентификаторы обучающихся, допущенные ошибки и изменения результатов по мере выполнения заданий. Такой состав отчетности позволяет отслеживать учебный прогресс без сбора избыточной информации.

Предложенную модель необходимо проверять по двум направлениям: безопасность работы системы и ее влияние на результаты обучения. Каждое из них требует самостоятельной оценки. Отсутствие программных сбоев само по себе не свидетельствует о повышении качества подготовки. Аналогично, улучшение результатов тестирования не означает, что помощник не допускает опасных рекомендаций.

Основой технической проверки должен стать набор сценариев с экспертной разметкой. Помимо ти-

повых заданий, в него необходимо включить неоднозначные ответы пользователей, критические ошибки и вопросы, выходящие за рамки предметной области. Решения помощника следует сопоставлять с экспертными оценками. Особое внимание нужно уделить случаям, в которых система принимает опасное действие за допустимое: такие ошибки непосредственно затрагивают безопасность обучения и должны учитываться отдельно.

Образовательную результативность предлагается оценивать путем сравнения двух групп. Основное содержание обучения и практическая часть должны быть одинаковыми; различаться будет организация самостоятельной подготовки. Первая группа использует обычные электронные материалы, вторая — интеллектуального помощника. При этом необходимо учитывать время, затраченное участниками на занятия. Без такого учета нельзя обоснованно установить, связано ли улучшение результатов с адаптивной поддержкой или с большей продолжительностью подготовки.

Оценивание следует проводить до подготовки, непосредственно после нее и после заранее установленного перерыва (табл. 3). Практические задания должен проверять инструктор, по возможности не осведомленный о принадлежности участника к группе.

В качестве основного образовательного исхода целесообразно заранее определить долю участников, допустивших хотя бы одну критическую ошибку при самостоятельном выполнении контрольного сценария. Такой показатель не позволяет скрыть опасное решение за высоким суммарным баллом по второстепенным вопросам.

Дополнительный анализ может учитывать число ошибок, качество переноса и отсроченные результаты. При статистической обработке необходимо принимать



во внимание повторные измерения у одного участника и групповой характер подготовки, если распределение проводится по учебным коллективам. Объем выборки определяется до начала исследования исходя из основного исхода, ожидаемого эффекта и выбранной схемы анализа.

Удовлетворенность пользователей следует рассматривать как самостоятельную характеристику удобства, а не как доказательство сформированности навыков. Аналогично сокращение времени ответа не всегда означает улучшение: поспешное решение может быть ошибочным. Скорость имеет смысл интерпретировать только совместно с правильностью действий и с учетом особенностей интерфейса.

В предлагаемой модели генерация учебных текстов играет вспомогательную роль. Основное внимание уделяется организации действий пользователя и проверке правильности их выполнения. Для этого диалоговая поддержка отделена от оценки предметных знаний и навыков: языковая модель может менять формулировки объяснений и подсказок, тогда как оценивание должно опираться на заранее заданные правила и критерии. Таким образом, гибкость общения сохраняется, но определение безопасной последовательности действий не зависит исключительно от ответов языковой модели.

При персонализации обучения важно не ограничиваться темами, в которых пользователь допускает ошибки. Если предлагать задания только по этим те-

мам, ранее освоенные действия могут остаться без необходимого повторения. Поэтому индивидуальный маршрут должен включать как работу над выявленными затруднениями, так и периодическую проверку выполнения всей последовательности действий.

Предложенная модель пока не реализована программно и не прошла эмпирическую проверку. На данном этапе она описывает архитектуру системы и требования к ее разработке. Делать выводы о повышении результативности обучения или достижении заданного уровня безопасности преждевременно: для этого необходимы программная реализация и последующая проверка модели.

### Заключение

В результате теоретико-проектного исследования предложена концептуальная модель интеллектуального помощника для обучения населения алгоритмам оказания первой помощи. Ее основой является разделение экспертно-проверенного содержания, сценарной логики, адаптации учебного маршрута и языкового взаимодействия.

Практическое применение помощника целесообразно в составе смешанной подготовки. Цифровая среда может поддерживать изучение и повторение порядка действий, тогда как отработка моторных навыков и подтверждение качества их выполнения требуют отдельной практической проверки.

### Литература

1. Станишевский А.Л. Некоторые аспекты готовности населения к оказанию первой помощи // Неотложная медицинская помощь. Журнал им. Н.В. Склифосовского. 2025. Т. 14. № 2. С. 416—422. DOI: 10.23934/2223-9022-2025-14-2-416-422. EDN: GGQHMP.
2. Минаева Н.В. Перспективы и возможности массового обучения населения оказанию первой помощи: взгляд региона // Актуальные вопросы современного медицинского образования: традиции и инновации : материалы IV Межд. науч.-практ. конф., Ижевск, 25—28 ноября 2024 г. Ижевск: Ижевская государственная медицинская академия, 2024. С. 89—94. EDN: EJLLRN.
3. Васильев Р.В. Внедрение информационных технологий в систему подготовки курсантов МЧС России: цифровизация обучения навыкам оказания первой помощи // Правовая информатика. 2026. № 2. С. 186—193. DOI: 10.24412/1994-1404-2026-2-186-193. EDN: JYEGFS.
4. Иванова Н.П. Интеллектуальный ассистент социального педагога // Вопросы педагогики. 2021. № 4-1. С. 128—132. EDN: DKFAWV.
5. Педагогические и психологические аспекты применения интеллектуальных помощников при самостоятельном освоении учебного материала / С.А. Бронев, В.В. Калитина, И.А. Аксененко, Е.А. Степанова // Фундаментальная и прикладная наука: состояние и тенденции развития : сб. ст. XXXI Межд. науч.-практ. конф., Петрозаводск, 22 июня 2023 г. Петрозаводск: Новая наука, 2023. С. 192—199. DOI: 10.46916/23062023-1-978-5-00215-032-8. EDN: NGFXJQ.
6. Пальчунов Д.Е., Якобсон А.А. Разработка интеллектуального помощника для подбора товаров в процессе диалога с пользователем // Бизнес-информатика. 2024. Т. 18. № 1. С. 7—21. DOI: 10.17323/2587-814X.2024.1.7.21. EDN: EJQWOY.
7. Персональный когнитивный ассистент: концепция и принципы работы / И.В. Смирнов, А.И. Панов, А.А. Скрынник, Е.В. Чистова // Информатика и ее применения. 2019. Т. 13. № 3. С. 105—113. DOI: 10.14357/19922264190315. EDN: QQSTUK.

8. Тополян С.Г. Перспективы развития генеративных моделей // Парадигма. 2025. № 5-5. С. 308—314. EDN: XWCKND.
9. Намиот Д.Е., Ильюшин Е.А. О киберрисках генеративного искусственного интеллекта // International Journal of Open Information Technologies. 2024. Т. 12. № 10. С. 109—119. EDN: JZCUQS.
10. Гафуров Н.Н. Современные способы обучения населения оказанию первой помощи пострадавшим при чрезвычайных ситуациях и несчастных случаях // Universum: медицина и фармакология : электрон. научн. журн. 2022. № 7 (90). URL: <https://7universum.com/ru/med/archive/item/14021> (дата обращения: 09.09.2026).

**SECTION:**  
REGULATORY INFORMATICS

## INTELLIGENT ASSISTANT FOR TEACHING THE GENERAL PUBLIC FIRST-AID PROCEDURES

Vasilyev R.V.<sup>2</sup>

**Keywords:** artificial intelligence, scenario-based simulator, feedback, learning-path adaptation, digital support.

### Abstract

**Purpose of work:** to substantiate the structure of an intelligent assistant for teaching first aid to the general public and to define criteria for evaluating such an educational tool.

**Research method:** Scientific publications devoted to the use of artificial intelligence and digital technologies in public training were analyzed.

**Results of the study:** An architecture of an intelligent assistant was proposed, including a knowledge base, training scenarios, a dialogue interface, a model of each user's learning progress, and knowledge assessment tools. This architecture is based on distinguishing between the content and the method of its presentation. Safety requirements remain unchanged, whereas explanations and the form in which the material is presented may be adapted to the learner's level of training. An approach to knowledge assessment was proposed in which critical errors are recorded separately. Correct answers to secondary questions do not compensate for errors that affect the safety of actions. Indicators were defined to assess the assistant's technical quality, the acquisition of first-aid procedures, and the transfer of the acquired knowledge to practical activities.

**Practical value:** The proposed concept may serve as a basis for preparing technical specifications for a digital educational tool and developing scenario-based simulators. The assistant may also be used for independent revision of the material between face-to-face classes. Its primary purpose is to supplement practical training under an instructor's guidance rather than replace it.

### References

1. Stanishevskii A.L. Nekotorye aspekty gotovnosti naseleniia k okazaniu pervoi pomoshchi // Neotlozhnaia meditsinskaia pomoshch'. Zhurnal im. N.V. Sklifosovskogo. 2025. T. 14. No. 2. S. 416—422. DOI: 10.23934/2223-9022-2025-14-2-416-422. EDN: GGQHMP.
2. Minaeva N.V. Perspektivy i vozmozhnosti massovogo obucheniia naseleniia okazaniu pervoi pomoshchi: vzgliad regiona // Aktual'nye voprosy sovremennogo meditsinskogo obrazovaniia: traditsii i innovatsii : materialy IV Mezhd. nauch.-prakt. konf., Izhevsk, 25—28 noiabria 2024 g. Izhevsk: Izhevskaiia gosudarstvennaia meditsinskaia akademiia, 2024. S. 89—94. EDN: EJLLRN.
3. Vasil'ev R.V. Vnedrenie informatsionnykh tekhnologii v sistemu podgotovki kursantov MChS Rossii: tsifrovizatsiia obucheniia navykam okazaniia pervoi pomoshchi // Pravovaia informatika. 2026. No. 2. S. 186—193. DOI: 10.24412/1994-1404-2026-2-186-193. EDN: JYEGFS.
4. Ivanova N.P. Intellektual'nyi assistent sotsial'nogo pedagoga // Voprosy pedagogiki. 2021. No. 4-1. S. 128—132. EDN: DKFAWV.

---

<sup>2</sup> **Roman V. Vasilyev**, Senior Lecturer, Department of Emergency Safety, Ural Institute of the State Fire Service of the Ministry of Emergency Situations of Russia, Ekaterinburg, Russian Federation.  
E-mail: [roman\\_vasilyev\\_1972@mail.ru](mailto:roman_vasilyev_1972@mail.ru)

5. Pedagogicheskie i psikhologicheskie aspekty primeneniia intellektual'nykh pomoshchnikov pri samostoiatel'nom osvoenii uchebnogo materiala / S.A. Bronov, V.V. Kalitina, I.A. Aksenenko, E.A. Stepanova // Fundamental'naia i prikladnaia nauka: sostoianie i tendentsii razvitiia : sb. st. XXXI Mezhd. nauch.-prakt. konf., Petrozavodsk, 22 iunia 2023 g. Petrozavodsk: Novaia nauka, 2023. S. 192—199. DOI: 10.46916/23062023-1-978-5-00215-032-8. EDN: NGFXJQ.
6. Pal'chunov D.E., Iakobson A.A. Razrabotka intellektual'nogo pomoshchnika dlia podbora tovarov v protsesse dialoga s pol'zovatelem // Biznes-informatika. 2024. T. 18. No. 1. S. 7—21. DOI: 10.17323/2587-814X.2024.1.7.21. EDN: EJQWOY.
7. Personal'nyi kognitivnyi assistent: kontseptsii i printsipy raboty / I.V. Smirnov, A.I. Panov, A.A. Skrynnik, E.V. Chistova // Informatika i ee primeneniia. 2019. T. 13. No. 3. S. 105—113. DOI: 10.14357/19922264190315. EDN: QQSTUK.
8. Topolian S.G. Perspektivy razvitiia generativnykh modelei // Paradigma. 2025. No. 5-5. S. 308—314. EDN: XWCKND.
9. Namiot D.E., Il'iushin E.A. O kiberriskakh generativnogo iskusstvennogo intellekta // International Journal of Open Information Technologies. 2024. T. 12. No. 10. S. 109—119. EDN: JZCUQS.
10. Gafurov N.N. Sovremennye sposoby obucheniia naseleniia okazaniu pervoi pomoshchi postradavshim pri chrezvychainykh situatsiiakh i neschastnykh sluchaiaikh // Universum: meditsina i farmakologiiia : elektron. nauchn. zhurn. 2022. 7(90). URL: <https://7universum.com/ru/med/archive/item/14021> (data obrashcheniia: 09.09.2026).



# ЦИФРОВИЗАЦИЯ ПРОЦЕССОВ НАУЧНОЙ КАРЬЕРЫ: ТРАНСФОРМАЦИЯ РОЛИ УНИВЕРСИТЕТОВ В СТРАНАХ ШОС

Башмакова В.И.<sup>1</sup>

**Ключевые слова:** цифровизация образования, цифровое неравенство, наукометрия, институциональная трансформация университетов, платформизация образования, суверенитет образовательных систем, интеграционные процессы, цифровая экосистема.

## Аннотация

Цель работы состоит в исследовании трансформации роли университетов государств — членов Шанхайской организации сотрудничества в условиях перехода от цифровых процедур приёма к комплексным системам управления научной карьерой исследователей, а также в выявлении институциональных рисков, сопровождающих данный переход.

**Метод исследования.** В работе применяется сравнительно-институциональный анализ, позволяющий сопоставить организационные и технологические решения, реализованные университетами России, Китая, Казахстана и иных государств — членов ШОС. Наряду с этим используется вторичный анализ эмпирических данных из рецензируемых источников, а также метод критического дискурс-анализа применительно к нормативным документам в сфере образовательной политики. Теоретическим основанием служит концепция платформизации, разработанная применительно к образовательной сфере Н. Селвином и Л. Кастанедой, а также исследования институциональных трансформаций университетов в условиях цифровой экономики.

**Результаты исследования.** Установлено, что цифровая трансформация университетов стран ШОС в сфере приёма и управления карьерой носит принципиально неравномерный характер. Выявлено, что платформизация управления карьерой порождает системный риск делегирования академической власти коммерческим платформам. Показано, что наукометрические системы государств ШОС формируют разнонаправленные давления на исследователей, нередко подавляя локальные научные повестки. Обосновывается тезис о необходимости модели «совместимости при разнообразии» как альтернативы унификации в рамках региональной образовательной интеграции. Представлены выводы, соответствующие практической достоверности, среди которых задокументированный опыт китайской реформы наукометрической политики, эмпирические данные о технологической зависимости постсоветских государств ШОС, зафиксированными в рецензируемых источниках, и концептуальная согласованность предлагаемых решений с действующей нормативной базой сотрудничества ШОС в сфере образования и цифровизации.

DOI: 10.24412/1994-1404-2026-3-320-326

## Введение и постановка задачи

Дискуссия о том, что именно происходит с университетом в условиях цифровизации, ведётся уже не первое десятилетие, однако её острота не убывает — напротив, по мере того как цифровые технологии проникают в новые сферы академической жизни, вопросы становятся более конкретными и практически значимыми [1]. Если первый этап цифровизации высшего образования был связан преимущественно с онлайн-обучением и электронным документообо-

ротом, то сегодня на первый план выходит иная, более глубокая трансформация: цифровые платформы из инструментов поддержки образовательного процесса превращаются в системы управления карьерой учёного — от самого начала академического пути, то есть с момента поступления в университет, до завершения исследовательской деятельности.

Именно это смещение — от цифрового приёма к цифровому управлению научной карьерой в целом —

<sup>1</sup> Башмакова Виктория Игоревна, аспирант кафедры административного и финансового права Российского университета дружбы народов имени Патриса Лумумбы, г. Москва, Российская Федерация.  
E-mail: bashmakova.v.i@rudn.ru



составляет предмет настоящего исследования. Как справедливо указывают М.В. Пашков и В.М. Пашкова, цифровые технологии не являются нейтральным инструментом: они несут в себе определённые ценностные установки, выражают стратегические интересы конкретных авторов и воспроизводят логику тех социально-экономических сил, в среде которых разрабатываются [2, с. 44]. Применительно к сфере управления научной карьерой это означает, что выбор той или иной платформы, той или иной метрики оценки исследователя — это не просто технический, но глубоко политический и институциональный выбор.

Данное обстоятельство приобретает особое измерение в контексте Шанхайской организации сотрудничества. ШОС, объединяющая государства с принципиально различными правовыми системами, образовательными традициями и уровнями технологического развития, представляет собой уникальную площадку для изучения того, как единые глобальные тенденции цифровизации преломляются через национальную специфику. Как показано в исследовании Дин Синьни, посвящённом межкультурному взаимодействию в рамках ШОС, культурные, языковые и экономические различия между государствами-членами создают как барьеры для интеграции, так и потенциал её содержательного обогащения [3, с. 88]. Этот вывод справедлив и применительно к образовательной интеграции: различие систем образования государств ШОС — не только проблема, требующая унификации, но и ресурс, требующий бережного управления.

Цель настоящей статьи — проследить траекторию трансформации роли университета в государствах — членах ШОС: от цифровизации приёмной процедуры к формированию комплексных цифровых экосистем управления научной карьерой — и выявить институциональные риски, сопровождающие данный процесс. В качестве отдельной задачи обосновывается модель гармонизации, альтернативная тотальной унификации.

### **Цифровизация приёма: начало институциональной трансформации**

Процедура приёма в университет — это, по существу, первая точка соприкосновения абитуриента с институтом высшей школы, и именно здесь цифровизация проявила себя наиболее зримо и наиболее рано. Однако за внешней простотой перехода от бумажных заявлений к электронным порталам скрываются значительные институциональные сдвиги, которые нередко остаются незамеченными в управленческих дискуссиях.

Применительно к государствам — членам ШОС можно выделить несколько характерных моделей цифровизации приёма, каждая из которых отражает специфику национального контекста. Российская модель, основанная на суперсервисе «Поступление в вуз онлайн» и централизованном механизме Единого государственного экзамена, наиболее последовательно

реализует логику государственной стандартизации процедуры. Китайская модель, опирающаяся на систему гаокао, исторически предшествовала цифровизации: здесь электронные технологии были последовательно наложены на уже сложившийся централизованный институт. Казахская система Единого национального тестирования концептуально близка российской, хотя и имеет существенные отличия в части распределения государственных образовательных грантов.

Что объединяет все три модели — и что заслуживает особого внимания, — так это то обстоятельство, которое точно зафиксировано в сравнительном анализе корпоративной культуры университетских комплексов: цифровые системы управления воспроизводят и нередко усиливают уже существующие иерархии и неравенства [4, с. 91]. Цифровой суперсервис приёма, будучи одинаковым для всех университетов страны — от ведущего федерального до регионального отраслевого вуза, — сглаживает различия между ними в глазах абитуриента. Однако это сглаживание носит скорее косметический характер: реальные различия в качестве образовательной среды, в научных традициях и в содержании учебных программ остаются, просто становятся менее видимыми за единым интерфейсом подачи заявления.

Не менее значим вопрос о том, какие группы населения выигрывают от цифровизации приёма, а какие оказываются в проигрыше. М.В. Пашков и В.М. Пашкова убедительно показывают, что цифровые технологии сами по себе не выравнивают образовательные возможности — напротив, они нередко воспроизводят сложившиеся социальные неравенства в новой форме [2, с. 48]. Преимущества от цифровизации приёма прежде всего извлекают те абитуриенты, которые заблаговременно обладают высокой цифровой грамотностью, устойчивым доступом к сети и умением навигировать в сложных информационных системах — то есть, как правило, выходцы из городских семей с высоким уровнем образования. Абитуриенты из отдалённых регионов, из семей с ограниченными ресурсами или с низким уровнем цифровой грамотности оказываются в условиях дополнительного структурного неравенства, хотя формально имеют равный доступ к той же платформе.

В государствах ШОС с относительно менее развитой цифровой инфраструктурой — в частности, в ряде центральноазиатских государств-членов — данная проблема стоит особенно остро. О.С. Мирошниченко и Л.А. Толстолесова в своём сравнительном анализе цифровой трансформации постсоветских государств ШОС фиксируют устойчивую технологическую зависимость этих стран от импорта ИКТ-товаров и недостаточный уровень финансирования собственных НИОКР в сфере информационных технологий [5, с. 66]. Это означает, что цифровая инфраструктура приёмных процедур в данных государствах строится преимущественно на импортных технологиях, что создаёт риски как

для технологического суверенитета, так и для устойчивости самих систем.

### **Платформизация управления карьерой: университет как субъект управления научным трудом**

Если цифровизация приёма затрагивает преимущественно «вход» в академическую систему, то следующий — и значительно более глубокий — уровень трансформации связан с цифровизацией управления научной карьерой в целом. Здесь речь идёт уже не просто о переводе административных процедур в электронный формат, но о принципиально новой институциональной логике, при которой университет из образовательного учреждения превращается в субъект управления научным трудом — с опорой на цифровые метрики, алгоритмические системы оценки и платформенные экосистемы.

Данный процесс в литературе обозначается термином «платформизация» — понятием, введённым применительно к образованию Н. Селвином и Л. Кастанедой и описывающим проникновение логики цифровых платформ в управление образовательными и исследовательскими процессами<sup>2</sup>. Платформизация управления карьерой проявляется в нескольких взаимосвязанных тенденциях.

Во-первых, это рост роли библиометрических платформ как инструментов оценки исследователей. Web of Science, Scopus и их национальные аналоги — российский РИНЦ, китайский CNKI — из систем поиска научной литературы превратились в системы присвоения репутации учёному. Когда решения о найме, продвижении, грантовом финансировании и аттестации принимаются с опорой на показатели этих платформ — h-индекс, квартиль журнала, число цитирований, — то алгоритмы платформ фактически начинают управлять карьерой исследователя. Это влечёт за собой принципиальное смещение власти: из рук академического сообщества она перетекает к владельцам платформ.

Во-вторых, это коммодификация публикационной деятельности — превращение научных статей из инструмента коммуникации знания в единицы измерения производительности труда. Как показывает исследование Ф. Шу, Лю Синь и В. Ларивьера, реформа оценки научной деятельности в Китае, направленная на частичный уход от «SCI-зависимости», свидетельствует о том, что даже в государстве с высоким уровнем централизации образовательной политики осознаются системные риски тотальной библиометризации [6, р. 330]. Тем более значимым этот вывод становится применительно к государствам ШОС с менее развитыми исследовательскими системами, где давление международных

библиометрических стандартов оказывается особенно деструктивным для локальных научных традиций.

В-третьих, цифровизация управления карьерой порождает феномен, который можно обозначить как «алгоритмическую гетерономию» учёного: его профессиональная траектория всё в большей степени определяется не собственным научным суждением и выбором исследовательской повестки, а логикой максимизации показателей в тех метриках, которые установлены внешними — нередко коммерческими — платформами. И.Г. Лакизо и А.Е. Гуськов в анализе эволюции оценки научной результативности в Китае фиксируют эту же тенденцию: на протяжении нескольких десятилетий китайские исследователи были вынуждены ориентироваться прежде всего на показатели, признаваемые международными базами данных, что оказывало существенное влияние на содержательную повестку китайской науки [7, с. 331].

### **Сравнительный анализ наукометрических систем государств ШОС**

Наукометрические системы оценки исследователей, сложившиеся в ведущих государствах — членах ШОС, при всём их внешнем сходстве обнаруживают принципиальные различия в логике и последствиях. Понимание этих различий необходимо для выработки сбалансированной политики академической интеграции в рамках организации.

В России формирование системы наукометрической оценки было тесно связано с реализацией программы поддержки ведущих университетов, ориентировавшей их на достижение определённых позиций в международных рейтингах. Как фиксирует Е. Винокуров в своём анализе динамики публикационной активности российских авторов, данная политика привела к значительному росту числа публикаций в журналах, индексируемых Scopus и Web of Science, однако этот рост имел неоднородный характер: в ряде дисциплин он сопровождался содержательным развитием исследований, тогда как в других — преимущественно адаптационными стратегиями, направленными на формальное выполнение показателей [8]. События 2022 года, повлёкшие существенные изменения в доступности международных баз данных для российских исследователей, поставили перед российским академическим сообществом вопрос о необходимости переосмысления наукометрической политики — вопрос, который в условиях ШОС приобретает и региональное измерение.

Китайская система оценки научной деятельности прошла несколько этапов эволюции, описанных в упомянутых выше работах Ф. Шу с соавторами и И.Г. Лакизо с А.Е. Гуськовым. Принципиально важным для понимания текущего момента является то, что КНР предприняла последовательные попытки снизить зависимость от международных библиометрических платформ при сохранении международной конкурентоспособности

<sup>2</sup> Castañeda L., Selwyn N. More than tools? Making sense of the ongoing digitizations of higher education // International Journal of Educational Technology in Higher Education. 2018. Vol. 15. Art. 22. DOI: 10.1186/s41239-018-0103-7.

своей науки. Введение системы «Четырёх оценок», отход от механического учёта публикаций в журналах SCI — всё это свидетельствует о стремлении государства вернуть себе определённый суверенитет в оценке научных результатов [6, р. 334; 7, с. 336].

Казахстанская система образования и науки, по оценкам исследователей, находится в процессе перехода от советской модели организации науки к модели, ориентированной на международные стандарты. Это переходное состояние создаёт специфические риски: ориентация на международные метрики оказывается особенно жёсткой именно потому, что национальная система оценки ещё не сформировалась в качестве состоятельной альтернативы. В условиях, когда публикация в журнале, индексируемом Scopus, де-факто является обязательным условием карьерного продвижения, а число таких журналов, специализирующихся на тематике, актуальной для казахстанского контекста, невелико, исследователи оказываются перед жёстким выбором: либо встраиваться в международные тематические приоритеты, либо жертвовать карьерными перспективами.

Контрастом на этом фоне выглядит образовательная система Китая с её национальной инфраструктурой цифровизации. Захаров М.Ю. и Шишкова А.В. в своём анализе цифровизации китайского образования как элемента форсайт-проекта «Датун» показывают, что Китай последовательно выстраивает собственные образовательные платформы, МООК-инфраструктуру и системы образовательной аналитики, не ограничиваясь заимствованием западных решений [9, с. 152]. К концу 2018 года число онлайн-учащихся в Китае достигло 172 млн человек, из которых 142 млн использовали мобильные устройства, а общий объём инвестиций в сферу EdTech составил около 4 млрд евро [9, с. 153]. Эта инфраструктурная самодостаточность создаёт для Китая возможности, недоступные для большинства других государств-членов ШОС: формировать собственную повестку цифровизации образования, а не следовать логике глобальных платформ.

### **Риски платформизации для академической идентичности университетов ШОС**

Анализ трансформации роли университетов в государствах ШОС позволяет выявить несколько системных рисков, которые сопровождают переход к цифровому управлению научной карьерой.

Первый и, пожалуй, наиболее серьёзный риск — это делегирование академической власти коммерческим платформам. Когда решения о карьере исследователя принимаются на основе показателей, алгоритмически вычисляемых внешними системами, университет как институт утрачивает значительную часть своей академической автономии. М.В. Пашков и В.М. Пашкова точно фиксируют этот процесс применительно к образовательным технологиям: «компьютерные инженеры, программисты и аналитики данных, созда-

ющие коммерческое программное обеспечение для образования, порой оказывают куда большее влияние на образовательный процесс, чем сами преподаватели» [2, с. 47]. Применительно к управлению карьерой та же логика означает, что стратегии развития науки фактически делегируются алгоритмам библиометрических баз данных.

Второй риск связан с тем, что можно назвать «метрической стандартизацией» исследовательской повестки. Давление наукометрических показателей побуждает исследователей в государствах ШОС концентрироваться на тематиках, востребованных международным академическим рынком, — зачастую в ущерб исследованиям, имеющим локальную или региональную значимость. В условиях ШОС это создаёт парадоксальную ситуацию: именно те вопросы, которые наиболее актуальны для устойчивого развития государств-членов, оказываются наименее «метрически выгодными» для исследователей.

Третий риск — воспроизведение и усиление цифрового неравенства между государствами-членами. О.С. Мирошниченко и Л.А. Толстолесова убедительно показывают, что страны постсоветского пространства в рамках ШОС испытывают устойчивую технологическую зависимость от импорта ИКТ-товаров, тогда как их доля в экспорте продукции данной группы ничтожно мала [5, с. 67]. Это означает, что цифровые платформы управления карьерой, которые развёртываются в этих странах, по большей части являются импортированными решениями, несущими в себе логику тех правовых порядков, в которых они были созданы.

Четвёртый риск связан с вопросом, который ставят М.В. Пашков и В.М. Пашкова применительно к высшему образованию в целом: сможет ли университет в условиях цифровизации продолжать выполнять свою роль в производстве «общих благ» — тех результатов, которые приносят пользу широким слоям населения, а не только непосредственным участникам образовательного рынка [2, с. 50]? Применительно к управлению научной карьерой этот вопрос трансформируется следующим образом: не ведёт ли логика цифровых метрик к тому, что ценность научного исследования всё в большей мере определяется его «видимостью» в международных базах данных, а не его реальным вкладом в решение актуальных общественных проблем?

### **Перспективы интеграции: в поисках модели «совместимости при разнообразии»**

Сказанное выше не означает, что академическая интеграция в рамках ШОС лишена смысла или что цифровизация управления карьерой неизбежно ведёт к негативным последствиям. Напротив, именно в рамках ШОС существуют уникальные условия для выработки альтернативной модели — модели, которую можно обозначить как «совместимость при разнообразии».

Суть данной модели состоит в том, что национальные системы управления научной карьерой сохраняют

свою специфику — свои метрики, свои языки научной коммуникации, свои представления о значимости исследований, — но при этом обеспечивают стандартизированные точки сопряжения, позволяющие данным о публикационной активности, грантовой истории и академических квалификациях перемещаться между национальными системами без потери смысла<sup>3</sup>. Технически это достижимо — аналогом может служить международный идентификатор ORCID, создающий наднациональный слой видимости исследователя при полном сохранении национальных систем оценки.

Для реализации данной модели в рамках ШОС необходимо несколько условий. Во-первых, политическая воля государств-членов к разработке совместных стандартов академической идентификации, не предполагающих унификации содержательных критериев оценки. Во-вторых, готовность национальных библиометрических платформ к открытию интерфейсов для взаимодействия — без утраты независимости. В-третьих, инвестиции в цифровую инфраструктуру государств — членов ШОС с менее развитыми ИКТ-секторами, позволяющие преодолеть технологическую зависимость, зафиксированную О.С. Мирошниченко и Л.А. Толстоловой [5, с. 73].

Межкультурное измерение данной задачи, зафиксированное в исследовании Дин Синьи, не менее значимо: различия в языках, религиях, политических системах и образовательных традициях государств ШОС создают реальные барьеры для интеграции, которые не могут быть преодолены исключительно техническими решениями [3, с. 91]. По мнению Д.М. Ковба и Е.Г. Грибовод, активизация академической мобильности приводит к интернализации и повышению прозрачности научного и образовательного процессов [10, с. 16]. Подлинная академическая интеграция в рамках ШОС требует не просто совместимых платформ, но и содержательного диалога между научными школами, между языками науки, между исследовательскими традициями — диалога, который цифровые инструменты могут поддержать, но не могут заменить.

### Результаты и выводы

Проведённое исследование позволяет сформулировать следующие выводы.

Во-первых, трансформация роли университета в государствах — членах ШОС — от преимущественно образовательного института к субъекту управления научным трудом — является реальным и уже происходящим процессом, хотя его интенсивность и формы существенно варьируются между государствами-членами.

Во-вторых, цифровизация приёма, будучи наиболее зримой и хорошо задокументированной частью

этой трансформации, несёт в себе риски воспроизведения цифрового неравенства, особенно острые в государствах ШОС с недостаточно развитой ИКТ-инфраструктурой. Формальное равенство доступа к цифровым платформам не тождественно реальному равенству возможностей.

В-третьих, платформизация управления научной карьерой — через библиометрические системы оценки, цифровые реестры квалификаций и алгоритмические системы аттестации — является наиболее системно значимой частью трансформации, поскольку именно она определяет, какая наука производится, кем и в каких институциональных условиях. Делегирование академической власти коммерческим платформам представляет собой институциональный риск, требующий осмысленной политической реакции.

В-четвёртых, опыт КНР по формированию суверенной наукометрической политики, зафиксированный в работах Ф. Шу с соавторами и И.Г. Лакизо с А.Е. Гуськовым, представляет практический интерес для иных государств-членов ШОС — не как образец для копирования, но как свидетельство принципиальной возможности сохранения национального суверенитета в условиях глобального давления библиометрических стандартов.

В-пятых, оптимальной моделью академической интеграции в рамках ШОС представляется не унификация, а «совместимость при разнообразии» — сохранение национальной специфики систем управления карьерой при обеспечении стандартизированных точек сопряжения между ними.

Практическая достоверность предложенных выводов подтверждается, во-первых, задокументированным опытом китайской реформы наукометрической политики, во-вторых, эмпирическими данными о технологической зависимости постсоветских государств ШОС, зафиксированными в рецензируемых источниках, и в-третьих, концептуальной согласованностью предлагаемых решений с действующей нормативной базой сотрудничества ШОС в сфере образования и цифровизации.

<sup>3</sup> Колегова О.Ю. ШОС как инструмент региональной интеграции: проблемы расширения // Вестник МГИМО Университета. 2013. № 1 (28). С. 249—253. EDN: PYVZSL.



## Литература

1. Петрова Т.Э., Черкасова Т.В. Цифровизация образования: взгляд студентов российских вузов // Мониторинг правоприменения. 2025. № 3 (56). С. 163—169.
2. Пашков М.В., Пашкова В.М. Проблемы и риски цифровизации высшего образования // Высшее образование в России. 2022. Т. 31. № 3. С. 40—57. DOI: 10.31992/0869-3617-2022-31-22-3-40-57.
3. Дин Синь. Основные вызовы межкультурного взаимодействия в рамках интеграционных процессов на пространстве ШОС // Постсоветские исследования. 2023. Т. 6. № 1. С. 87—97.
4. Козлова Ю.Б. Сравнительный анализ корпоративной культуры университетских комплексов: исторический аспект и современные тенденции // История и педагогика естествознания. 2024. № 1. С. 90—95. DOI: 10.24412/2226-2296-2024-1-90-95.
5. Мирошниченко О.С., Толстолесова Л.А. Цифровая трансформация как фактор роста и устойчивого развития национальных экономик: сравнительный анализ стран постсоветского пространства, входящих в ШОС // Россия и мир в XXI веке. 2024. № 3. С. 59—77. DOI: 10.31249/rsm/2024.03.04.
6. Shu F., Liu S., Larivière V. China's Research Evaluation Reform: What are the Consequences for Global Science? // Minerva. 2022. Vol. 60. P. 329—347. DOI: 10.1007/s11024-022-09468-7.
7. Лакизо И.Г., Гуськов А.Е. Эволюция оценки научной результативности в Китае // Вестник Российской академии наук. 2023. Т. 93. № 4. С. 329—341. DOI: 10.31857/S0869587323040047.
8. Vinokurov E. Dynamics of the Publication Activity and Citation of Russian Authors // Sociology of Science and Technology. 2021. Vol. 12. № 3.
9. Захаров М.Ю., Шишкова А.В. Цифровизация образования в Китае как элемент трансформации общественного идеала «Датун» в национальный форсайт-проект // Миссия Конфессий. 2023. Т. 12. Ч. 3. С. 147—156.
10. Ковба Д.М., Грибовод Е.Г. Международная академическая мобильность сквозь призму теории «мягкой силы» // Образование и наука. 2019. № 10. С. 9—30.

SECTION:  
REGULATORY INFORMATICS

# DIGITALIZATION OF ACADEMIC CAREER PROCESSES: TRANSFORMING THE ROLE OF UNIVERSITIES IN THE SCO COUNTRIES

**Bashmakova V.I.<sup>4</sup>**

**Keywords:** digitalization of education, digital inequality, scientometrics, institutional transformation of universities, platformization of education, sovereignty of educational systems, integration processes, digital ecosystem.

## Abstract

**Purpose of work:** This study examines the transformation of the role of universities in the member states of the Shanghai Cooperation Organisation (SCO) amid the transition from digital admissions procedures to comprehensive systems for managing researchers' academic careers. It also identifies the institutional risks associated with this transition.

**Research methods:** The study employs comparative institutional analysis to examine the organisational and technological solutions implemented by universities in Russia, China, Kazakhstan, and other SCO member states. It also draws on a secondary analysis of empirical data from peer-reviewed sources and applies critical discourse analysis to regulatory documents in the field of education policy. The theoretical framework is based on the concept of platformization as applied to education by Neil Selwyn and L. Castañeda, as well as on studies of institutional transformations in universities under the conditions of the digital economy.

**Research results:** The study demonstrates that the digital transformation of universities in SCO countries, particularly in the areas of admissions and academic career management, is highly uneven. It reveals that the platformization of career

---

<sup>4</sup> **Viktoria I. Bashmakova**, Ph.D. student, Department of Administrative and Financial law, Peoples' Friendship University of Russia named after Patrice Lumumba, Moscow, Russian Federation.  
E-mail: [bashmakova.v.i@rudn.ru](mailto:bashmakova.v.i@rudn.ru)

*management generates a systemic risk of delegating academic authority to commercial platforms. The findings indicate that scientometric systems in SCO countries exert divergent pressures on researchers, frequently suppressing locally relevant research agendas. The study substantiates the need for a model of “compatibility through diversity” as an alternative to unification within the framework of regional educational integration. The conclusions are supported by documented evidence, including the experience of China’s scientometric policy reform, empirical data on the technological dependence of post-Soviet SCO states reported in peer-reviewed sources, and the conceptual consistency of the proposed solutions with the existing SCO regulatory framework for cooperation in education and digitalization.*

### References

1. Petrova T.E., Cherkasova T.V. Tsifrovizatsiia obrazovaniia: vzgliad studentov rossiiskikh vuzov // Monitoring pravoprimeneniia. 2025. No. 3 (56). S. 163—169.
2. Pashkov M.V., Pashkova V.M. Problemy i riski tsifrovizatsii vysshego obrazovaniia // Vysshee obrazovanie v Rossii. 2022. T. 31. No. 3. S. 40—57. DOI: 10.31992/0869-3617-2022-31-22-3-40-57.
3. Din Sin’i. Osnovnye vyzovy mezhkul’turnogo vzaimodeistviia v ramkakh integratsionnykh protsessov na prostranstve ShOS // Postsoverskie issledovaniia. 2023. T. 6. No. 1. S. 87—97.
4. Kozlova Iu.B. Sravnitel’nyi analiz korporativnoi kul’tury universitetskikh kompleksov: istoricheskii aspekt i sovremennye tendentsii // Istoriia i pedagogika estestvoznaniia. 2024. No. 1. S. 90—95. DOI: 10.24412/2226-2296-2024-1-90-95.
5. Miroshnichenko O.S., Tolstolesova L.A. Tsifrovaia transformatsiia kak faktor rosta i ustoichivogo razvitiia natsional’nykh ekonomik: sravnitel’nyi analiz stran postsoverskogo prostranstva, vkhodiashchikh v ShOS // Rossiia i mir v XXI veke. 2024. No. 3. S. 59—77. DOI: 10.31249/rsm/2024.03.04.
6. Shu F., Liu S., Larivière V. China’s Research Evaluation Reform: What are the Consequences for Global Science? // Minerva. 2022. Vol. 60. P. 329—347. DOI: 10.1007/s11024-022-09468-7.
7. Lakizo I.G., Gus’kov A.E. Evoliutsiia otsenki nauchnoi rezul’tativnosti v Kitae // Vestnik Rossiiskoi akademii nauk. 2023. T. 93. No. 4. S. 329—341. DOI: 10.31857/S0869587323040047.
8. Vinokurov E. Dynamics of the Publication Activity and Citation of Russian Authors // Sociology of Science and Technology. 2021. Vol. 12. No. 3.
9. Zakharov M.Iu., Shishkova A.V. Tsifrovizatsiia obrazovaniia v Kitae kak element transformatsii obshchestvennogo ideala “Datun” v natsional’nyi forsait-proekt // Missiia Konfessii. 2023. T. 12. Ch. 3. S. 147—156.
10. Kovba D.M., Gribovod E.G. Mezhdunarodnaia akademicheskai mobil’nost’ skvoz’ prizmu teorii “miagkoi sily” // Obrazovanie i nauka. 2019. No. 10. S. 9—30.

