ISSN 1994-1404

1

2024

ПРАВОВАЯ ИНФОРМАТИКА

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

Международная научно-практическая конференция

ИННОВАЦИОННЫЕ, ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

1-10 октября, г.Сочи

ПРАВОВАЯ ИНФОРМАТИКА

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ
№ 1, 2024 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 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).

Учредитель и издатель:
Федеральное бюджетное учреждение «Научный центр правовой информации при Министерстве юстиции Российской Федерации»

Отпечатано в РИО НЦПИ при Минюсте России.
Печать цветная цифровая.
Подписано в печать 30.03.2024 г.
Общий тираж 100 экз. Цена свободная.

Адрес редакции:
125437, Москва, Михалковская ул., 65, стр.1
Телефон: +7 (495) 539-25-29
E-mail: inform360@yandex.com
Требования, предъявляемые к рукописям, размещены на сайте
http://uzulo.su/prav-inf

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс: 34077

LEGAL INFORMATION

RESEARCH PEER-REVIEWED JOURNAL
2024, No. 1
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 1st 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).

Founder and publisher:
Federal State-Funded Institution "Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation"

Printed by the Printing and Publication Division of the Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation.
Printed in digital colour. Approved for print on the 30th of June 2023.
Number of items printed: 100. Free price.

Postal address:
Mikhalkovskaya str., bld. 65/1,
125 438, Moscow, Russia
Telephone: +7 (495) 539-25-29
E-mail: inform360@yandex.com
Guidelines for preparing manuscripts for publication can be found on the website
http://uzulo.su/prav-inf

CONTENTS

The journal can be subscribed to at post offices through the Press of Russia (Pressa Rossii) Catalogue. Publication index: 34077

ПРАВОВЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РОССИИ

Карцхия А.А.[1], Макаренко Г.И.[2]

Ключевые слова: *нейронные сети, машинное обучение, безопасность искусственного интеллекта, правовая база.*

Аннотация

Цель работы: показать правовые проблемы при развитии и внедрении искусственного интеллекта в российской действительности.

Результат. Сделан обзор темы для России, США и Китая. Хотя Россия по использованию искусственного интеллекта находится на 10-м месте в мире, однако его внедрение идет быстрыми темпами. Авторам хотелось показать (и предостеречь), что внедрение того, что называют искусственным интеллектом, развивалось еще в СССР. Один из авторов еще в 1970 году создал лабораторию машинного проектирования для автоматического проектирования 13-слойных печатных плат бортовых вычислительных машин (авиакосмических комплексов). К 1980 году в СССР были сотни подразделений в самых разных областях техники, которые занимались автоматизацией проектирования и управления. Развитие автоматизации остановилось в России в связи с остановкой развития промышленности в стране — практически полностью было ликвидировано пассажирское самолетостроение, станкостроение, приборостроение и только в последние годы страна опомнилась и начала говорить о развитии промышленности. Правда, на примере самолетостроения мы видим, что даже давно испытанные и ранее выпускавшиеся пассажирские самолеты никак не начнут выпускаться.

На пути внедрения искусственного интеллекта — не только искусственные преграды в лице нерадивых чиновников, но и объективные обстоятельства: отсутствие правовой базы.

Практическая ценность: настоящая работа является дополнением статьи авторов «Правовые горизонты технологий искусственного интеллекта: национальный и международный аспект» (журнал «Вопросы кибербезопасности», № 1 за 2024 год) и может быть полезной при разработке правовой базы.

DOI: 10.21681/1994-1404-2024-1-4-19

Введение

Современный ландшафт искусственного интеллекта (ИИ), по мнению экспертов[3], показывает, что ИИ может быть отнесен к технологиям моделирования когнитивных функций человека, позволяющей компьютерам и машинам выполнять такие задачи, как решение проблем, принятие решений, понимание и воспроизведение естественного языка, распознавание паттернов и адаптация к изменяющейся среде. Взаимодействия человека и машины могут быть прямыми, когда люди взаимодействуют с интерфейсами ИИ, или косвенными, когда системы ИИ работают на втором плане для повышения производительности или принятия решений. ИИ может использовать преимущества других новых технологий и создавать синергию с ними. Например, блокчейн может записывать данные, которые когда-нибудь могут быть использованы ИИ для построения моделей и принятия обоснованных решений на основе проверенных данных. ИИ используется также для мониторинга транзакций как в децентрализованных финансах, так и в высокочастотной торговле традиционными финансовыми продуктами. Криптовалюты для оплаты могут применять вычислительную мощность ИИ. Инструменты и датчики Интернета вещей могут предоставлять огромные объемы данных, необходимых для обучения и обработки ИИ. Облачные технологии с их огромной вычислительной мощностью используются многими моделями и приложениями ИИ.

[3] Global Standards Mapping Initiative 4.0, November 2023. URL: https://gbbcouncil.org/wp-content/uploads/2023/11/GBBC-GSMI-4.0-Update-November-2023.pdf , pp. 11–12.

[1] ***Карцхия Александр Амиранович,*** *доктор юридических наук, профессор РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва, Российская Федерация.*

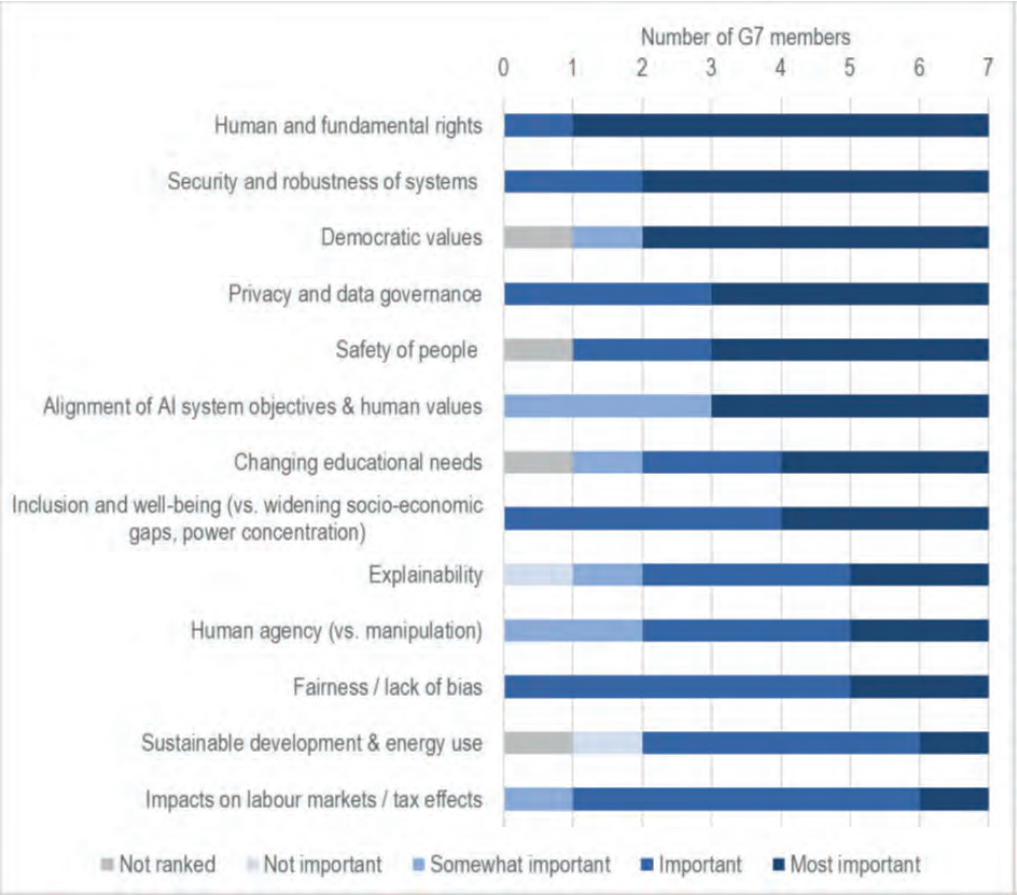
E-mail: arhz50@mail.ru

[2] ***Макаренко Григорий Иванович,*** *старший научный сотрудник ФБУ НЦПИ Минюста России, г. Москва, Российская Федерация.*

E-mail: t7920518@yandex.ru

Таблица 1.

G7 Hiroshima process on Artificial Intelligence (AI)



Вместе с тем выделяются и наиболее важные приоритеты ИИ, включая права человека и основные свободы, безопасность и надежность систем ИИ, демократические ценности, а также конфиденциальность и управление данными (см. табл. 1)[4].

В каждой из стран, входящих в лидеры разработок ИИ, в настоящее время активно реформируются направления и способы его правового регулирования[5], что подробнее мы рассмотрим далее.

Правовое регулирование сферы искусственного интеллекта в России

Для Российской Федерации развитие правового регулирования искусственного интеллекта связано, прежде всего, с ***Национальной стратегией развития искусственного интеллекта на период до 2030 года*** (далее — Стратегия), принятой в 2019 году и получившей существенные дополнения в 2024 году[6]. Стратегия провозглашает целями развития ИИ

[4] Необходимо особо ответить тем, кто боится искусственного интеллекта, кто верит, что будет восстание роботов и тому подобное. В ближайшие 50 лет такое невозможно представить. Любой существующий ИИ не способен создать ничего, чего бы не было, даже генеративный интеллект. Решение генерируется из анализа и комбинации существующих решений — вот почему любая программа генерирующего интеллекта обучается на основе большой базы решений. В этом у программ ИИ преимущество перед специалистом-человеком — человек выборку решений может выполнить за сутки и недели, в то время как программа ИИ делает это за секунды. Именно поэтому программы распознавания лиц нашли широкое распространение, так как задача сравнения лиц всегда работает с базой имеющихся лиц. Кстати, телевидение 15.03.2024 г. сообщило, что в России недавно было вынесено судебное решение об освобождение из заключения человека, которого программа ИИ определила как вероятного убийцу: сходство с портретом убийцы, произошедшее 20 лет назад, программа определила как 57%. Человек находился под следствием в заключении более года — виновата, разумеется, не программа, а следователи, которые при столь небольшом сходстве продержали человека в заключении более года. Хотелось бы знать, как наказаны следователи — если наказаны?

[5] Насколько преждевременны ожидания ИИ, показывает разоблачительная новость — компания Амазон закрывает магазины с технологией «взял и иди», где не нужно оплачивать товар на кассе, а просто уходить с ним. По задумке, компьютер сам распознавал, что Вы взяли, и автоматически списывал деньги с карты. Оказалось, что вместо ИИ за все отвечали свыше тысячи индусов, которые по камерам смотрели за покупателями и сами пробивали товар: так как технология ИИ слишком дорога для внедрения, в компании решили сэкономить с помощью дешевой рабочей силы. (Новость с Телеграмм-канала Левченко)

[6] Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации». URL: http://www.kremlin.ru/acts/bank/44731

в Российской Федерации обеспечение роста благосостояния и качества жизни ее населения, обеспечение национальной безопасности и правопорядка, достижение устойчивой конкурентоспособности российской экономики, в том числе лидирующих позиций в мире в области ИИ.

Понятие искусственного интеллекта получило уточнение в новой редакции Стратегии, где ***искусственный интеллект определяется*** как комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в т. ч. такое, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.

Сформулировано определение ***модели искусственного интеллекта,*** под которой понимается программа для электронных вычислительных машин (ее составная часть), предназначенная для выполнения интеллектуальных задач на уровне, сопоставимом с результатами интеллектуального труда человека или превосходящем их, использующая алгоритмы и наборы данных для выведения закономерностей, принятия решений или прогнозирования результатов.

Стратегия выделяет несколько новых понятий, включая:

- *большие генеративные модели* ИИ, которые способны интерпретировать (предоставлять информацию на основании запросов, например об объектах на изображении или о проанализированном тексте) и создавать мультимодальные данные (тексты, изображения, видеоматериалы и тому подобное) на уровне, сопоставимом с результатами интеллектуальной деятельности человека или превосходящем их;
- *большие фундаментальные модели* ИИ, т. е. модели, являющиеся основой для создания и доработки различных видов программного обеспечения, обученные распознаванию определенных видов закономерностей, содержащие не менее 1 млрд параметров и применяемые для выполнения большого количества различных задач;
- *перспективные методы* ИИ, т. е. методы, направленные на создание принципиально новой научно-технической продукции, в том числе в целях разработки универсального (сильного) искусственного интеллекта (автономное решение различных задач, автоматический дизайн физических объектов, автоматическое машинное обучение, алгоритмы решения задач на основе данных с частичной разметкой и (или) незначительных объемов данных, обработка информации на основе новых типов вычислительных систем, интерпретируемая обработка данных и другие методы);
- *доверенные технологии* ИИ — технологии, отвечающие стандартам безопасности, разработанные с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку и нарушения его основополагающих прав и свобод, нанесения ущерба интересам общества и государства.

Стратегия отмечает, что ИИ является одной из самых важных технологий, которые доступны человеку в настоящее время: уже сейчас благодаря ИИ происходит рост мировой экономики, ускорение инноваций во всех областях науки, повышение качества жизни населения, доступности и качества медицинской помощи, качества образования, производительности труда и качества отдыха. Технологии ИИ являются областью международной конкуренции. Технологическое лидерство в области ИИ может позволить государствам достичь значимых результатов по основным направлениям социально-экономического развития. В конце 2010-х годов органы власти развитых стран стали уделять особое внимание развитию технологий ИИ. К настоящему времени более 60 стран разработали и утвердили собственные национальные стратегии развития ИИ.

Как указано в новой редакции Стратегии, в 2022—2023 годах в мире произошел новый скачок в развитии технологий ИИ благодаря совершенствованию больших генеративных моделей в области языка, изображений (включая видеоизображения) и звука. Большие фундаментальные модели уже сейчас способны писать программные коды по техническим заданиям, сочинять поэмы на заданную тему, давать точные и понятные ответы на тестовые вопросы различных уровней сложности, в том числе из образовательных программ. Модели ИИ за секунды создают изображения на любую тему по заданному текстовому описанию или наброску, что создает угрозу распространения запрещенной информации, нарушения авторских прав и генерации ошибочных сведений.

Искусственный интеллект окажет существенное влияние на экономический рост в мире. По оценкам экспертов, дальнейшее развитие больших генеративных моделей может вызвать резкое повышение производительности труда, которое приведет к увеличению мирового валового внутреннего продукта на 1—2% ежегодно и позволит повысить оплату труда специалистов во всех отраслях экономики за счет увеличения объема выпуска продукции (товаров, работ, услуг) и улучшения ее качества.

По итогам 2023 года, как отмечено в новой редакции Стратегии, в Российской Федерации созданы необходимые правовые условия для достижения целей, выполнения основных задач и реализации мер, предусмотренных настоящей Стратегией:

а) Правительство Российской Федерации утвердило Концепцию развития регулирования отношений в сфере технологий ИИ и робототехники до 2024 года[7];

б) сняты отдельные административно-правовые барьеры, препятствовавшие внедрению технологий ИИ в отдельных областях, включая здравоохранение, транспорт, государственно-частное партнерство и другие области;

в) принят Кодекс этики в сфере искусственного интеллекта[8], создана Комиссия по реализации Кодекса этики в сфере искусственного интеллекта и определены уполномоченные по этике в каждой организации, подписавшей данный Кодекс (по состоянию на ноябрь 2023 г. — 43 федеральных органа исполнительной власти, 17 органов исполнительной власти субъектов Российской Федерации, более 330 российских организаций и 23 иностранные организации присоединились к Кодексу этики в сфере искусственного интеллекта как стандарту, признанному на международном уровне);

г) сформирована система регулирования общественных отношений в области ИИ посредством публикации негосударственных актов рекомендательного характера («мягкое право»).

Российскими организациями создаются модели ИИ мирового уровня, в том числе в области генерации изображений, генерации и обработки текстов на русском и английском языках, медицины, генетики.

Как указывается в новой редакции Стратегии, изменение экономической ситуации, односторонние ограничительные меры недружественных иностранных государств и иные изменения рыночной конъюнктуры, которые произошли в 2022—2023 годах, определили новые вызовы для Российской Федерации:

а) нехватка вычислительных мощностей, недостаточное развитие отечественных решений в области ИИ, включая программно-аппаратные комплексы и электронную компонентную базу;

б) дефицит высококвалифицированных специалистов и инновационных разработок в области ИИ;

в) низкий уровень внедрения технологий ИИ в государственном управлении;

г) нехватка кадров для обеспечения массового внедрения технологий ИИ;

д) недостаточное субсидирование организаций, осуществляющих деятельность в области ИИ, и недостаток частных инвестиций в их развитие, в том числе на этапах предоставления венчурного финансирования, разработки концепции, проведения исследований, тестирования, промышленной разработки и эксплуатации технологий ИИ;

е) нормативные барьеры, препятствующие внедрению технологий ИИ в отдельных отраслях экономики, включая отсутствие методологической базы для обеспечения систем ИИ достоверными исходными данными;

ж) необходимость обеспечения безопасности при разработке и использовании технологий ИИ;

з) необходимость обеспечения защиты персональных данных и иной информации ограниченного доступа, объектов интеллектуальных прав при создании и обучении моделей ИИ;

и) ограничение доступа к технологиям ИИ в связи с недобросовестной конкуренцией со стороны недружественных иностранных государств и введением ими односторонних ограничительных мер;

к) возникновение в сфере разработки, создания и использования технологий ИИ новых типов угроз информационной безопасности, нехарактерных для других сфер применения информационных технологий;

л) дополнительные международные барьеры, препятствующие развитию ИИ в России и ограничивающие международное сотрудничество со стороны граждан и организаций недружественных иностранных государств.

Кроме того, новая редакция Стратегии определила цели и основные задачи развития ИИ, основные принципы развития и использования технологий ИИ, а также направления поддержки развития инфраструктуры и разработчиков технологий ИИ, стимулирование их внедрения и другие принципиальные вопросы регулирования ИИ.

Вместе с тем для обеспечения и защиты национальных интересов Российской Федерации от внешних и внутренних угроз, в том числе от недружественных действий иностранных государств, как указано в Стратегии национальной безопасности Российской Федерации[9], необходимо повысить эффективность использования имеющихся достижений и конкурентных преимуществ Российской Федерации с учетом долгосрочных тенденций мирового развития. Для решения поставленных задач в сфере национальной безопасности ИИ используется как инструмент обеспечения информационной безопасности на основе применения передовых технологий, включая технологии ИИ и квантовые вычисления, как средство модернизации промышленных предприятий и инфраструктуры, цифровизации в целях повышения производительности труда, а также в целях научно-технологического развития России установлено развитие перспективных высоких технологий, таких как нанотехнологии, робототехника, медицинские, биологические, генной инженерии, информационно-коммуникационные, квантовые, ИИ, обработки больших данных, энергетические, лазерные, аддитивные, создания новых материалов, когнитивные, природоподобные технологии.

В целях повышения эффективности государственной научно-технической политики и обеспечения технологической независимости и конкурентоспособ-

[7] Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ. 2020. № 35. Ст. 5593.

[8] Кодекс этики в сфере искусственного интеллекта. URL: https://ethics.a-ai.ru/

[9] Указ Президента РФ от 02.07.2021 № 400 (ред. от 15.02.2024) «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

ности Российской Федерации, достижения ее национальных целей развития и реализации стратегических национальных приоритетов принят ***Указ Президента Российской Федерации от 02.11.2023 № 818 «О развитии природоподобных технологий в Российской Федерации»***[10], предусматривающий определение основных принципов и критериев отнесения технологий к природоподобным, а также разработку плана мероприятий, направленных на развитие природоподобных технологий в Российской Федерации и ее субъектах, в т. ч. на создание передовой научной инфраструктуры, формирование кадровых ресурсов и проведение научных исследований в этой сфере.

Природоподобные технологии представляют собой технологии, воспроизводящие системы и процессы живой природы в виде технических систем и технологических процессов, интегрированных в естественный природный ресурсооборот — так называемые конвергентные НБИКС-технологии (нано-, био-, информационные, когнитивные и социогуманитарные науки и технологии), которые, по мнению специалистов Курчатовского института[11], открывают возможность воспроизведения абсолютно всех систем и процессов живой природы и позволят создать гармоничную ноосферу, в которой три ее составляющие — биосфера, техносфера и общество — будут не конфликтовать, а дополнять друг друга, то есть будут конвергентны. Природоподобные технологии основаны на изучении образцов, объектов и процессов живой природы, осмыслении их механизмов и затем воспроизводстве в виде технических решений. В идеале возможно создание «биоискусственной клеточной системы», включая человека или его органов.

Эти технологии могут реализовываться в сочетании с технологиями ИИ. К примеру, японские специалисты смогли впервые в мире разработать технологию, которая с помощью генеративного искусственного интеллекта позволяет создавать изображения на основе обработки сигналов человеческого мозга (декабрь 2023 г.). Ранее проведенные исследования показали, что изображения, увиденные человеком, могут быть реконструированы на основе сигналов мозга, обработанных с помощью функциональной МРТ, но воспроизведению таким способом поддавались только изображения ограниченного круга. Теперь же разработанная программа преобразовывает сигналы мозга в числовые значения, на основе которых уже обученный искусственный интеллект воссоздает изображения[12].

В то же время российская ***Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники*** (далее — Концепция)[13], разработанная в целях определения основных подходов к трансформации системы нормативного регулирования в Российской Федерации для обеспечения возможности создания и применения таких технологий в различных сферах экономики с соблюдением прав граждан и обеспечением безопасности личности, общества и государства, исходит из того, что для развития технологий ИИ и робототехники необходимо создание регуляторной среды, комфортной для безопасного развития и внедрения указанных технологий, основанной на балансе интересов человека, общества, государства, компаний — разработчиков систем ИИ и робототехники, а также потребителей их товаров, работ, услуг.

К технологиям, основанным на использовании искусственного интеллекта, Концепцией (п. 5) отнесены:

а) компьютерное зрение;

б) обработка естественного языка;

в) распознавание и синтез речи;

г) интеллектуальная поддержка принятия решений;

д) перспективные методы искусственного интеллекта.

Перспективными методами искусственного интеллекта признаются:

а) автономное решение различных задач;

б) автоматический дизайн физических объектов;

в) автоматическое машинное обучение;

г) алгоритмы решения задач на основе данных с частичной разметкой и (или) незначительных объемов данных;

д) обработка информации на основе новых типов вычислительных систем;

е) интерпретируемая обработка данных;

ж) другие методы.

В Концепции отмечается, что повышение степени автономности систем ИИ и робототехники, снижение контроля человека за процессом их применения, не полностью прозрачный процесс принятия решений создают общественный запрос на регуляторные ограничения применения систем ИИ и робототехники. В настоящее время в мире отсутствуют единые подходы к регулированию технологий ИИ и робототехники, что связано с наличием ряда проблем, не имеющих однозначного решения.

В Концепции формулируется ***российская правовая модель регулирования искусственного интеллекта*** в соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 г., которая предусматривает следующие основные направления создания комплексной системы регулирования общественных отношений, возникающих в связи с развитием и внедрением технологий ИИ:

[10] Собрание законодательства РФ. 2023. № 45. Ст. 8035.

[11] URL: https://nauka.tass.ru/nauka/19185825?ysclid=lq7qhbicfb382166577

[12] URL: https://nauka.tass.ru/nauka/19556253

[13] Утв. Распоряжением Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ. 2020. № 35. Ст. 5593.

а) обеспечение благоприятных правовых условий (в том числе посредством создания экспериментального правового режима) для доступа к данным, преимущественно обезличенным, включая данные, собираемые государственными органами и медицинскими организациями;

б) обеспечение особых условий (режимов) для доступа к данным, включая персональные, в целях проведения научных исследований, создания технологий ИИ и разработки технологических решений на их основе;

в) создание правовых условий и установление процедур упрощенного тестирования и внедрения технологических решений, разработанных на основе ИИ, а также делегирования информационным системам, функционирующим на основе ИИ, возможности принятия отдельных решений (за исключением решений, которые могут ущемлять права и законные интересы граждан), в том числе при исполнении государственными органами государственных функций (за исключением функций, направленных на обеспечение безопасности населения и государства);

г) устранение административных барьеров при экспорте продукции (работ, услуг) гражданского назначения, созданной на основе ИИ;

д) создание единых систем стандартизации и оценки соответствия технологических решений, разработанных на основе ИИ, развитие международного сотрудничества Российской Федерации по вопросам стандартизации и обеспечение возможности сертификации продукции (работ, услуг), созданной на основе ИИ;

е) стимулирование привлечения инвестиций посредством совершенствования механизмов совместного участия инвесторов и государства в проектах, связанных с разработкой технологий ИИ, а также предоставления целевой финансовой поддержки организациям, осуществляющим деятельность по развитию и внедрению технологий ИИ (при условии, что внедрение таких технологий повлечет за собой существенные позитивные эффекты для отраслей экономики Российской Федерации);

ж) разработка этических правил взаимодействия человека с ИИ.

Такие направления должны стать основными ориентирами при создании комплексной системы регулирования общественных отношений, возникающих в связи с развитием и внедрением технологий ИИ и робототехники.

В Концепции предусматривается, что с учетом экономической и социальной значимости применения технологий ИИ и робототехники в различных сферах их разработка и эксплуатация не должны ограничиваться регуляторными мерами, за исключением случаев, связанных с высоким риском причинения вреда жизни и здоровью граждан. Не допускается также применение технологий ИИ и робототехники, представляющих явную угрозу обороне страны и безопасности государства.

Для выработки конкретных регуляторных решений требуется использовать риск-ориентированный подход, основанный на оценке размера потенциального вреда указанным ценностям с учетом вероятности его наступления по сравнению с потенциальным положительным эффектом от внедрения технологий ИИ и робототехники, необходимости принятия мер по минимизации соответствующих рисков.

Сам факт использования систем ИИ и робототехники не должен являться основанием для установления регуляторных ограничений.

Следует поддерживать развитие регулирования, вырабатываемого и приводимого в исполнение силами участников рынка (саморегулирование), включая принятие и использование документов национальной системы стандартизации, кодексов (сводов) этических правил и иных документов саморегулируемых организаций, а также иных инструментов.

Учитывая принципиальную сложность регулируемой сферы правоотношений, для выработки режима регулирования технологий ИИ и робототехники требуется активное вовлечение представителей компаний — разработчиков систем ИИ и робототехники, научно-исследовательских организаций в процесс экспертной проработки соответствующих нормативных правовых актов. В дальнейшем может также потребоваться уточнение отдельных норм законодательства в целях нормативного правового регулирования новых видов правоотношений.

В российском законодательстве также предусмотрены специальные экспериментальные правовые режимы регулирования ИИ. Так, Федеральным законом от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»[14] предусмотрена возможность установления специального регулирования в целях создания необходимых условий для разработки и внедрения технологий ИИ в городе Москве, а также последующего возможного использования результатов применения ИИ.

Важным вопросом является финансовое стимулирования разработок ИИ, в т. ч. в целях предоставления субсидии из федерального бюджета на поддержку разработки и коммерциализации новых технологий пилотных проектов апробации технологий ИИ в приоритетных отраслях установлены критерии соответствия технологии ИИ[15]. В частности, финансирование предоставляется, если проект удовлетворяет критерию базовой технологии проекта, а его мероприятия предусматривают создание, и (или) развитие, и (или) внедрение

[14] Собрание законодательства РФ. 2020. № 17. Ст. 2701.

[15] Приказ Минэкономразвития России от 29.06.2021 № 392 «Об утверждении критериев определения принадлежности проектов к проектам в сфере искусственного интеллекта». URL: http://pravo.gov.ru, 29.07.2021.

не менее чем одной из технологий ИИ, а также если его мероприятия направлены на решение технологических задач, установленных перечнем технологических задач, на реализацию которых может быть направлен проект в сфере ИИ, приведенным в приложении к настоящим Критериям.

Для целей определения соответствия проекта критерию базовой технологии к перспективным методам ИИ относятся автономная работа физических машин (робототехника) и обработка информации на основе новых типов специализированных вычислительных систем для задач ИИ.

В то же время необходимо учитывать, что безопасность, надежность и устойчивость применения современных технологий, особенно ИИ, ставится во главу угла регулирования этой сферы, в т. ч. в сфере сбора и обработки информации.

Учитывая существенный объем информации, доступный для потребления человеку, размещаемый в социальных сетях и иных площадках в Интернете, для упрощения его получения используются «рекомендательные алгоритмы», которые предлагают пользователю контент на основе его интересов и предпочтений. Однако подобные технологии не всегда добросовестно используются владельцами социальных сетей и иных информационных ресурсов. Так, под видом рекомендации пользователю может быть умышленно представлена информация, вводящая его в заблуждение или нарушающая законы Российской Федерации (распространение «фейковых» новостей, скрытая реклама и т. п.)[16].

В связи с этим был принят и с 1 октября 2023 года вступил в силу Федеральный закон от 31.07.2023 № 408-ФЗ «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации»[17], который устанавливает новые требования для владельцев сайтов в сети Интернет и мобильных приложений (за исключением операторов государственных информационных систем, государственные органы и органы местного самоуправления), применяющие технологии предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети Интернет («рекомендательные технологии»). Владелец такого сайта или приложения обязан не допускать применения рекомендательных технологий, которые нарушают права и законные интересы граждан и организаций, а также применения их в целях предоставления информации с нарушением законодательства Российской Федерации. Обязательно также размещение на сайте или в приложении правил применения рекомендательных технологий, которые должны включать в себя описание процессов и методов сбора, систематизации, анализа сведений, относящихся к предпочтениям пользователей сети Интернет, способов осуществления таких процессов и методов, перечень сведений, относящихся к предпочтениям пользователей сети Интернет, которые используются для предоставления информации с применением рекомендательных технологий, а также источники получения таких сведений. В случае установления факта неисполнения владельцем информационного ресурса, на котором применяются рекомендательные технологии, указанных обязанностей, ресурс может быть заблокирован Роскомнадзором.

Актуальное регулирование искусственного интеллекта в США

В марте 2023 г. Президент США утвердил новую редакцию Национальной стратегии в области кибербезопасности[18], которая определяет, что защита критически важной инфраструктуры США стала приоритетом национальной безопасности. Инициатива направлена на то, чтобы переложить часть бремени снижения рисков кибербезопасности с конечных пользователей и операторов критически важной инфраструктуры на предприятия частного сектора, которые лучше всего расположены для достижения значимых успехов в области безопасности и отказоустойчивости. В Стратегии также подчеркивается необходимость изменения стимулов в пользу долгосрочных инвестиций частного сектора. Стратегия построена на пяти основных задачах:

1) защита критически важной инфраструктуры;

2) выявление и уничтожение субъектов угроз;

3) формирование рыночных механизмов повышения безопасности и устойчивости;

4) инвестиции в устойчивое будущее;

5) налаживание международных партнерских отношений для достижения общих целей.

Каждый компонент содержит конкретные стратегические цели, разработанные на основе предыдущих программ, и направляющие усилия по реализации государственных структур и организаций частного сектора.

Стратегия сформулировала новую волну регулирования, которая направлена на внедрение новой парадигмы регулирования кибербезопасности в секторах критически важной инфраструктуры путем перехода от добровольных руководящих принципов к обязательным кибернетическим правилам, которые, как признается в Стратегии, потребуют определенных законодательных действий. Движущей силой этой инициативы является требование более целенаправленного, более скоординированного и более обеспеченного ресурсами подхода к киберзащите.

В Стратегии также признаются повышенные риски в нынешнюю эпоху глобальной цифровизации и углубления цифровой зависимости, ускоряемого появлением новых технологий. Стремительный технологический

[16] Разъяснение Прокуратуры Московской области от 16.11.2023 «Упорядочено применение рекомендательных технологий на сайтах в Интернете». URL: https://epp.genproc.gov.ru/web/proc_50, 16.11.2023.

[17] Собрание законодательства РФ. 2023. № 32 (Часть I). Ст. 6140.

[18] URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

прогресс также вынуждает секторы критически важной инфраструктуры бороться с рисками конвергенции информационных технологий и операционных технологических систем, которые должны проектироваться и защищаться совершенно разными способами. Сложная геополитическая обстановка усугубляет эти риски, поскольку число киберугроз для критически важной инфраструктуры, спонсируемых государством, растет. Хотя конкретные способы реализации Стратегии не определены, оперативная реализация целей будет иметь ключевое значение в развивающемся мире, где угрозы могут опережать регулирование и законотворчество. Администрация Байдена сослалась на некоторые всеобъемлющие принципы в дополнение к обязательным нормативным актам, например, продуманная безопасность как основной бизнес-принцип, оперативная доступность, позволяющая избежать системных сбоев, содействие гармонии нормотворчества в разных юрисдикциях.

Введен новый вид страхования — киберстрахование как относительно новый вид страхования, который покрывает различные виды ответственности или прямые убытки от событий, связанных с электронной деятельностью и системами, а также предполагающий партнерство между правительством и страховой отраслью для поддержки системам кибербезопасности коммерческих организаций в соответствии с национальными целями.

При всех ее преимуществах и перспективных инициативах анализ и реализация Стратегии сопряжены с некоторыми трудностями, включая формулирование и реализацию требований отчетности для частных компаний, столкнувшимся с киберинцидентами. Федеральное правительство установило меры для улучшения национальной кибербезопасности и возможностей перед лицом усиливающихся угроз кибербезопасности. Среди них — рекомендации Агентства кибербезопасности и инфраструктурной безопасности (входит в состав Министерства внутренней безопасности США) по спецификации программного обеспечения и обновлению межотраслевых показателей кибербезопасности, предлагаемые требования Комиссии по ценным бумагам и биржам США в отношении рисков кибербезопасности, меморандум Агентства по охране окружающей среды США в отношении систем общественного водоснабжения и распространение директив Управления транспортной безопасности, ориентированных на безопасность трубопроводов, на авиационный и железнодорожный секторы.

Кроме того, владельцам и операторам критически важной инфраструктуры предписано предпринять ряд ключевых мер, включая:

- участие в разработке официальных требований и стандартов образование регулирующих органов имеет решающее значение;
- координация деятельности внутренних IT и кадровых структур безопасности, комплаенса и юридическими подразделениями;
- использование рекомендаций, стандартов, лучших практик и непрерывное обучение для укрепления кибербезопасности.

Вместе с тем обращает на себя внимание откровенно агрессивный характер документа, который, в частности, легитимизирует наступательные кибероперации в качестве превентивной или ответной меры для подавления хакерских группировок и иных киберсил в информационном пространстве третьих стран. Этот подход в целом укладывается в логику известных американских концепций «постоянного воздействия» и «наступательной обороны», продвигаемых Агентством национальной безопасности и киберкомандованием Вооруженных сил США. Наглядным примером является ставка на проведение экстерриториальных расследований киберпреступлений. На это нацелена не ратифицированная Россией так называемая Будапештская конвенция. Она призвана легитимизировать право США без уведомления властей других стран вторгаться в их информационное пространство для сбора «цифровых улик»[19]. Характерно, что международные аналитические исследования[20] подтверждают доминирование наступательных методов в стратегиях кибербезопасности таких государств, как США, Великобритания и Украина.

30 октября 2023 г. президент Байден издал новый Указ о безопасном и заслуживающим доверия искусственном интеллекте *(Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence)*[21], который устанавливает новые стандарты безопасности ИИ, предусматривает комплекс практических мер и поручений госорганам по реализации конкретной политики для решения проблемных вопросов в сфере национальной безопасности, защиты данных, трудовых отношений и социального здравоохранения. Указ предусматривает обязанность компаний — разработчиков самых мощных систем ИИ сообщать результаты испытаний по безопасности ИИ и другую важную информацию правительству США. В соответствии с Законом об оборонном производстве Указ требует от компаний — разработчиков базовых моделей ИИ, потенциально представляющих серьезную угрозу национальной безопасности, национальной экономической безопасности или национальному общественному здравоохранению, уведомлять федеральное правительство при обучении модели ИИ о результатах всех пентестов (red-team) на оценку кибербезопасности модели ИИ до того, как компании обнародуют эти результаты.

---

[19] Интервью заместителя секретаря Совета безопасности РФ О. Храмова «Российской газете» 11 октября 2023 года. URL: http://www.scrf.gov.ru/news/allnews/3573/

[20] Стратегии кибербезопасности. Аналитический отчет, InfoWatch, 2022. URL: https://www.infowatch.ru/analytics/analitika/strategii-kiberbezopasnosti

[21] URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

Этот указ включает более сотни конкретных директивных указаний, касающихся безопасности ИИ, более чем двадцати федеральным агентствам, ставя перед ними задачи по реализации конкретной политики для решения проблемных областей, таких как национальная безопасность, защита данных, предвзятость на рабочем месте и общественное здравоохранение. Он также налагает требования на частные компании, разрабатывающие мощные системы ИИ, которые могут представлять угрозу национальной безопасности или общественному здоровью, требуя от них делиться результатами и методами испытаний на безопасность и другой важной информацией с правительством США. Большинство директив, изданных президентом Байденом в соответствии с Исполнительным указом, должны быть выполнены в течение 2024 г.

Правовое регулирование искусственного интеллекта в КНР

За последние несколько лет Китай добился значительных успехов в своих усилиях стать технологической сверхдержавой, постоянно прилагая усилия для утверждения себя в качестве ведущего мирового производителя ИС.

Страна превратилась из экономики с низкой заработной платой в высокотехнологичную державу. Фактически, по данным Всемирной организации интеллектуальной собственности (ВОИС), на Китай пришлось 46,8% всех патентных заявок по всему миру в 2023 году[22] , что свидетельствует о его стремлении избавиться от своего прошлого имиджа.

13 июля 2023 года правительство Китая опубликовало правила по генеративному искусственному интеллекту, Временные меры по управлению службами генеративного искусственного интеллекта (далее — Временные меры ГАИ)[23], которые вступили в силу 15 августа 2023 года. Целью Временных мер ГАИ является регулирование генеративного ИИ, который в первую очередь предназначен для создания контента, и они являются последним дополнением к формирующейся системе регулирования искусственного интеллекта в КНР, которая уже включает ряд специфичных для ИИ и местных законов.

Китайское правительство с самого начала начало поддерживать свою индустрию ИИ на национальном уровне. В 13-м пятилетнем плане Пекина (2016—2020) ИИ определен как ключевой для достижения целей экономического роста. В 2017 года китайское правительство представило свое вйдение развития ИИ в Китае, опубликовав свой план развития ИИ следующего поколения. В Плане представлена комплексная стратегия Пекина по сосредоточению ИИ в усилиях Китая по социально-экономическому развитию — индустрия ИИ, которая сделает Китай мировым лидером в области ИИ к 2030 году.

Со временем в рамках этих более широких стратегий в Китае на различных уровнях были собраны воедино различные законы об ИИ. На региональном уровне первый провинциальный закон Китая о разработке ИИ вступил в силу 1 октября 2020 года с принятием Шанхайских правил содействия развитию ИИ индустрии, которые направлены на продвижение индустрии ИИ на муниципальном уровне в Шанхае. Вскоре после этого правительство Шэньчжэня приняло аналогичный закон, Положение о продвижении индустрии искусственного интеллекта в Особой экономической зоне Шэньчжэня, который вступил в силу 1 ноября 2022 года.

Пекин также начал закладывать основу для конкретного решения проблемы генеративных систем ИИ. Положения об управлении алгоритмическими рекомендациями информационной службы Интернета («Положения об алгоритмических рекомендациях»), которые устанавливают структуру управления для регулирования систем рекомендаций, вступили в силу 1 марта 2022 года. Кроме того, правительство КНР выпустило целевые правила для генеративного ИИ через Положения об управлении глубоким синтезом интернет-сервиса («Положения о глубоком синтезе»), которые вступили в силу 10 января 2023 года и применяются к результатам глубокой подделки с помощью технологии ИИ. Временные меры ГАИ основаны на Положениях о глубоком синтезе, предоставляя более конкретные правила и принудительные меры конкретно для генеративного ИИ.

Вместе с Положениями об алгоритмических рекомендациях и Положениями о глубоком синтезе Временные меры ГАИ составляют основную правовую основу для соблюдения нормативных требований и надзора за ИИ индустрией в Китае.

Временные меры ГАИ отличаются от других законов тем, что конкретно регулируют использование генеративной технологии ИИ, определяемой как «модели и связанные с ними технологии, которые обладают способностью генерировать контент, такой как текст, изображения, аудио и видео», для предоставления услуг по генерации контента населению на материковой части КНР. По сравнению с положениями Deep Synthesis, генеративные технологии ИИ, подпадающие под временные меры GAI, охватывают нечто бóльшее, чем генеративные технологии, основанные на алгоритмах, и могут синтезировать технологии, включая также модели и системы, основанные на правилах.

Временные меры ГАИ применяются к поставщикам генеративных услуг ИИ, определяемым как организации и частные лица, которые используют генеративные технологии ИИ для предоставления генеративных услуг ИИ, включая предоставление этих услуг через интерфейсы прикладного программирования (API). Указано также, что «пользователи» генеративных услуг ИИ определяются как организации и от-

[22] IP Facts and Figures, WIPO, 2023. URL: https://www.wipo.int/en/ipfactsandfigures/patents

[23] URL: http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm

дельные лица, которые используют генеративные услуги ИИ для создания контента. Временные меры ГАИ охватывают предоставление генеративных услуг ИИ населению косвенно посредством деловых соглашений. Однако учреждения, которые разрабатывают и применяют генеративную технологию ИИ, но не предоставляют генеративные услуги ИИ населению, освобождаются от ответственности. Кроме того, Временные меры ГАИ устанавливают экстерриториальную сферу действия, уточняя, что они применяются к предоставлению услуг населению на материковой территории КНР, потенциально распространяя их применение на частных лиц и организации за пределами Китая, которые предоставляют генеративные услуги ИИ лицам в КНР. Этот нюанс дополняется другим положением, в котором говорится, что несоблюдение Временных мер ГАИ и других законов поставщиками генеративного ИИ за пределами КНР приведет к уведомлению соответствующих учреждений о принятии технических мер и других необходимых мер для борьбы с ними. Примечательно, что Временные меры ГАИ имеют значительно меньшую сферу применения по сравнению с ранним проектом, который также применялся бы к исследованиям, разработке и использованию продуктов с генеративными функциями ИИ. Однако эта формулировка не упоминается во Временных мерах ГАИ.

Временные меры ГАИ устанавливают ряд общих требований к предоставлению и использованию генеративных услуг ИИ:

- Уважение общественной морали и нравственности Китая и отстаивание «основных социалистических ценностей».
- «Эффективные меры» должны применяться во время разработки алгоритмов, отбора обучающих данных, генерации и оптимизации моделей, предоставления услуг и других процессов для предотвращения дискриминации по таким факторам, как раса, этническая принадлежность, религиозные убеждения, национальность, регион, пол, возраст, профессия или состояние здоровья.
- Уважение прав интеллектуальной собственности, коммерческой этики и защита коммерческой тайны, а также запрет на использование в целях монополии и недобросовестной конкуренции.
- Уважение законных прав и интересов других лиц и запрет на создание угрозы физическому и психологическому благополучию других лиц или нарушение их прав и интересов, включая их имидж, репутацию, честь, неприкосновенность частной жизни и личную информацию.
- Необходимо использовать эффективные меры для повышения прозрачности, точности и надежности услуг генеративного ИИ.

Кроме того, предоставление и использование генеративных услуг ИИ не должно генерировать контент, который может привести к следующим негативным результатам:

- подстрекательство к подрыву национального суверенитета или свержению социалистической системы;
- создание угрозы национальной безопасности и интересам или нанесение ущерба имиджу китайской нации;
- разжигание сепаратизма или подрыв национального единства и социальной стабильности;
- пропаганда терроризма или экстремизма;
- пропаганда этнической ненависти и дискриминации, насилия и непристойностей, а также фальшивой и вредной информации.

Временные меры ГАИ предъявляют более конкретные эксплуатационные требования к поставщикам услуг генеративного ИИ, чем первая версия. Эти операционные требования касаются целого ряда вопросов, таких как разработка модели, управление данными, стандарты обслуживания и модерация контента, и включают следующее.

- Данные для обучения. Поставщики должны использовать данные и базовые модели из «законных источников» и применять «эффективные меры» для повышения качества, достоверности, точности, объективности и разнообразия данных для обучения.
- Права на неприкосновенность частной жизни. Провайдеры несут ответственность как обработчики личной информации и должны получать согласие при использовании личной информации, если не применяется исключение, и соблюдать правила конфиденциальности, включая сбор и минимизацию данных, хранение данных и индивидуальные права в отношении доступа, исправления и удаления.
- Маркировка данных. Поставщики услуг должны установить четкие, конкретные и практичные правила маркировки, которые соответствуют требованиям Временных мер ГАИ в процессе исследований и разработок для генеративного ИИ.
- Модерация контента и маркировка. Провайдеры несут ответственность как производители информационного онлайн-контента и должны маркировать созданный контент в соответствии с требованиями Положений Deep Synthesis, оперативно устранять «незаконный контент» с помощью «эффективных мер», таких как прекращение генерации или передачи контента, его удаление и исправление с помощью обучения оптимизации модели, а также сообщать о проблеме в соответствующие органы.
- Взаимодействие с пользователями и жалобы. Провайдеры должны заключать соглашения об обслуживании с пользователями для уточнения прав и обязанностей, использовать «эффективные меры» для предотвращения зависимости или чрезмерного увлечения несовершеннолетними пользователями и разработать механизмы рассмотрения жалоб пользователей.

– Оценка безопасности. Поставщики генеративных услуг ИИ, обладающих «свойствами общественного мнения» или «способностью к социальной мобилизации», должны проводить оценки безопасности и соблюдать требования к алгоритмической подаче документов в соответствии с Положениями алгоритмических рекомендаций.

За нарушения соответствующие регулирующие органы должны налагать штрафы в соответствии с применимыми законами и административными постановлениями, включая законы КНР о кибербезопасности, о безопасности данных, о защите личной информации и о научно-техническом прогрессе, если нарушение не касается определенной области, соответствующие регулирующие органы могут выносить предупреждения, публиковать критические замечания и предписывать поставщикам соблюдать требования законодательства. При «серьезных обстоятельствах» или в случае отказа в таких распоряжениях власти могут распорядиться о приостановке работы услуг генеративного ИИ. Однако, в отличие от черновой версии, которая предусматривала бы денежные штрафы в размере от 10 000 до 100 000 юаней за нарушения, Временные меры ГАИ не предусматривают денежных штрафов.

Поставщики услуг также должны быть готовы сотрудничать с инспекциями регулирующих органов, имея возможность объяснить обучающие данные, включая их источники, модели, типы, правила маркировки и алгоритмы, а также предоставить любую другую необходимую помощь. Органы власти, участвующие в регулировании генеративного ИИ, также обязаны сохранять конфиденциальность конфиденциальных данных, таких как коммерческая тайна и личная информация, полученная в ходе выполнения своих обязанностей, и не должны разглашать или незаконно передавать эти данные третьим лицам.

Современное законодательство ЕС в сфере ИИ

В марте 2024 г. Европарламент принял самый амбициозный закон, регулирующий ИИ, текст которого согласовали все страны ЕС. Закон об ИИ ЕС (*EU Artificial Intelligence Act*)[24] (далее — Закон) занимает более 200 страниц и применяется как к поставщикам, так и к пользователям технологий, основанных на ИИ, в частном и государственном секторах. Как и в других законодательных актах ЕС, связанных с данными, Закон также применяется экстерриториально к компаниям и организациям за пределами ЕС.

Закон определяет ***систему искусственного интеллекта*** (в англоязычной версии) как *машинную систему, предназначенную для работы с различными уровнями автономии, которая может как проявлять адаптивность после развертывания и которая для достижения явных или неявных целей выводит из получаемых входных данных, так и генерировать выходные данные, такие как прогнозы, контент, рекомендации или решения, которые могут влиять на физическую или виртуальную среду.* Это соответствует определению Организации экономического сотрудничества и развития (ОЭСР).

Согласно определению, ключевой характеристикой, отличающей системы ИИ от традиционного программного обеспечения, является то, что система ИИ делает выводы на основе входных данных (*«выводит из получаемых входных данных и генерирует выходные данные»*). Это призвано подчеркнуть способность систем ИИ создавать модели и (или) алгоритмы из входных данных. Первоначально Закон предполагал исключить системы, основанные на правилах, которые определяются исключительно физическими лицами, для выполнения автоматических процессов, из сферы действия Закона об ИИ. По определению, возможности систем ИИ должны выходить за рамки базовых операций по обработке данных и пониматься скорее как обучение, рассуждения или моделирование. Определение в Законе также предполагает, что системы ИИ *«предназначены для работы с различными уровнями автономии»*. Соответственно, должна быть определенная степень независимости действий системы от людей. Другими словами, система должна быть способна работать без вмешательства человека. Характеристика *«адаптивности»* предназначена для выражения способности системы ИИ (продолжать) изучать саму себя и, таким образом, постоянно меняться.

Технологии ИИ, которые представляют явный риск для основных прав человека (биометрические системы категоризации на основе чувствительных характеристик, социальный рейтинг или ИИ, используемый для манипулирования поведением человека), будут запрещены в Европе. Системы ИИ, считающиеся высокорискованными, используемые, например, в критической инфраструктуре, образовании, здравоохранении, правоохранительных органах, управлении границами или на выборах, должны будут соответствовать строгим требованиям.

Закон определяет *модели искусственного интеллекта общего назначения (GPAI)*. Среди прочих требований, разработчики моделей GPAI должны создавать и обновлять техническую документацию модели, включающую определенные минимальные элементы, а также предоставлять подробную информацию и документацию поставщикам, которые интегрируют эти модели в свои системы ИИ, соблюдать законы об авторском праве ЕС и публиковать «достаточно» подробное изложение контента, используемого для обучения модели GPAI.

Отдельно выделяются *модели искусственного интеллекта общего назначения с системным риском*. Закон налагает повышенные требования на поставщиков моделей GPAI «с системными рисками», которые включают требования к проведению оценки модели, включая состязательное тестирование модели, для оценки и смягчения возможных системных рисков на уровне

[24] URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

ЕС, а также обеспечения адекватной защиты в области кибербезопасности.

Предусмотрены *исключения из систем искусственного интеллекта высокого риска.* Наиболее жесткие требования Закона распространяются на системы ИИ «высокого риска». В Законе определены два типа систем ИИ, представляющих высокий риск:

(1) системы ИИ, предназначенные для использования в качестве продуктов (или компонентов безопасности продуктов), на которые распространяется специальное законодательство ЕС, перечисленное в приложении II к Закону, и

(2) системы ИИ, используемые для целей, перечисленных в Приложении III к Закону, таких как определенное использование систем удаленной биометрической идентификации и определенных систем ИИ, используемых для правоохранительных органов.

Есть и исключение из этого требования: если система искусственного интеллекта, подпадающая под действие Приложения III, «не представляет значительного риска нанесения вреда здоровью, безопасности или основным правам физических лиц», поставщик может задокументировать это и на этом основании исключить систему из обязательств Закона в отношении таких систем. Органы по надзору за рынком уполномочены оценивать системы, которые, по их мнению, были неправильно классифицированы, и предписывать меры по исправлению положения. Провайдеры также будут подвергнуты штрафам, если орган по надзору за рынком установит, что провайдер неправильно классифицировал свою систему ИИ, чтобы обойти применение обязательств к системам ИИ высокого риска.

Организации, внедряющие системы, которые регулируются публичным правом, частные операторы, предоставляющие государственные услуги, и (за некоторыми исключениями) операторы, внедряющие системы ИИ высокого риска для оценки кредитоспособности физического лица, установления кредитного рейтинга физического лица или оценки рисков и цен в связи со страхованием жизни или здоровья физического лица, должны выполнить оценку воздействия на основные права перед внедрением системы ИИ высокого риска. Эти требования включают:

- процессы разработчика, в которых система ИИ высокого риска будет использоваться в соответствии с ее назначением;
- описание периода времени и частоты, с которой предполагается использовать систему ИИ высокого риска;
- категории физических лиц и групп, которые могут пострадать от его использования в конкретном контексте;
- конкретные риски причинения вреда, которые могут повлиять на категории лиц или группу лиц, определенных как подверженные влиянию, принимая во внимание информацию, предоставленную поставщиком услуг в соответствии с его обязательствами по прозрачности в соответствии со статьей 13;
- описание реализации мер по надзору за персоналом в соответствии с инструкциями по использованию; и
- меры, которые необходимо предпринять в случае реализации этих рисков, включая их механизмы внутреннего управления и подачи жалоб.

Закон предусматривает требования по прозрачности для поставщиков и пользователей определенных систем ИИ и моделей GPAI, включая

(1) поставщиков систем ИИ и GPAI, генерирующих синтетический аудио-, графический, видео- или текстовый контент,

(2) разработчиков систем распознавания эмоций или биометрической категоризации,

(3) разработчиков систем ИИ, которые генерируют или манипулируют изображениями, аудио- или видеоконтентом, составляющими подделку, и

(4) разработчиков систем, которые генерируют или манипулируют текстом, опубликованным с целью подделки или для информирования общественности по вопросам, представляющим общественный интерес. Закон налагает дополнительные обязательства по обеспечению прозрачности на лиц, внедряющих определенные системы ИИ высокого риска. В некоторых случаях контент должен быть помечен машиночитаемым способом, чтобы его можно было идентифицировать как искусственно созданный или подвергнутый манипуляциям. Закон об ИИ предусматривает исключения при некоторых обстоятельствах, в т. ч. когда система ИИ используется в художественных, сатирических, творческих или аналогичных целях.

Быстрорастущие модели ИИ общего назначения (GPAI) также должны будут соответствовать обязательствам по прозрачности и правилам ЕС об авторском праве, в то время как к наиболее мощным моделям будут предъявляться дополнительные требования безопасности. Учитывая возрастающие трудности с распознаванием искусственных или подделанных аудиовизуальных носителей («фейков») в Интернете, такой контент должен иметь четкую маркировку.

В Законе установлены и другие ограничения: согласованы гарантии в отношении ИИ общего назначения; предусмотрено ограничение использования систем биометрической идентификации правоохранительными органами; установлен запрет на социальный скоринг и ИИ, используемый для манипулирования уязвимостями пользователей или эксплуатации их уязвимостей; предусмотрено право потребителей подавать жалобы и получать содержательные объяснения.

Штрафы за нарушение Закона варьируются от 35 млн евро (7% от годового оборота) до 7,5 млн евро (1,5% от оборота).

Закон вступит в силу через 20 дней после его публикации в Официальном журнале ЕС и, как правило, начнет применяться к организациям через 2 года после

его вступления в силу, за некоторыми исключениями: запреты на определенные методы использования ИИ вступят в силу через 6 месяцев, правила в отношении моделей GPAI вступят в силу через 12 месяцев (за исключением моделей GPAI, которые были размещены на рынке до этой даты; они вступят в силу еще через 24 месяца), а также правила, применимые к ИИ высокого риска, включенному в Приложение II: системы вступят в силу через 36 месяцев.

Признавая потенциальную угрозы правам граждан, создаваемых определенными приложениями ИИ, **Закон запрещает**:

- системы биометрической категоризации, использующие конфиденциальные характеристики (например, политические, религиозные, философские убеждения, сексуальная ориентация, раса);
- нецелевое извлечение изображений лиц из Интернета или видеозаписей с камер видеонаблюдения для создания баз данных распознавания лиц;
- распознавание эмоций на рабочем месте и в учебных заведениях;
- социальный рейтинг, основанный на социальном поведении или личных характеристиках;
- системы ИИ, которые манипулируют поведением людей в обход их свободной воли;
- системы ИИ, использующие уязвимости людей (из-за их возраста, инвалидности, социального или экономического положения).

Строгие ограничения налагаются в отношении *использования систем биометрической идентификации* (RBI) в общедоступных местах в целях обеспечения правопорядка при условии предварительного разрешения суда и для строго определенных списков преступлений. Они должны использоваться строго при целенаправленном поиске лица, осужденного или подозреваемого в совершении серьезного преступления. RBI в режиме реального времени должны соответствовать строгим условиям, и их использование будет ограничено по времени и местоположению в следующих целях:

- целенаправленные поиски жертв (похищение, торговля людьми, сексуальная эксплуатация),
- предотвращение конкретной и существующей террористической угрозы или
- локализация или идентификация лица, подозреваемого в совершении одного из конкретных преступлений, упомянутых в постановлении (например, терроризм, торговля людьми, сексуальная эксплуатация, убийства, похищения людей, изнасилования, вооруженное ограбление, участие в преступной организации, экологические преступления).

Закон требует оценки воздействия на основные права, прежде чем система ИИ высокого риска будет выведена на рынок. Кроме того, для систем, которые (i) взаимодействуют с людьми, (ii) используются для обнаружения эмоций или определения связи с (социальными) категориями на основе биометрических данных или (iii) генерируют контент или манипулируют им («дипфейк»), обязательно информирование пользователей об их автоматизированном характере, например, для информирования физических лиц, когда они подвергаются воздействию системы распознавания эмоций, или для эффективного нанесения водяных знаков на контент, созданный ИИ, в соответствии с техническими стандартами. Граждане будут иметь право подавать жалобы на системы ИИ и получать разъяснения по поводу решений, полученных при помощи систем ИИ высокого риска, которые затрагивают их права.

С учетом широкого круга задач, которые могут выполнять системы ИИ, и быстрого расширения его возможностей Законом предусмотрено, что системы ИИ общего назначения (GPAI) и модели GPAI, на которых они основаны, должны будут соответствовать требованиям прозрачности, первоначально предложенным парламентом. Они включают составление технической документации, соблюдение законодательства ЕС об авторском праве и распространение подробных сведений о контенте, используемом для обучения.

Для высокоэффективных моделей GPAI с системным риском участникам парламентских переговоров удалось добиться более строгих обязательств. Если эти модели соответствуют определенным критериям, они должны будут проводить оценку моделей, оценивать системные риски и снижать их, проводить состязательное тестирование, сообщать Комиссии о серьезных инцидентах, обеспечивать кибербезопасность и сообщать об их энергоэффективности. Депутаты Европарламента также настаивали на том, что до публикации гармонизированных стандартов ЕС GPAI с системным риском могут полагаться на кодексы практики для соблюдения регламента.

Кроме того, Закон включает список запрещенных практик для тех систем ИИ, использование которых считается неприемлемым как противоречащее ценностям ЕС, таких как когнитивно-поведенческие манипуляции или обман, использование уязвимостей, нецелевое извлечение изображений лиц из Интернета или видеозаписей с камер видеонаблюдения, классификация социального поведения, социальный рейтинг, биометрическая категоризация для вывода конфиденциальных данных, таких как сексуальная ориентация или религиозные убеждения, и некоторые случаи превентивного полицейского воздействия на отдельных лиц.

Законом создан специальный надзорный орган ЕС — Офис искусственного интеллекта при Еврокомиссии, который будет осуществлять надзор за самыми передовыми моделями ИИ, способствовать внедрению стандартов и практик тестирования, а также обеспечивать соблюдение общих правил во всех государствах-членах. Научная группа независимых экспертов будет консультировать Офис искусственного интеллекта по моделям GPAI. Совет по искусственному интеллекту будет действовать как координационная платформа и консультативный орган при Комиссии, будет также

создан консультативный форум для заинтересованных сторон, таких как представители промышленности, малого и среднего бизнеса, стартапы, гражданское общество и научные круги, для предоставления технической экспертизы Совету по искусственному интеллекту.

Поставщики автономных систем ИИ высокого риска и определенные пользователи систем ИИ высокого риска, которые являются государственными организациями, должны зарегистрироваться в базе данных ЕС по системам ИИ высокого риска.

Поставщики систем ИИ обязаны также соблюдать обязательства по мониторингу и отчетности в отношении пострыночного мониторинга и отчетности, а также расследования инцидентов и неисправностей, связанных с ИИ.

Заключение

С быстрым распространением технологий ИИ он стал значительной силой, которая меняет методы работы предприятий и взаимодействия людей с машинами в различных производственных сферах, включая:

- *автоматизацию* повторяющихся задач, повышение эффективности и уменьшение количества человеческих ошибок;
- быстрый *анализ обширных наборов данных* ИИ для принятия решений на их основе;
- *персонализация* и адаптация опыта пользователей с представлением рекомендаций по контенту или спросу на продукцию на основе индивидуальных предпочтений и потребительского поведения;
- *стимулирование инноваций*, способствуя разработке новых продуктов, услуг и иных решений, которые ранее были недостижимы, за счет автоматизации тестирования или генерации новых формул;
- *улучшение принятия управленческих решений* — ИИ может предоставлять информацию и прогнозы, помогающие лицам, принимающим решения, в различных областях, от диагностики здравоохранения до финансового прогнозирования;
- *повышение безопасности* на базе систем ИИ благодаря таким функциям, как автономное вождение и прогнозируемое техническое обслуживание и др.;
- *создание нового контента* — алгоритмы ИИ используются для создания контента в литературе, искусстве и других областях человеческой деятельности. Например, Creative Commons использует генеративный ИИ для создания контента способами, которые поддерживают открытый доступ к образованию и творческим разработкам.

Литература

1. Карцхия А.А., Макаренко Г.И. Правовые горизонты технологий искусственного интеллекта: национальный и международный аспект // Вопросы кибербезопасности. 2024. № 1. С. 2—14. DOI: 10/21681/2311-3456-2024-1-2-14 .
2. Мохов А.А. Демографическая безопасность и ее правовое обеспечение // Юрист. 2023. № 6. С. 62—67.
3. Amatova N.E., Social consequences of the implementation of NBIC-technologies: risks and expectations. Univ. Soc. Sci. 9 (8) (2014). URL: http://7universum.com/en/social/archive/item/1549 (accessed 22 Jan 2020).
4. S. Klaus, C. Jung, Legal Aspects of «Artificial Intelligence» (AI). Information and Communication Technology Newsletter, 2019, No. 10. URL: https://www.swlegal.com/media/filer_public/ce/e4/cee498cc-910d-4af8-a020-5b4063662b35/sw_newsletter_october_i_english.pdf
5. Haskins A., Arora S., Nilawar U. Impact of Artificial Intelligence on Indian Real Estate: Transformation Ahead. Collier's Radar Property Research (India). 05.10.2017. 13 p. P. 4.
6. Capabilities and risks from frontier AI, AI Safety Summit, 2023. URL: https://assets.publishing.service.gov.uk/media/65395abae6c968000daa9b25/frontier-ai-capabilities-risks-report.pdf
7. Frontier AI Regulation: Managing Emerging Risks to Public Safety, November 7, 2023. URL: https://arxiv.org/abs/2307.03718
8. The Paradox of Artificial Intelligence in the Legal Industry: Both Treasure Trove and Trojan Horse? The Perils of Deepfakes, Wolters Kluwer, 2021. URL: http://arbitrationblog.kluwerarbitration.com
9. Марков А.С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1 (53). С. 2—12.
10. Карцхия А.А. LegalTech как основа цифровой правовой экосистемы / LegalTech в сфере предпринимательской деятельности : монография (отв. ред. И.В. Ершова, О.В. Сушкова). М. : Проспект, 2023. С. 25—33.
11. Карцхия А.А., Макаренко Г.И., Макаренко Д.Г. Правовые перспективы технологий искусственного интеллекта // Безопасные информационные технологии : сборник трудов Двенадцатой международной научно-технической конференции МВТУ им Н. Э. Баумана. 2023. С. 154—161.
12. Крутских А.В., Зиновьева Е.С. Международная информационная безопасность: подходы России. М. : МГИМО МИД России, 2021. С. 6.

LEGAL PROBLEMS IN USING ARTIFICIAL INTELLIGENCE IN RUSSIA

Aleksandr Kartskhiia, *Dr.Sc. (Law), Professor at the Gubkin Russian State University of Oil and Gas, Moscow, Russian Federation.*
E-mail: arhz50@mail.ru

Grigory Makarenko, *Senior Researcher at the Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation, Moscow, Russian Federation.*
E-mail: t7920518@yandex.ru

Keywords: *neural networks, machine learning, artificial intelligence security, legal basis.*

Abstract

Purpose of the work: showing the legal problems in the development and implementation of artificial intelligence (AI) in Russian reality.

Study findings. A review of the topic for Russia, USA, and China was carried out. Although Russia is at the 10th place in the world in terms of using AI, its implementation is progressing rapidly. The authors wanted to show (and to warn) that the implementation of what is now called AI was under development already in the USSR. Back in the 1970, one of the authors of this paper set up a computer-aided design laboratory for automated design of 13-layer printed circuit boards for on-board computers (used in aerospace systems). By 1980 there were already hundreds of units in the USSR, in different fields of technology and industry, engaged in the automation of design and management. The development of automation in Russia stopped due to the stop of the development of industry in the country: passenger aircraft industry, machine tool industry, instrumentation engineering were nearly completely destroyed, and it is only in the recent years that the country came to its senses and started to discuss the development of its industry. However, as we can see from the example of aircraft industry, even passenger aircraft that were tested long ago and already produced before still can't reach the production stage.

There stand not only artificial obstacles such as negligent officials in the way of implementation of AI but also objective circumstances such as a lack of a legal basis.

Practical importance: this paper is a follow-up to a paper by the authors "Legal horizons of artificial intelligence technologies: national and international aspects" (the Cybersecurity Issues journal, No. 1 for 2024) and may be useful in developing the said legal basis.

References

1. Kartskhiia A.A., Makarenko G.I. Pravovye gorizonty tekhnologii iskusstvennogo intellekta: natsional'nyi i mezhdunarodnyi aspekt. Voprosy kiberbezopasnosti, 2024, No. 1, pp. 2–14. DOI: 10/21681/2311-3456-2024-1-2-14 .
2. Mokhov A.A. Demograficheskaia bezopasnost' i ee pravovoe obespechenie. Iurist, 2023, No. 6, pp. 62–67.
3. Amatova N.E., Social consequences of the implementation of NBIC-technologies: risks and expectations. Univ. Soc. Sci. 9 (8) (2014). URL: http://7universum.com/en/social/archive/item/1549 (accessed 22 Jan 2020).
4. S. Klaus, C. Jung, Legal Aspects of "Artificial Intelligence" (AI). Information and Communication Technology Newsletter, 2019, No. 10. URL: https://www.swlegal.com/media/filer_public/ce/e4/cee498cc-910d-4af8-a020-5b4063662b35/sw_newsletter_october_i_english.pdf
5. Haskins A., Arora S., Nilawar U. Impact of Artificial Intelligence on Indian Real Estate: Transformation Ahead. Collier's Radar Property Research (India). 05.10.2017. 13 p. P. 4.
6. Capabilities and risks from frontier AI, AI Safety Summit, 2023. URL: https://assets.publishing.service.gov.uk/media/65395abae6c968000daa9b25/frontier-ai-capabilities-risks-report.pdf
7. Frontier AI Regulation: Managing Emerging Risks to Public Safety, November 7, 2023. URL: https://arxiv.org/abs/2307.03718
8. The Paradox of Artificial Intelligence in the Legal Industry: Both Treasure Trove and Trojan Horse? The Perils of Deepfakes, Wolters Kluwer, 2021. URL: http://arbitrationblog.kluwerarbitration.com

9. Markov A.S. Vazhnaia vekha v bezopasnosti otkrytogo programmnogo obespecheniia. Voprosy kiberbezopasnosti, 2023, No. 1 (53), pp. 2–12.
10. Kartskhiia A.A. LegalTech kak osnova tsifrovoi pravovoi ekosistemy. LegalTech v sfere predprinimatel'skoi deiatel'nosti : monografiia (otv. red. I.V. Ershova, O.V. Sushkova). M. : Prospekt, 2023, pp. 25–33.
11. Kartskhiia A.A., Makarenko G.I., Makarenko D.G. Pravovye perspektivy tekhnologii iskusstvennogo intellekta. Bezopasnye informatsionnye tekhnologii : sbornik trudov Dvenadtsatoi mezhdunarodnoi nauchno-tekhnicheskoi konferentsii MVTU im N. E. Baumana, 2023, pp. 154–161.
12. Krutskikh A.V., Zinov'eva E.S. Mezhdunarodnaia informatsionnaia bezopasnost': podkhody Rossii. M. : MGIMO MID Rossii, 2021, p. 6.

СТАНОВЛЕНИЕ ИНСТИТУТА ИНФОРМИРОВАННОГО СОГЛАСИЯ В МЕДИЦИНЕ

Запольский С.В.[1], Пестрикова А.А.[2]

Ключевые слова: *информированное согласие, информация, договор на оказание медицинских услуг, медицинское вмешательство, диагностика, диагноз, права пациента, медицинские риски, модель.*

Аннотация

Цель работы: анализ российской и иностранной практики по информированию пациентов медицинских учреждений о рисках и возможных последствиях медицинского вмешательства.

Методы исследования: системный и исторический анализ, специальные методы: сравнительно-правовой, формально-юридический и социологический.

Результаты исследования: научно обоснованные предложения по совершенствованию информационно-правового обеспечения информирования пациентов медицинских учреждений, конкретизации законодательства по добровольному информированному согласию, предотвращению конфликтов и судебных споров в этой области.

DOI:10.21681/1994-1404-2024-1-20-28

Здоровье человека — естественное благо, данное человеку в силу его рождения и социального статуса. За пределами особых ситуаций, предусмотренных законом, ни государство, ни та или иная организация, в том числе медицинская, без согласия человека не вправе осуществлять вмешательство в ход физиологических процессов в его организм, изменять, дополнять, совершенствовать органы и части тела. Свободное распоряжение своим телом для любого человека — *правовой принцип* [8] прав человека и конституционный институт бóльшей части развитых стран.

Авторы уже обращались к проблематике института *информированного согласия* на медицинское вмешательство. Предыдущая статья [6] была посвящена юридической защите прав и законных интересов пациента при *генетических* исследованиях и последующих медицинских вмешательствах.

Правовой режим получения, хранения, использования, передачи и утилизации биологических материалов человека формирует высокий «юридический стандарт», но не исчерпывает, по мнению авторов, всего объема проблематики, поскольку не менее актуальными вопросами остаются информированное согласие в сфере хирургии, применения лечебных препаратов и технических устройств, психиатрии, педиатрической помощи детям, трансплантации органов и многих других сферах медицины.

В настоящей статье анализируются отечественные и иностранные юридические подходы к информированному *добровольному согласию* [2—4] на медицинское вмешательство в целом, в том числе и со стороны субъективного правопонимания пациента медицинского учреждения, а также в аспекте прокурорского надзора и отраслевого *контроля* за законностью в сфере медицины. Здесь мы наблюдаем идеальное пересечение *информационно-правовой* [7] и *правоохранительной* функций осуществления публичной власти в целях защиты прав человека.

Институт информированного согласия, занимающий достаточно значимое место в правовом регулировании отношений в области медицины, предусмотрен в статье 20 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации»[3].

Важно заметить, что условие об информированном согласии действует не только при поступлении гражданина, нуждающегося в лечении, в стационарное медицинское учреждение, но и при получении первичной медико-санитарной помощи, при выборе врача и медицинской организации на срок их выбора. Следовательно, при любом продолжении или изменении лечения или обследований (экспертиз), смены медицинской организации или лечащего врача должно оформляться новое информированное согласие.

Закон исходит также из того, что при даче информированного согласия в целом на весь курс медицинских

[3] Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // СПС «КонсультантПлюс».

[1] ***Запольский Сергей Васильевич,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, главный научный сотрудник Института государства и права Российской академии наук, г. Москва, Российская Федерация.*

E-mail: zpmoscow@mail.ru

[2] ***Пестрикова Анастасия Александровна,*** *кандидат юридических наук, доцент кафедры конституционного и административного права Тольяттинского государственного университета, г. Тольятти, Российская Федерация.*

E-mail: anastasia801@yandex.ru

мероприятий гражданин вправе отказаться от определенных видов медицинского вмешательства. Из этого вытекает, что *пертинентная информация* [8], предоставляемая в целях получения согласия, должна содержать развернутую картину предстоящих медицинских мероприятий, включая персональное обеспечение (данные о враче или врачах), инструментальное и техническое обеспечение (оборудование), фармакологическую сторону, а также важнейшие *риски*, могущие возникнуть.

Как инструмент правового регулирования этот институт предполагает высокую степень информированности пациента о существе, характере, целях, предполагаемых последствиях, в том числе и негативных, оказания профессиональной медицинской помощи в лицензированном медицинском учреждении.

В этой области действуют также подзаконные акты: Приказ Минздрава от 23.04.2012 № 390-н «Об утверждении перечня определенных видов медицинских вмешательств, на которые граждане дают информированное добровольное согласие при выборе врача и медицинской организации для получения первичной медико-санитарной помощи» и Приказ Минздрава РФ от 12.11.2021 № 1051н «Об утверждении порядка дачи информированного добровольного согласия на медицинское вмешательство и отказа от медицинского вмешательства, формы информационного добровольного согласия на медицинское вмешательство и формы отказа от медицинского вмешательства».

Институт информированного добровольного согласия вошел в медицинскую практику и широко применяется во всех без исключения медицинских учреждениях. Вместе с тем наблюдается достаточно высокая степень формализма при получении информированного добровольного согласия; соответствующий документ заранее истребуется у пациента, нередко в порядке действий среднего медицинского персонала, когда тактика и методика оказания медицинской помощи еще не проведена, а соответствующие исследования не завершены до конца. В целом степень информированности пациента о характере медицинской помощи оставляет желать лучшего.

В юридическом ключе информированное добровольное согласие пока не служит тем правовым инструментом, который мог бы предотвратить конфликты, возникающие в ходе оказания медицинской помощи, оценки их последствий и выяснения причин возникновения негативных последствий оказания медицинской помощи. Информированное добровольное согласие охватывает только собственно медицинское вмешательство и почти не касается *психологических* [11] и морально-этических последствий этого вмешательства.

В связи с вышеизложенным представляет большой интерес история становления института информированного добровольного согласия в других странах, которые начали применять, хотя бы даже в зачаточном режиме, этот институт ранее, нежели в России. Речь идет о медицинском вмешательстве, построенном на коммерческих началах, где отношения между пациентом и медицинским учреждением так или иначе первоначально строились на договорных, эквивалентно-возмездных отношениях, и где согласие пациента на ту или иную медицинскую помощь было определенной гарантией от возможного предъявления впоследствии претензий и исков имущественного характера.

Доктрина информированного согласия в сфере здравоохранения связана с профессиональной этикой и правовыми аспектами. Во второй половине XX в. информированное согласие стало частью правовых систем [7]; ранее клиническая информация оставалась «делом врача» в силу клятвы Гиппократа и основывалась на патерналистских отношениях между врачом и пациентом. На протяжении бóльшей части истории медицины специалисты по медицинской этике были больше озабочены тем, чтобы наилучшим образом скрыть потенциально вызывающую стресс информацию от пациентов, чтобы уменьшить вред и тревогу.

Информированное согласие является не только этической и моральной концепцией, но и правовой концепцией, разработанной в судах, начиная с серии дел в 1950-х гг. Одно из первых судебных разбирательств, касающихся признания права пациента на получение информации и самоопределения в отношении своего здоровья, было дело «Шлёндорф против Нью-Йоркской больницы» в 1914 г. Согласно решению, каждый человек в зрелом возрасте и здравом уме имеет право определять, что ему делать со своим телом, а хирург, который проводит операцию без согласия своего пациента, совершает нападение, за которое он несет ответственность в виде возмещения ущерба[4].

Впервые информированное согласие появилось в решении Калифорнийского апелляционного суда 22 октября 1957 г. в деле о злоупотреблении служебным положением — «Салго против Леланда». Суд пришел к выводу, что врач нарушает свой долг перед пациентом и подвергает себя ответственности, если он умалчивает о каких-либо фактах, которые необходимы пациенту для обоснования разумного согласия последнего на предлагаемое лечение. При обсуждении рисков необходимо проявлять определенную степень осмотрительности в соответствии с полным раскрытием фактов, необходимых для получения информированного согласия [16].

В течение следующих 15 лет суды усовершенствовали *концепцию* [8] *информированного согласия*, установив стандарты и определив исключения, когда информированное согласие не требуется. Ряд судебных дел в 1970-х гг., в частности, дело «Кентбери против Спенса»[5], заложили основы стандарта раскрытия информации, ориентированные на пациента. В этом деле в 1972 г. пациент перенес операцию по поводу грыжи межпозвоночного диска и в результате был парализован. Он по-

[4] URL: https://casetext.com/case/schloendorff-v-new-york-hospital

[5] URL: https://www.psychologicalscience.org/observer/diversity-trust-informed-consent

дал в суд на врача, утверждая, что его не предупредили о рисках, связанных с операцией. Врач утверждал, что риск был небольшим, и его раскрытие могло спровоцировать ненужное беспокойство.

Апелляционный суд округа Колумбия вынес решение в пользу пациента, указав, что врач был обязан сообщить пациенту о всех рисках, даже незначительных, характере вмешательства, вероятных результатах, альтернативных формах лечения, серьезных рисках и осложнениях, которые могут возникнуть в процессе вмешательства. Это решение резко изменило стандартную практику раскрытия информации от прежнего подхода, ориентированного на врача, когда соответствующий объем информации, необходимый для получения информированного согласия определялся тем, что другие врачи сделали бы в аналогичных обстоятельствах. Новый подход ориентирован на пациента, при котором соответствующий объем информации определяется объемом информации, который потребуется разумному пациенту для осознанного принятия решения.

Здесь важно рассмотреть вопрос о видах взаимодействия врача и пациента, поскольку это является основой понимания и дальнейшего формирования института добровольного информированного согласия. Различают несколько моделей.

Патерналистская модель — врач принимает все решения (это первая исторически сложившаяся модель).

Информационная — врач обязан предоставить пациенту все существующие сведения, а пациент самостоятельно осуществляет выбор лечения.

Интерпретационная — врач обязан информировать пациента о состоянии здоровья, вариантах лечения, достоинствах и недостатках. Врач играет активную роль, прилагая все усилия, чтобы выбор пациента пал на более разумное решение[6].

Модель сотрудничества — врач вовлекает пациента в диалог, разъясняет ему все возможные варианты лечения и рекомендует один из них, являющейся, по мнению специалиста, наиболее подходящим.

Концепция автономии пациента заключается в том, что он имеет возможность выбора метода лечения на основе детального обсуждения с врачом всех альтернативных вариантов и определения оптимального[7], отвечающего позициям обеих сторон — как врача, так и пациента.

Для формирования *концепции информированного согласия* важно рассмотреть практику раскрытия информации пациентам и важность учитывать все обстоятельства и критерии. Ведь в процессе развития науки и биотехнологий неизменно меняется *правосознание* [7]. Именно поэтому сохраняется актуальность изучения правового регулирования медицинского обслуживания за рубежом, проведение сравнительно-правовых исследований. Здоровье в западных правопорядках все чаще рассматривается как товар, а пациент — потребитель услуг здравоохранения, способный осуществлять осознанный выбор при условии предоставления ему необходимой информации [17]. Пациент по общему правилу не обязан подвергаться какому-либо лечению. Чтобы дать согласие на проведение процедуры, он должен быть проинформирован о своем состоянии и прогнозе развития заболевания, о сущности, назначении и характере процедуры, связанных с ней болевых ощущениях и неудобствах, вероятности благоприятного исхода, возможных рисках, альтернативах и последствиях отказа от лечения, знать имена и квалификацию медицинского персонала [1].

Определение круга необходимых сведений может исходить из объективных и субъективных критериев. *Объективные* критерии: критерии среднего разумного врача (определяемые стандартами профессионального поведения) и среднего разумного пациента (какие сведения желает получить обычный разумный человек, чтобы согласиться или отказаться от медицинского вмешательства)[8].

В этой части интересно рассмотреть некоторые сложившиеся в практике прецеденты, которые постепенно формировали концепцию информированного согласия в медицинской практике и сейчас могут быть полезными для формирования национального правового регулирования общественных отношений по поводу биологического материала человека. Например, *правило Болама* (дело *"Bolam v Friern 1957"*): врач не виноват в халатности, если он действует в соответствии с практикой, общепринятой медиками-профессионалами в данной области. При разрешении спора судья обращается к экспертам, и если хоть одно мнение противоположное, то иск о халатности не удовлетворяется[9]. В 2015 г. по делу *"Montgomery v Lanarkshire Health Board"* (Шотландия) было высказано мнение, что объем раскрытия информации пациенту и обсуждение рисков не определяется медицинским образованием или опытом. Применение правила Болама может привести к санкционированию различий в практике, которые могут быть связаны не с различием школ медицинской науки, а с различием взглядов врачей на степень уважения своих пациентов. Необходимо разграничивать правовой характер обстоятельств, когда, например, врач не применяет достижения медицины, и совсем другой вопрос, когда пациент игнорирует инструкцию к лекарству. Обязан ли врач обсуждать риски, если пациент дает понять, что предпочитает это не обсуждать? Врач обязан раскрыть информацию своему пациенту, если исходя из разумных соображений врача это может нанести вред здоровью или жизни, именно поэтому

[6] Esmanuel E. Four models of the physician-patient relationship // JAMA. Chicago. 1992. Vol 267. № 2. P. 2221–2225.

[7] Savulescu J. Choosing the best: against the paternalistic practice guidelines // Bioethics. Oxford. 1996. Vol. 10 № 4. P. 323–335.

[8] Ross I.A. Practice guidelines, patient interests and risky procedures. Bioethics. Oxford. 1996. Vol. 10. № 4. P. 311–322.

[9] McManus F., Russel E. Delict: A Comprehensive Guide to the Law. Chichester: Wiley, 1998. XLIII, 646 p.

применять правило Болама всегда и безапелляционно нецелесообразно[10]. Так, истица, страдающая диабетом, отказалась от кесарева сечения, хотя были показания и врач не уведомил ее о риске 9—10% для плода. Родился ребенок с инвалидностью из-за дистоции плеча, был предъявлен иск о халатности. Иск был отклонен на основании того, что истица отказалась бы от кесарева сечения даже при информировании о риске.

В 1998 г. в Англии рассматривалось дело о применении принудительных мер в отношении дееспособной пациентки, используя конструкцию временной недееспособности. Женщина согласилась на проведение операции кесарева сечение, поскольку риск гибели ребенка при естественных родах составлял 50%. Но когда выяснился факт необходимости применения анестезии, женщина отказалась от инъекционной анестезии (из-за патологической боязни игл), а потом и от анестезии через маску (из-за боязни задохнуться). Больница обратилась в суд за разрешением применить *принудительное* медицинское вмешательство. Суд дал согласие, опираясь на то обстоятельство, что пациентка согласна на операцию, но под воздействием фобии не способна адекватно оценить информацию и, кроме того, продолжительность негативного влияния на нее при использовании анестезии и в случае рождения ребенка-инвалида или его смерти — существенное обстоятельство для разрешения принудительного медицинского вмешательства [1].

Примером *критерия разумности* пациента служит дело *"Rogers v Whitaker 1992"*. Пациентка в результате травмы ослепла на один глаз, врач предложил операцию на нем для улучшения внешнего вида. В результате пациентка ослепла на оба глаза, так как был риск развития симпатической офтальмии (составлявший 1 случай на 14 тысяч). Было представлено два экспертных заключения и в одном указывалось, что не предупреждение о таком малом проценте риска — это обычная врачебная практика. И по правилу Болама иск должен был быть отклонен, но иск удовлетворили, исходя их критерия, что, зная о риске, пациент мог отказаться от операции [1].

На международном уровне этот принцип вытекал из Нюрнбергского процесса 1946 г., который констатировал обязательное согласие заинтересованной стороны на прохождение лечения и протоколы научных исследований [14]. В *Хартии основных прав*[11] Европейского союза закреплено, что в области медицины и биологии необходимо свободное и информированное согласие заинтересованного лица в порядке, установленным законом.

Стоит обратить внимание на Правила, которые были приняты в мае 2016 г. Международным обществом исследования стволовых клеток (*International society for stem cell research, ISSCR*), в которых также подробно указываются основания и порядок получения информированного согласия. Как указывается в Правилах, важно понимать, что необходимо получать информированное согласие на предоставление всех биоматериалов, в том числе и от доноров гамет. Информированное согласие должно быть получено в момент предполагаемой передачи любых биоматериалов исследовательской группе или если биоматериалы собираются и хранятся для использования в будущих научных исследованиях. Согласие должно быть получено и в отношении биоматериала, который собран в результате проведения медицинских процедур, если он будет в дальнейшем использоваться для проведения исследований.

В 2020 г. Европейский союз разработал программу «Горизонт»[12], которая включает в себя руководство по проведению исследований с биологическим материалом человека. Участие в любых исследованиях и экспериментах должно быть полностью добровольным, и необходимо получить и четко оформить документ, подтверждающий получение предварительного информированного согласия участников.

Что касается Российской Федерации, то сто́ит заметить, что институт информированного согласия не сформирован в должной мере, нет единства формирования и получения согласия, единых стандартов и практики. Это является недопустимым с точки зрения защиты субъектов правоотношений, возникающих по поводу биологического материала человека. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» в статье 20 определяет порядок получения добровольного информированного согласия на медицинское вмешательство и отказ от него. Указано, что согласие дается на основании предоставленной медицинским работником в доступной форме *полной* информации о целях, методах оказания медицинской помощи, связанном с ними риске, возможных вариантах медицинского вмешательства, его последствиях, а также результатах оказания медицинской помощи.

В отношении несовершеннолетних и недееспособных согласие дают родители или иные законные представители. При отказе от медицинского вмешательства в доступной форме должны быть разъяснены возможные последствия отказа. Медицинская организация в этом случае вправе обратиться в суд для защиты прав несовершеннолетнего (недееспособного) в случае, если медицинское вмешательство необходимо для спасения его жизни. Информированное согласие хранится в медицинской документации лица. Форма информированного согласия утверждена Приказом Министерства здравоохранения РФ от 20 декабря 2012 г. № 1177н «Об утверждении порядка дачи информиро-

[10] McManus F., Russel E. Delict: A Comprehensive Guide to the Law. Chichester: Wiley, 1998. XLIII, 646 p.

[11] Хартия стала обязательной со вступлением в силу Лиссабонского договора в декабре 2009 г. // Wayback Machine (Internet Archive).

[12] URL: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf (дата обращения: 02.02.2021).

ванного добровольного согласия на медицинское вмешательство и отказа от медицинского вмешательства в отношении определенных видов медицинских вмешательств, форм информированного добровольного согласия на медицинское вмешательства и форм отказа от медицинского вмешательства».

Таким образом, в сфере здравоохранения информированное согласие стало актом как юридической, так и этико-деонтологической значимости. Тема информированного согласия становится все более актуальной в связи с *цифровизацией* [9] системы здравоохранения, использованием телемедицины, биомедицинских исследований, паллиативной помощи, генетических исследований и редактированием генома человека [12, 15].

Очевидно, что информационные стандарты различаются в правовых системах разных стран. В настоящее время наиболее распространены две модели:

- *«разумный практикующий врач»* — объем информации должен соответствовать тому, что в данной ситуации мог бы предоставить разумный врач;
- *«стандарт разумного пациента»* — уровень информации должен касаться того, что стандартный пациент хотел бы знать о своем состоянии.

Согласно правовой медицинской доктрине, информированное согласие должно быть личным, свободным, текущим, выраженным, осознанным, обязательным, конкретным, отзываемым в любое время.

Сложным аспектом остается отношение к информированному согласию как к необходимой бюрократической процедуре, часто выраженной просто в подписании необходимых документов и бланков: нельзя быть точно уверенным, что пациент понял или получил весь объем информации и действительно выразил свое согласие. Сто́ит также обратить внимание на то, что в зависимости от пациента встречается две типичных поведенческих реакции на получение полной информации. *Первая* — пациент полностью знает о всех последствиях медицинского вмешательства, у него вырабатывается *психологический иммунитет* [14], что положительно влияет на протекание болезни и в результате — более быстрое выздоровление. *Вторая* реакция — эффект ноцебо (от лат *nocebo* — «я повредить»), когда пациент, зная о возможных побочных реакциях и эффектах, «находит» их и в результате возможно ухудшение клинического состояния.

Достижения в генетических и геномных исследованиях еще более усугубили традиционное понимание концепции информированного согласия. За 20 с лишним лет с тех пор, как генетическое тестирование стало обычным явлением в клиниках и исследовательских учреждениях, врачи, исследователи и специалисты по этике пытались применить стандарты информированного согласия, используемые в медицине в более широком смысле, и обнаружили, что некоторые из них особенно сложны в использовании в генетическом контексте.

Например, информированное согласие требует способности принимать решения, но если вмешательство связано с генетическим отклонением, затрагивающим умственную деятельность (умственная отсталость, аутизм, нейродеградация и др.), то получить информированное согласие не представляется возможным. Способность принимать решения может варьироваться в зависимости от уровня риска, связанного с вмешательством или генетическим тестом — более рискованные вмешательства требуют более высокого уровня способности принимать решения и понимания информации.

Добровольность может быть поставлена под сомнение, так как члены семьи, для которых генетическое тестирование также может иметь последствия, могут оказать влияние на субъекта информированного согласия.

Исследования в области генетики и геномики требуют доступа к ДНК человека из любых образцов биологического материала человека. Биологический материал можно хранить и использовать в нескольких исследованиях, и даже анонимизированный биологический материал можно идентифицировать в любое время. Кроме популярных сейчас во многих странах национальных биобанков образцов биологического материала населения, многие исследователи и фармацевтические компании собирают и хранят биологические образцы, клинические данные и генетическую информацию, создаются клеточные линии, которые позволяют практически бесконечно использовать биологические материалы и данные ДНК. При этом хранение и широкий обмен биологическими образцами делает невозможным описать подробно или даже предположить все будущие исследования, которые могут быть проведены, возможные риски, связанные с исследованиями, в момент сбора образцов. Вероятно, получение информированного согласия должно быть разделено на два или более этапов: при сборе биологического материала, при использовании биологического материала в последующих исследованиях.

В любом случае необходимо рассматривать получение информированного согласия *как процесс*, а не как акт подписания необходимых документов и бланков. В процессе общения врач или исследователь передает информацию о медицинском вмешательстве или научном исследовании, включая связанные с этим риски и преимущества, пациент передает информацию о своих целях, ожиданиях, приоритетах, связанных со здоровьем, предпочтениях и опасениях. Клиницист должен оценить понимание пациентом передаваемой информации, задавая вопросы или используя обучающие методики.

В идеале процесс получения информированного согласия — это длительная процедура, так как пациент может по-разному реагировать на полученную информацию в разное время; необходимо в целом оценивать понимание и полное согласие на медицинское вмешательство или научное исследование. Документ, подтверждающий информированное согласие, является лишь одним из аспектов процесса информированного согласия. Цель документа о согласии — запротоколи-

ровать, что вся этически соответствующая информация обсуждалась в присутствии всех заинтересованных сторон. При этом стоит учитывать, что последние исследования показали: наиболее *достоверным* [7, 8] является информированное согласие, полученное не в результате однократного действия, а когда все участвующие стороны ведут длительный, динамичный диалог на всех этапах взаимодействия [13]. Таким образом, исследователи должны обеспечить широкие возможности для доноров биоматериалов, чтобы обсудить их участие на всех стадиях исследований. Исследователи при получении информированного согласия должны раскрывать информацию о всех возможных долгосрочных рисках.

Наиболее значимые риски, связанные с клиническим генетическим тестированием, являются социальными и психологическими, например, стресс или тревога, связанные с предсимптомным знанием того, что может развиться генетическое заболевание, для которого не существует лечения в настоящее время, а кроме того, существует потенциальный риск стигмы (общее название кожных заболеваний) или дискриминации из-за результатов тестирования.

Секвенирование генома позволило быстро и недорого получить большой объем генетической информации, что привело к широкому внедрению панельного генетического тестирования и более широкому использованию экзомного и геномного секвенирования как в клинических, так и исследовательских целях.

Геномное секвенирование сопряжено с рядом проблем и рисков, которые носят, среди прочего, *психологический*, социальный и семейный характер, включая обнаружение неожиданных биологических отношений (кровное родство, неправильное определение отцовства и др.) [15]. Значительным преимуществом является возможность постановки диагноза или выявление нескольких диагнозов, которые имеют значение, что может помочь в методике лечения.

Проблемой получения информированного добровольного согласия в Российской Федерации является то, что информация часто предоставляется в устной форме, поскольку нет четкого алгоритма и требований закона о закреплении всей детальной информации о медицинском вмешательстве в информированном согласии. Поэтому оно остается формальной процедурой, которая выполняется медицинским персоналом часто и после оказания медицинской помощи, поэтому проверить объем и достоверность предоставленной пациенты информации часто невозможно. Как справедливо отмечает Ю.Д. Сергеев, «*недостатком* формы информированного согласия является его усредненность, не позволяющая учитывать индивидуальные особенности пациента»[13].

Вопрос о предварительном характере информированного согласия — дискуссионный: «*за какой период до начала медицинского вмешательства его можно и нужно давать, и на какой отрезок времени?*» [5]. Как предлагают некоторые авторы, российское законодательство должно давать ориентиры, так как точные временны́е периоды вряд ли могут быть установлены в части определения сроков получения согласия; поэтому необходимо учитывать масштабность и сложность медицинского вмешательства [10].

Одним из вариантов решения проблемы получения информированного согласия в генетических исследованиях может быть поэтапное или многоуровневое согласие. Поэтапное согласие носит длительный характер, раскрытие информации происходит постепенно по мере появления новых результатов, что облегчает решение проблемы нехватки времени и в то же время пациент не будет перегружен информацией и сможет принять решение более свободно и осознанно. Конечно, поэтапное согласие требует больше времени для всех участвующих субъектов, что также может быть решено с использованием *компьютерных технологий* и внедрения должности генетических консультантов. Очевидно, что врачам и исследователям важно использовать более индивидуальный и гибкий подход к информированному согласию, когда речь идет о генетических технологиях.

Исследования биологического материала человека могут привести к нарушениям прав человека, например, занесение генетической информации о человеке в одном государстве может привести к раскрытию этой информации в другом государстве. Раскрытие *генетической информации* может неправомерно использоваться при предоставлении страховки или при трудоустройстве.

Исследования генетической информации важны и нужны, но необходимо защитить права всех участвующих субъектов. Получение общественного доверия — элемент развития научного прогресса. Правовое регулирование необходимо для инкорпорации общественных и индивидуальных интересов, принятия четких стандартов и определений, не допускающих двойного толкования и понимания, возможностей для обхода закона и злоупотребления правом. Коммерциализация отношений, связанных с генетикой, влияет на их правовое регулирование и правовое сознание потребителей данной информации (граждан), создает сложности для правоприменительной практики.

Как можно предположить из вышеприведенного, совершенствование института добровольного информированного согласия на медицинское вмешательство, включая генетические исследования, охватывает широчайший круг проблем и направлений развития медицины как науки и как института гражданского общества; формализм и поверхностность использования этого института в течение длительного времени будет всё более и более вызывать социальные противодействия. Понимая проблему не только как медицинскую или научную, но и как *информационно-правовой* и социальный феномен, можно обозначить некоторые на-

[13] Сергеев Ю.Д. Медицинское право : учеб. комплекс: в 3 т. Т. 1. М. : ГЭОТАР-Медиа, 2008. 784 с. (С. 295).

правления совершенствования правового регулирования добровольного информированного согласия. В частности, следовало бы конкретизировать процедуру дачи такого согласия в аспекте состава участников, момента, с которого это согласие будет действительно информированным, а также добровольным. На наш взгляд, весьма неопределенные нормы регулируют осуществление медицинского вмешательства без получения согласия или при отсутствии возможности получить согласие, при этом должна быть исключена сама возможность обвинения медицинского или иного технического персонала (спасатели, полицейские, педагоги и др.) в недостаточной квалификации или умении оказания медицинской помощи.

Должна также быть продолжена работа по углублению *принципа ясности* информированного добровольного согласия: очевидно, врач при информировании пациента о существе медицинской помощи должен использовать термины и понятия, заведомо известные пациенту или могущие быть разъясненными дополнительно. Принцип ясности и понятности будет усилен в том случае, когда *технико-правовые регламенты* по осуществлению информированного согласия будут построены отдельно по различным видам медицинского вмешательства, поскольку генетические исследования имеют мало общего с хирургическим вмешательством, а последние — с психиатрией.

Несомненно одно: информированное добровольное согласие есть важнейший инструмент информационно-правового обеспечения охраны здоровья граждан нашей страны, повышения действенности медицинской помощи населению и развития медицинской науки.

Рецензент: ***Исаков Владимир Борисович,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, действительный государственный советник Российской Федерации 1 класса, заведующий кафедрой теории права и сравнительного правоведения Национального исследовательского университета «Высшая школа экономики», г. Москва, Российская Федерация.*
E-mail: visakov@hse.ru

Литература

1. Афанасьева Е.Г. Право на информированное согласие как основа юридического статуса пациента // Современное медицинское право в России и за рубежом : сб. науч. тр. / ИНИОН РАН. М. : ИНИОН, 2003. С. 138—156.
2. Беляева О.В. Добровольное информированное согласие на медицинское вмешательство в свете практики судов Российской Федерации и Европейского Суда по правам человека // Медицинское право: теория и практика. 2018. Т. 4. № 2 (8). С.13—20.
3. Гарипова И.И. Добровольное согласие граждан на медицинское вмешательство в аспекте гражданско-правовой деятельности // Медицинское право. 2016. № 2. С. 39—44.
4. Гоглова О.О. Добровольное информированное согласие с позиции норм биоэтики // Правовые вопросы в здравоохранении. 2011. № 3. С. 46—53.
5. Долинская Л.М. Согласие на медицинское вмешательство // Законы России: опыт, анализ, практика. 2015. № 1. С. 39—43.
6. Запольский С.В., Пестрикова А.А. Информированное согласие на медицинское вмешательство: правовой аспект // Правовая информатика. 2023. № 2. С. 6—13. DOI: 10.21681/1994-1404-2023-2-6-13 .
7. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
8. Ловцов Д.А. Информационная теория эргасистем. Тезаурус : монография. М. : Наука, 2005. 248. ISBN 5-02-033779-X.
9. Ловцов Д.А. Цифровая трансформация инфосферы правовых эргасистем и оценка защищенности привилегированной информации // Образовательное и правовое пространство цифрового мира: современность, перспективы и безопасность : монография. Краснодар: СКФ РГУП, 2023. С. 9—17. ISBN 978-5-907663-78-7.
10. Поваров Ю.С. Требования к согласию на проведение исследования, лечения или диагностики, связанных с геномом человека // Юридический вестник Самарского университета. Т. 5. № 2. 2019. С. 23—28.
11. Auguste E., Bowdring M., Kasparek S.W., McPhee J., Tabachnick A.R., Tung I., Galán C.A. Psychology's contributions to anti-Blackness in the United States within psychological research, criminal justice, and mental health // Perspectives on Psychological Science. 2023.
12. Fatumo S., Chikowore T., Choudhury A., Ayub M., Marin A.R., Kuchenbaecker K. A roadmap to increase diversity in genomic studies. Nature Medicine. 2022. No. 28. Pp. 243–250.
13. Flory J., Emanuel E. Interventions to improve research participants' understanding in informed consent for research: a systematic review. JAMA. 2004. 292. Pp. 1593–1601.
14. Guerra F., La Rosa P., Guerra F., Raimondi L., Marinozzi S., Miatto I., Vergati D., Ndokaj A., Gasperini N., Corridore D., et al. Risk Management for a Legally Valid Informed Consent. La Clin. Ter. 2021. P. 484–488. DOI: 10.7417/CT.2021.2361 .

15. Kim A. Diversity, Trust, and Informed Consent: Making Genetics Research Effective for All. Psychological science. 2023.
16. Matshabane O.P., Whitted C.G., Koehly L.M. Addressing diversity and inclusion challenges in global neuro-psychiatric and behavioral genomics research. Frontiers in Genetics. 2022. Article 1021649.
17. Robert D. Miller. History of The Use of the Term "Informed Consent" up to Salgo. University of Wisconsin. Madison. 2020.
18. Tuoby P. Children's consent to medical treatment. New Zealand Law. J. Wellington. 2001. Pp. 253–356.

FORMATION OF THE INSTITUTION OF INFORMED CONSENT IN HEALTHCARE

Sergei Zapol'skii, *Dr.Sc. (Law), Professor, Honoured Lawyer of the Russian Federation, Principal Researcher at the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.*
E-mail: zpmoscow@mail.ru

Anastasiia Pestrikova, *Ph.D. (Law), Associate Professor at the Department of Constitutional and Administrative Law of the Togliatti State University, Togliatti, Russian Federation.*
E-mail: anastasia801@yandex.ru

Keywords: *informed consent, information, contract for providing healthcare services, medical intervention, diagnosing, diagnosis, rights of the patient, healthcare risks, model.*

Abstract

Purpose of the work: analysing domestic and foreign practice of providing to patients of healthcare institutions information about the risks and possible consequences of medical interventions.

Methods used in the study: system and historical analysis, special methods, i.e. the comparative legal, formal legal, and sociological ones.

Study findings: research-based proposals for improving legal information support for providing information to patients of healthcare institutions, making legal regulations on voluntary informed consent more specific, and preventing conflicts and lawsuits in this field.

References

1. Afanas'eva E.G. Pravo na informirovannoe soglasie kak osnova iuridicheskogo statusa patsienta. Sovremennoe meditsinskoe pravo v Rossii i za rubezhom : sb. nauch. tr. INION RAN. M. : INION, 2003, pp. 138–156.
2. Beliaeva O.V. Dobrovol'noe informirovannoe soglasie na meditsinskoe vmeshatel'stvo v svete praktiki sudov Rossiiskoi Federatsii i Evropeiskogo Suda po pravam cheloveka. Meditsinskoe pravo: teoriia i praktika, 2018, t. 4, No. 2 (8). S.13–20.
3. Garipova I.I. Dobrovol'noe soglasie grazhdan na meditsinskoe vmeshatel'stvo v aspekte grazhdansko-pravovoi deiatel'nosti. Meditsinskoe pravo, 2016, No. 2, pp. 39–44.
4. Goglova O.O. Dobrovol'noe informirovannoe soglasie s pozitsii norm bioetiki. Pravovye voprosy v zdravookhranenii, 2011, No. 3, pp. 46–53.
5. Dolinskaia L.M. Soglasie na meditsinskoe vmeshatel'stvo. Zakony Rossii: opyt, analiz, praktika, 2015, No. 1, pp. 39–43.
6. Zapol'skii S.V., Pestrikova A.A. Informirovannoe soglasie na meditsinskoe vmeshatel'stvo: pravovoi aspekt. Pravovaia informatika, 2023, No. 2, pp. 6–13. DOI: 10.21681/1994-1404-2023-2-6-13 .
7. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 s. ISBN 978-5-93916-505-1.
8. Lovtsov D.A. Informatsionnaia teoriia ergasistem. Tezaurus : monografiia. M. : Nauka, 2005. 248. ISBN 5-02-033779-X.
9. Lovtsov D.A. Tsifrovaia transformatsiia infosfery pravovykh ergasistem i otsenka zashchishchennosti privilegirovannoi informatsii. Obrazovatel'noe i pravovoe prostranstvo tsifrovogo mira: sovremennost', perspektivy i bezopasnost' : monografiia. Krasnodar: SKF RGUP, 2023, pp. 9–17. ISBN 978-5-907663-78-7.
10. Povarov Iu.S. Trebovaniia k soglasiiu na provedenie issledovaniia, lecheniia ili diagnostiki, sviazannykh s genomom cheloveka. Iuridicheskii vestnik Samarskogo universiteta, t. 5, No. 2, 2019, pp. 23–28.

11. Auguste E., Bowdring M., Kasparek S.W., McPhee J., Tabachnick A.R., Tung I., Galán C.A. Psychology's contributions to anti-Blackness in the United States within psychological research, criminal justice, and mental health. Perspectives on Psychological Science. 2023.
12. Fatumo S., Chikowore T., Choudhury A., Ayub M., Marin A.R., Kuchenbaecker K. A roadmap to increase diversity in genomic studies. Nature Medicine. 2022. No. 28. Pp. 243–250.
13. Flory J., Emanuel E. Interventions to improve research participants' understanding in informed consent for research: a systematic review. JAMA. 2004. 292. Pp. 1593–1601.
14. Guerra F., La Rosa P., Guerra F., Raimondi L., Marinozzi S., Miatto I., Vergati D., Ndokaj A., Gasperini N., Corridore D., et al. Risk Management for a Legally Valid Informed Consent. La Clin. Ter. 2021. P. 484–488. DOI: 10.7417/CT.2021.2361 .
15. Kim A. Diversity, Trust, and Informed Consent: Making Genetics Research Effective for All. Psychological science. 2023.
16. Matshabane O.P., Whitted C.G., Koehly L.M. Addressing diversity and inclusion challenges in global neuro-psychiatric and behavioral genomics research. Frontiers in Genetics. 2022. Article 1021649.
17. Robert D. Miller. History of The Use of the Term "Informed Consent" up to Salgo. University of Wisconsin. Madison. 2020.
18. Tuoby P. Children's consent to medical treatment. New Zealand Law. J. Wellington. 2001. Pp. 253–356.

ГОСУДАРСТВЕННО-ПРАВОВЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ТЕНЕВОЙ ВНЕШНЕЙ ПОЛИТИКЕ НЕДРУЖЕСТВЕННЫХ СТРАН

Агишев Р.Г.[1]

Ключевые слова: *межгосударственные отношения, латентное противоборство, привлечение к ответственности, уголовная и административная ответственность.*

Аннотация

Цель работы: определить государственно-правовые подходы к противодействию скрытой вредоносной внешней политике иностранных государств.

Методы исследования: диалектика, разработанные на ее основе научные методы познания и системный подход.

Полученные результаты: показана система правовых мер, используемых государством в защите от угроз, исходящих от теневой внешней политики недружественных стран. Раскрыты возможности применения в этих целях уголовного и административного права. Отмечены пробелы в уголовном праве относительно проведения иностранцами и апатридами иной (помимо разведывательной) деятельности, направленной на нанесение ущерба безопасности Российской Федерации.

Научная новизна: исследовано состояние регулирования вопросов противодействия акциям и операциям скрытой внешней политики недружественных стран с позиции внутригосударственного права. Систематизированы правовые меры, применяемые Россией и некоторыми другими государствами в целях защиты от акций и операций, латентно проводимых недружественными странами. Выделены встречающиеся в этой сфере проблемы в Российской Федерации и внесены предложения по их решению.

EDN: IAPGIQ

Введение

События последних лет лишний раз показывают опасность внешних угроз, генерируемых недружественными странами, для суверенитета и могущества России. Наряду с открытыми конфликтами, данные угрозы реализуются также в сфере межгосударственных отношений латентного противоборства, которая менее изучена в научном плане по сравнению с официальными, публичными отношениями между странами мира. В целях реализации собственных национальных интересов недружественные страны прибегают к скрытным, теневым методам борьбы, широко используя подставные организации и подбирая проводников своей политики среди граждан Российской Федерации (далее — РФ). Справедливо расценивая деятельность последних как деструктивную по отношению к безопасности России, законодатель обозначил таких проводников политики недружественных государств термином «иностранные агенты». Какие меры противопоставлены нашим государством и некоторыми другими державами по отношению к внешним угрозам со стороны недружественных стран с точки зрения внутреннего законодательства? Ответ на этот вопрос постараемся представить в настоящей статье.

Результаты исследования

Деятельность недружественных стран по генерации угроз РФ точнее всего, по нашему мнению, отражает понятие теневой внешней политики [1, с. 228—283]. Эта деятельность охватывает тайные операции и акции иностранных спецслужб и организаций, подстрекательство граждан РФ к деструктивной деятельности, введение так называемых санкций, заключение дипломатических союзов, направленных против РФ, и т. д. Деструктивная деятельность может состоять из совокупности весьма разнородных деяний, ядро которых является уголовно наказуемым.

Для защиты от этих разнообразных угроз осуществляется политика государственной безопасности, которая воплощается в жизнь через систему общегосу-

[1] ***Агишев Ришат Габитович,*** *доктор юридических наук, профессор, академик АВН, профессор кафедры публичного и международно-правового обеспечения национальной безопасности РГУ нефти и газа имени И.М. Губкина, г. Москва, Российская Федерация.*

E-mail: agish.gubkin@gmail.com

дарственных мер борьбы с деятельностью иностранных спецслужб и организаций по применению теневой внешней политики. Система включает в себя правовые, научные, организационные, дипломатические, политические, экономические, военные, разведывательные, воспитательные, кадровые, информационно-пропагандистские меры [1, с. 357].

С точки зрения классификации отраслей права правовые меры противодействия теневой внешней политике состоят из конституционно-правовых, уголовно-правовых, уголовно-процессуальных, гражданско-правовых, гражданско-процессуальных, административно-правовых и др.

Уголовно-правовые и уголовно-процессуальные меры, осуществляемые компетентными органами страны, включают уголовное расследование дел о преступлениях, наносящих ущерб безопасности государства, рассмотрение этих дел в судах и исполнение определенных судом наказаний.

Вместе с тем следует отметить, что физические и юридические лица, принимающие участие в акциях и операциях теневой внешней политики иностранных государств, в ряде случаев могут быть привлечены к гражданско-правовой ответственности.

Гражданско-правовые меры действуют в рассматриваемой сфере в области международного частного права и призваны регулировать имущественные и прочие материальные отношения между юридическими и физическими лицами, часть из которых может оказаться в роли объектов иностранной теневой внешней политики, а другие — служить посредническими звеньями для совершения акций и операций субъектами теневой внешней политики иностранного государства. Данные меры направлены на судебное возмещение неправомерного нанесения ущерба юридическим и физическим лицам, представляющим РФ, через которые иностранные спецслужбы и организации пытаются достичь своих целей, нанося ущерб интересам страны.

Важную роль в деле противодействия теневой внешней политике иностранных государств играют административно-правовые меры, которые включают:

- меры, регулирующие порядок встреч и общения отечественных должностных лиц с иностранными гражданами[2];
- режимные меры охраны государственной границы[3];
- меры, регулирующие порядок открытия и деятельности представительств иностранных финансово-промышленных и коммерческих корпораций, СМИ и аккредитации их сотрудников, представительств иностранных религиозных организаций и т. п. в стране-объекте[4];
- меры, регулирующие порядок пребывания и передвижения иностранных граждан на территории страны[5]; меры, регулирующие порядок открытия, деятельности и ликвидации отечественных юридических лиц, среди которых могут быть организации, используемые иностранными спецслужбами и организациями в теневой внешней политике иностранного государства в качестве подставных [2, с. 596][6];
- меры административного пресечения и взыскания[7].

Меры административного принуждения, применяемые с целью предупреждения и пресечения акций теневой внешней политики иностранного государства, могут включать в себя: лишение аккредитации фирм и иностранных корреспондентов соответственно в Торгово-промышленной палате и Министерстве иностранных дел РФ; выдворение из пределов России; лишение разрешения на временное проживание или вида на жительство в стране-объекте; депортацию; закрытие въезда иностранцам в РФ; штраф; предупреждение; дисквалификацию; административный арест; конфискацию.

Наиболее распространенными формами теневой внешней политики являются тайные операции и акции влияния (внешнеполитического воздействия) на различные важные объекты в России. Так, основанная на них подспудная политика недружественных государств в сфере межгосударственных отношений

[2] См., например, Указ Президента Российской Федерации от 2 июля 1993 года № 981 «О загранкомандировках должностных лиц центральных органов исполнительной власти» // Собрание актов Президента и Правительства Российской Федерации. 1993. № 28.

[3] См., например, Закон Российской Федерации «О государственной границе Российской Федерации» от 1 апреля 1993 г. № 4730-1 // ВСНД РФ и ВС РФ. 1993. № 17. Ст. 594; Собрание законодательства РФ. 2005. № 10. Ст. 763; Федеральный закон «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» от 15 августа 1996 г. № 114-ФЗ // Собрание законодательства РФ. 1996. № 34. Ст. 4029; 2003. № 27 (ч. 1). Ст. 2700; Таможенный кодекс Российской Федерации от 28 мая 2003 г. № 61-ФЗ // Собрание законодательства РФ. 2003. № 22. Ст. 2066.

[4] См., например, Закон Российской Федерации «О торгово-промышленных палатах в Российской Федерации» от 7 июля 1993 г. № 5340-1 // ВСНД РФ и СНД РФ. 1993. № 33. Ст. 1309; Собрание законодательства РФ. 2003. № 50. Ст. 4855; Закон Российской Федерации «О средствах массовой информации» от 27 декабря 1991 г. № 2124-1 // ВСНД РФ и СНД РФ. 1992. № 7. Ст. 300; Собрание законодательства РФ. 2005. № 30 (ч.1). Ст. 3104; Постановление Правительства Российской Федерации от 2.02.1998 г. № 130 «О порядке регистрации, открытия и закрытия в Российской Федерации представительств иностранных религиозных организаций» от 20 февраля 1998 г. № 130 // Собрание законодательства РФ. 1998. № 6. Ст. 754; Федеральный закон «Об общественных объединениях» от 19 мая 1995 г. № 82-ФЗ // Собрание законодательства РФ. 1995. № 21. Ст. 1930; 2004. № 45. Ст. 4377; Федеральный закон «О некоммерческих организациях» от 12 января 1996 г. № 7-ФЗ // Собрание законодательства РФ. 1996. № 3. Ст. 145.

[5] См., например, Федеральный закон «О правовом положении иностранных граждан в Российской Федерации» от 27 июля 2002 г. № 115-ФЗ // Собрание законодательства РФ. 2002. № 30. Ст. 3032; 2004. № 35. Ст. 3607.

[6] См., например, Федеральный закон «О государственной регистрации юридических лиц» от 8 августа 2001 г. № 129-ФЗ // Собрание законодательства РФ. 2001. № 33. (ч.1). Ст. 3431; 2005. № 27. Ст. 2722. Ст. 61, 64 ГК РФ от 30 ноября 1994 г. № 51-ФЗ. Ч.1 // Собрание законодательства РФ. 1994. № 32. Ст. 3301; 2005. № 30 (ч.2). Ст. 3120.

[7] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства РФ. 2002. № 1 (ч.1). Ст. 1.

латентного противоборства способствовала осуществлению в СССР государственного переворота, ознаменовавшего колоссальные территориальные потери. Страна потеряла примерно 5,2 млн км^2 территории, что превышает территорию всего Европейского союза (4,2 млн км^2) или Индии (3,4 млн км^2). Произошел коренной слом общественно-экономической формации, распад экономического, дипломатического и военного содружества стран, составлявших мировую систему социализма [1, с. 355].

Оценка акций влияния (как правило, это элементы, входящие в состав тайных операций) с позиции уголовного права позволяет заключить, что принимающие в них участие иностранные разведчики подлежат уголовной ответственности как организаторы, подстрекатели или пособники государственной измены, совершаемой участвующими в акциях влияния агентами иностранных спецслужб из числа граждан России. Деяния агентов иностранных спецслужб из числа граждан России, связанные с выполнением заданий в рамках акций влияния, как правило, должны квалифицироваться как государственная измена в форме оказания финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности РФ.

Сущность данного вида деятельности, которая охватывается составом государственной измены, заключается в том, что гражданин России, вступив в контакт с представителями иностранного государства или иностранной организации, оказывает им содействие в осуществлении различного рода акций в ущерб суверенитету, территориальной целостности, обороноспособности и государственной безопасности РФ.

Признаки «иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации» в законе (ст. 275 Уголовного кодекса РФ, далее — УК) не сформулированы.

По объективным свойствам, с оказанием иной помощи сходен целый ряд преступлений, направленных против интересов государственной службы, на подрыв государственной власти, общественной безопасности, общественного порядка и на подрыв экономики страны: ст. 285. Злоупотребление должностными полномочиями; ст. 286. Превышение должностных полномочий; ст. 282. Возбуждение национальной, расовой или религиозной вражды; ст. 178. Монополистические действия и ограничение конкуренции; ст. 179. Принуждение к совершению сделки или отказу от ее совершения; ст. 142. Фальсификация избирательных документов, документов референдума или неправильный подсчет голосов; ст. 279. Вооруженный мятеж; ст. 280. Публичные призывы к насильственному изменению конституционного строя РФ; ст. 105. Убийство; ст. 208. Организация незаконного вооруженного формирования или участие в нем; ст. 212. Массовые беспорядки; ст. 358. Экоцид и т. д.

На наш взгляд, подлежит квалификации как государственная измена в форме оказания финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации, — выполнение иностранными агентами из российских граждан следующих трех основных групп заданий иностранных спецслужб в рамках акций влияния.

Первая группа. Задание агента иностранной спецслужбы заключается в распространении дезинформации или тенденциозно подобранных иностранной разведкой материалов, изданий, в публикации материалов, подрывающих доверие к нашей стране как к добросовестному участнику межгосударственных договоров, в содействии экономической блокаде РФ, помощи в провоцировании международных конфликтов, принуждение к выполнению заданий агентов, вышедших из подчинения, или их ликвидация, уничтожение, блокирование, искажение компьютерной информации, повреждение телекоммуникационных систем и т. д., — словом, в реализации непосредственно функции влияния (воздействия).

Например, в 1930 г. резидент советской разведки в Стамбуле Г. Агабеков встал на путь предательства, установив контакт с представителями спецслужб Великобритании, проводившими подрывную работу против СССР. Через некоторое время Агабеков распространил сведения, составляющие государственную тайну. Он опубликовал за границей книгу, в которой раскрыл многие операции советской разведки в Иране, назвал ее сотрудников, осуществлявших эти операции, и иностранцев, помогавших им в разведывательной деятельности. Последствия измены имели необратимый характер. Просоветское коммунистическое и национально-освободительное движение в Иране было разгромлено. Арестовано более 400 человек, 27 расстреляно. Доверие правящего в то время шаха Р. Пехлеви к СССР было резко подорвано, и со стороны Ирана были приложены усилия, чтобы в наибольшей степени сократить развернувшееся было сотрудничество между двумя странами, как это и требовалось правящим кругам Великобритании [2, с. 771].

Вторая группа. Задание агента иностранной спецслужбы состоит в подборе и изучении перспективных кандидатов на вербовку, их вербовке, продвижении их на работу в руководящие структуры РФ, во внедрении в депутатский корпус, в ВПК, СМИ, оказании консультационной помощи по поводу работы различных организаций, министерств и ведомств России, предоставлении услуг по получению документов другими иностранными разведчиками и агентами, нелегально проникшими и находящимися на территории РФ, — иначе говоря, связано с созданием разведывательных позиций.

Например, осужденный за измену в форме оказания помощи Хван по заданию иностранной разведки занимался подбором кандидатов на вербовку и вербовкой для сбора шпионских сведений не только наших соотечественников, но и иностранных граждан [2, с. 741, 749].

Третья группа. Задания агента являются по своему характеру реализацией организационных, управленческих или снабженческих функций по отношению к шпионской и подрывной работе. Например, настройка функций шифрования в мессенджере для организации шпионской связи с разведцентром, поддержка деньгами организаций, ведущих деятельность против РФ, предоставление транспортных средств другим иностранным разведчикам и агентам, консультационная помощь по поводу работы различных устройств, приборов, перемещения войск, и прочих фактов, если такая информация передается в целях использования против безопасности России.

Так, житель Ленинграда Лубман, осужденный за измену Родине в форме оказания помощи иностранному государству в проведении враждебной деятельности против нашей страны, с помощью связника сообщил в ЦРУ США данные о государственном регистрационном номере автомобиля, которым пользовался один из руководителей страны, и о маршрутах его передвижения по городу [2, с. 674].

Установление контакта с представителями иностранного государства, иностранной организацией считается приготовлением к данному преступлению. С 2022 г. при отсутствии признаков преступления, предусмотренных ст. 275 УК, установление такого контакта на конфиденциальной основе в целях содействия иностранному государству в деятельности, направленной против безопасности России, является самостоятельным преступлением, предусмотренным ст. 275.1 УК РФ.

При реализации акции влияния агент иностранной спецслужбы может одновременно добывать сведения об объекте разведывательного воздействия и о других представляющих для спецслужб интерес предметах, то есть заниматься шпионажем, и осуществлять само воздействие, составляющее оказание иностранному государству, международной либо иностранной организации или их представителям помощи в деятельности, направленной против безопасности обороняющейся страны. Это наглядно показывает следующий пример. Во время Первой мировой войны агент английской разведки добыл бланки и печати морского министерства Германии и ее военной цензуры (т. е. реализовал разведывательную функцию). После этого подготовил и записал на бланке от имени морского министерства Германии приказ, который предписывал немецкой эскадре, находившейся у побережья Чили, совершить переход от порта Вальпараисо к Фолклендским островам. Далее агент заверил приказ необходимыми печатями и, зашифровав, отправил с берлинского телеграфа в адрес эскадры (реализовал разведывательное воздействие). Немецкая эскадра, в составе которой входили крейсеры с новейшими дальнобойными орудиями, выполняя ложный приказ, выдвинулась в указанное место, где ее поджидали английские военные крейсеры, расстрелявшие немцев в упор [3, с. 170]. В подобном случае имеет место государственная измена в двух формах, квалифицируемых по одной ст. 275.

В процессе выполнения задания иностранной спецслужбы по оказанию помощи в проведении деятельности, направленной на нанесение ущерба безопасности России, иностранный агент может совершать деяния, образующие самостоятельные составы преступления. Например, может совершить убийство охранника, препятствующего проникновению на интересующий объект, или пограничника при нелегальном пересечении Государственной границы, или уничтожить бывшего агента в связи с его отказом продолжить шпионскую деятельность. Так, бывший заместитель директора департамента министерства общественной безопасности Польши Юзеф Святло, будучи завербован ЦРУ США, по заданию этой спецслужбы занимался фальсификаций уголовных дел. Злоупотребляя служебным положением, Святло незаконно привлек к уголовной ответственности многих руководящих работников Польши, Венгрии, Чехословакии и Болгарии. Некоторые из них были казнены. Выполнив задание, Святло в 1953 г. бежал в США [2, с. 752, 753, 761].

Если задание по оказанию влияния включает также деяния, которые при отсутствии преступной связи виновного с иностранным государством или иностранной организацией рассматривались бы как самостоятельное преступление (например, привлечение заведомо невиновного к уголовной ответственности или незаконное возбуждение уголовного дела, фальсификация избирательных документов, возбуждение национальной вражды, терроризм, массовые беспорядки, убийство, злоупотребление должностными полномочиями, дача взятки, посредничество во взяточничестве, склонение других лиц к преступлениям), то действия гражданина РФ по выполнению такого задания должны квалифицироваться, наряду со статьями УК, предусматривающими ответственность за такие преступления, также и по статье «Государственная измена в форме оказания финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации».

Иностранные спецслужбы проявляют особую заботу об используемых в своих интересах агентах влияния. Встречи с ними могут проводиться в основном за границей [4, с. 244]. Однако согласно ч. 1 ст. 12 УК РФ сотрудничество российских граждан с иностранной разведкой вне пределов РФ уголовно наказуемо, если в отношении этих лиц по данному преступлению не имеется решения суда иностранного государства[8]. По

[8] Статья 12. Действие уголовного закона в отношении лиц, совершивших преступление вне пределов Российской Федерации // УК РФ.

данному преступлению, естественно, никогда не будет вынесено решение суда иностранного государства, в пользу которого совершается государственная измена. Например, если российский гражданин, находясь на территории ФРГ, под влиянием немецких разведчиков совершает акт государственной измены в пользу Германии, то германская сторона, разумеется, рассматривает это не как преступление, а как акт оказания помощи немецкой разведке в решении стоящих перед ней задач.

Операции теневой внешней политики иностранных государств предусматривают шпионскую и подрывную работу среди оппозиции [5, с. 83]. Шпионская и подрывная работа среди оппозиции зачастую проводится втемную, когда оппозиционеры действуют, не понимая того, что ими на самом деле манипулируют не зарубежные единомышленники, а сотрудники иностранной разведки.

Операции иностранной теневой внешней политики предусматривают также использование государственного аппарата подрываемого государства, то есть связь с должностной преступностью, когда втемную используются чиновники. В этих случаях используемые чиновники, как правило, не вербуются и, соответственно, не ведают, кому именно они служат. Поэтому правомерен вывод, что иностранные спецслужбы должны гибко использовать свои связи в государственном аппарате России. Так, по мнению одного из экспертов ВПК, американцы провели удачную операцию по нанесению ущерба боеготовности Сухопутных войск России, добившись через советских чиновников включения в Договор по РСМД от 08.12.1987 обязательства ускоренного уничтожения российской стороной ракет ОТР-23 «Ока» (по классификации НАТО — SS-23 Spider), которые по своим характеристикам (например, по дальности) вообще не подпадали под действие данного соглашения[9].

Механизм преступного использования должностных лиц в операциях иностранной теневой внешней политики без их вербовки может сводиться к следующим трем основным вариантам.

При первом варианте иностранный разведчик непосредственно воздействует на должностное лицо, а тот принимает выгодное иностранному государству управленческое решение или содействует реализации мер иностранного государства в отношении России. При этом разведчик использует легенду прикрытия своей заинтересованности, благодаря которой должностное лицо искренне полагает, что от него требуется совершить определенное деяние якобы не во вред своей стране. В случае если требуемое деяние осуществляется в рамках должностных полномочий служащего (то есть он вправе избрать этот вариант действий как один из нескольких возможных), состав преступления в его действиях отсутствует. Несмотря на это, можно заключить, что поведение разведчика представляет значительную общественную опасность. Для противодействия ему могут использоваться институты административного и международного права. Так, иностранный разведчик, не пользующийся дипломатическим иммунитетом, может быть лишен разрешения на временное проживание или вида на жительство в России на основании соответственно ст. 7 и 9 Федерального закона от 25 июля 2002 года «О правовом положении иностранных граждан в Российской Федерации», если его действия создают угрозу безопасности РФ. В пятнадцатидневный срок он обязан выехать из России, а в случае неисполнения этой обязанности подлежит депортации в соответствии со статьей 31 этого же закона. Впоследствии ему может быть закрыт въезд в Россию на основании пунктов 1, 2 статьи 27 Федерального закона от 18 июля 1996 года «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию». В случае если иностранный разведчик обладает дипломатическим иммунитетом, он, в соответствии со статьей 9 Венской конвенции о дипломатических сношениях 1961 года, может быть объявлен персоной нон грата[10]. При этом аккредитирующее государство не обязано мотивировать свое решение.

Если предпринятые должностным лицом действия противоречат интересам государственной службы или явно выходят за пределы его полномочий, то они подпадают под признаки преступления, предусмотренного статьей 285 (злоупотребление должностными полномочиями) или статьей 286 (превышение должностных полномочий) УК РФ. Если при этом иностранный разведчик воздействует на должностное лицо уговорами, посулами, обещаниями, угрозами, то его действия следует квалифицировать по статьям 33 и 285 либо по статьям 33 и 286 УК РФ.

Вместе с тем действия должностного лица, наносящие существенный ущерб интересам РФ, но совершаемые им по собственной инициативе, без связи с представителем иностранного государства, в ряде случаев уголовно не наказуемы. Это объясняется тем, что в УК РФ 1996 года статья о вредительстве не включена. Такое поведение российского гражданина, способное перерасти в государственную измену, следует называть, как указано в статье 2 Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», «антиобщественным». В целях недопущения совершения должностным лицом правонарушений, наносящих ущерб интересам России, статья 8 этого федерального закона требует оказать на него воспитательное воздействие, а также принять меры социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение при-

[9] Руднев М. Как предательство Горбачева породило уникальный ракетный комплекс // КОНТ. 07.11.2018. URL: https://cont.ws/@Grubz/1119074 (дата обращения: 30.08.2022).

[10] См.: Сб. важнейших документов по международному праву. Ч. II, особенная. М. : Ин-т междунар. права и экономики; Триада Лтд, 1997. С. 305.

чин и условий, способствующих совершению правонарушений.

Согласно статьям 6, 17, 19—23 вышеуказанного федерального закона профилактика может принимать такие формы, как:

- профилактическая беседа;
- объявление официального предостережения о недопустимости действий, создающих условия для совершения правонарушений, либо недопустимости продолжения антиобщественного поведения;
- профилактический учет;
- внесение представления об устранении причин и условий, способствующих совершению правонарушения;
- профилактический надзор.

Должностные лица компетентных органов страны в целях предупреждения правонарушений уполномочены применять специальные меры профилактики правонарушений оперативно-разыскного характера[11]. Специальные меры направлены непосредственно на предупреждение конкретных видов правонарушений (государственная измена, содействие террористической деятельности и т. д.).

Согласно американской разведывательной практике, подкуп влиятельных политических деятелей, парламентариев, высших чиновников, служащих госучреждений, журналистов, высокопоставленных военных и других лиц, которые по своему положению могут способствовать реализации тайных операций ЦРУ, считается одной из форм акций, которые служат в конечном счете достижению одной главной политической цели администрации США — поддержке и укреплению зарубежных союзников и изоляции, ослаблению и устранению противников [5, с. 84, 86, 91, 92].

При втором варианте, который можно рассматривать в качестве очередной ступени деятельности иностранного разведчика по втягиванию должностного лица в преступную деятельность, разведчик осуществляет воздействие, предоставляя ему денежное вознаграждение в открытой или в замаскированной форме (в виде гонорара за опубликованную за границей книгу или за прочтенные лекции, под видом грантов и премий заграничных фондов и т. п.) либо оказывая услугу материального характера (помогает устроить детей на учебу за границу, организует поездку за границу членам семьи, помогает организовать за границей бизнес членам семьи, вывести денежные средства на оффшорные счета и т. п.). В этом случае действия должностного лица также подпадают под признаки преступления, предусмотренного статьей 290 (получение взятки), а действия разведчика — дополнительно под признаки статьи 291 (дача взятки) УК РФ. В отличие от статьи 285, диспозиция статьи 290 УК РФ существенно расширяет сферу деятельности должностного лица, в которой он несет ответственность за получение взятки, при условии, что она связана с его должностным положением, хотя и не входит в круг его прямых должностных обязанностей. Здесь Закон имеет в виду такие случаи, когда должностное лицо хотя само и не обладает полномочиями для выполнения в интересах иностранного разведчика соответствующих действий, но в силу своего должностного положения (например, высокий пост в Правительстве России, в аппарате Администрации Президента России, Государственной Думы и т. д.) может за взятку, используя свой авторитет и влияние, обеспечить совершение этих действий[12].

В соответствии со статьей 12 УК, в случае получения российским должностным лицом взятки за границей это его деяние уголовно наказуемо, если в отношении этого лица по данному преступлению не имеется решения суда иностранного государства. А под действие закона иностранного государства это деяние, скорее всего, не подпадет, так как не посягает на охраняемые общественные отношения в данном государстве — субъекте теневой внешней политики. Напротив, с морально-нравственной точки зрения для правосудия этой страны такое деяние будет выглядеть как некая доблесть спецслужб, удачная операция национальной разведки. С учетом этого правоохранительным органам в обязательном порядке необходимо собрать доказательства преступной деятельности лица на территории нашей страны или (и) доказать наличие причинно-следственной связи между действиями лица вне пределов РФ и их общественно опасными последствиями, наступившими на территории нашей страны.

При третьем варианте иностранный разведчик воздействует на должностное лицо через посредника, с которым иностранной спецслужбой установлен контакт, а также сотрудников фирм и компаний, используемых в акциях влияния. Если посредник из числа российских граждан сознает, что действует в интересах иностранной спецслужбы, то его деяния следует квалифицировать по совокупности статей 275 и 291 УК РФ. Но в случае, если интерес спецслужбы залегендирован и перед посредником, последний должен отвечать за подстрекательство к злоупотреблению должностным положением или превышению должностных полномочий или (и) за посредничество во взяточничестве (ст. 291.1 УК РФ).

Как можно видеть, борьба с акциями влияния как составными элементами теневой внешней политики иностранного государства должна включать работу по выявлению и пресечению должностных и коррупционных преступлений, вовлекаемых в сферу теневой внешней политики иностранных государств и организаций.

К преступлениям коррупционной направленности, кроме получения и дачи взятки, посредничества во взяточничестве, отнесены:

[11] Федеральный закон от 23 июня 2016г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // СПС «Гарант».

[12] См.: Комментарий к Уголовному кодексу Российской Федерации. М.: НОРМА-ИНФРА-М, 1999. С. 674.

– ст. 141.1 (нарушение порядка финансирования избирательной кампании кандидата, избирательного объединения, избирательного блока, деятельности инициативной группы по проведению референдума, иной группы участников референдума);
– п. «б» ч. 3 ст. 188 (контрабанда должностным лицом с использованием своего служебного положения);
– ст. 294 (коммерческий подкуп);
– ст. 289 (незаконное участие в предпринимательской деятельности) УК РФ.

При наличии ряда дополнительных критериев к преступлениям коррупционной направленности относятся также:

– ст. 174 (легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем);
– ст. 174.1 (легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления);
– ч. 3 ст. 210 (организация преступного сообщества (преступной организации) или участие в нем (ней));
– ст. 202 (злоупотребление полномочиями частными нотариусами и аудиторами);
– ч. 3, 4 ст. 183 (незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну);
– ч. 3, 4 ст. 159 (мошенничество);
– ст. 169 (воспрепятствование законной предпринимательской или иной деятельности);
– ст. 178 (недопущение, ограничение или устранение конкуренции);
– ст. 179 (принуждение к совершению сделки или к отказу от ее совершения) и некоторые другие статьи УК РФ[13].

Интересным представляется вопрос о привлечении иностранных граждан к уголовной ответственности за наносящую ущерб безопасности России деятельность в тех случаях, когда они проводят ее за границей, вне территории России. Так, противодействие теневой внешней политике иностранного государства, связанной с подкупом должностных лиц России, теоретически все-таки в некоторых случаях возможно и с использованием норм зарубежного законодательства.

Например, в Австрии, Испании и Франции введена уголовная ответственность за так называемую торговлю влиянием. Данный состав преступления вытекает из Конвенции ООН против коррупции от 31 октября 2003 г. и Конвенции Совета Европы об уголовной ответственности за коррупцию от 27 января 1999 г. В УК Франции уголовная ответственность за торговлю влиянием регламентирована в статье 433-2 и включает в себя два состава преступления: 1) совершение любым лицом деяния, выражающегося в требовании или принятии прямо или косвенно подношений, обещаний, подарков, презентов или каких бы то ни было преимуществ, с тем чтобы злоупотребить своим влиянием, действительным или мнимым, с целью добиться от государственного органа власти или управления наград, должностей, сделок или любого другого благоприятного решения, 2) в уступке указанным выше требованиям, или прямом или косвенном предложении без законных на то оснований подношений, обещаний, подарков, презентов или каких бы то ни было преимуществ, с тем чтобы какое-либо лицо злоупотребило своим влиянием, действительным или мнимым, с целью добиться получения от какого-либо государственного органа власти или управления наград, должностей, сделок или любого другого благоприятного решения [6, с. 167—172].

Закон США о коррупции за рубежом (Foreign Corrupt Practices Act) 1977 г. также запрещает подкуп публичных должностных лиц в процессе ведения внешнеэкономической деятельности за рубежом[14]. Закон начал активно применяться с 2005 г. и за период с 2010 по 2013 гг. Комиссия по ценным бумагам привлекла к ответственности за подкуп иностранных публичных должностных лиц и их родственников в разных странах, за подарки, «откаты» и другие неправомерные платежи, 44 компании. Среди них оказались «Джонсон энд Джонсон», «Ральф Лаурен Корпорейшн», «Дженерал Электрик», «Пфайзер», «Даймлер», «Мерседес-Бенц Рус», «Сименс». Компании «Даймлер» пришлось выплатить 200 млн долларов штрафа, «Мерседес-Бенц Рус» — 27 млн долларов, «Сименс» — около 2 млрд долларов[15] [7, с. 30—48]. (Аналогичным образом ответственность юридических лиц за коррупцию, начиная с 2009 года, предусмотрена статьей 19.28 КоАП РФ.)

Закон Великобритании о взяточничестве (United Kingdom Bribery Act) имеет экстерриториальное юридическое действие. Закон стремится внедрить интернациональный подход в борьбе с коррупцией, в частности, привести антикоррупционные локальные нормативные документы компаний в различных странах в соответствие с требованиями Конвенции Организации экономического сотрудничества и развития по борьбе с подкупом иностранных должностных лиц при осуществлении международных коммерческих сделок. Закон предусматривает ответственность компании за преступление в виде штрафа, причем не ограничивает его размер, а отдает его определение на усмотрение суда, а также ответственность физических лиц в виде лишения свободы сроком до 10 лет. Ответственность

[13] Перечень преступлений коррупционной направленности / Информационные и аналитические материалы по противодействию коррупции / Информационно-аналитические материалы / Документы / Главное управление Федеральной службы судебных приставов по Оренбургской области. URL: https://r56.fssp.gov.ru/Prkorr7 (дата обращения 06.09.2022).

[14] Foreign corrupt practices act. URL: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act (дата обращения: 06.09.2022).

[15] SEC Enforcement Actions: FCPA Cases. URL: https://www.sec.gov/enforce/sec-enforcement-actions-fcpa-cases (дата обращения: 05.02.2024).

возлагается не только на взяткодателя, но и на компанию, интересы которой представляет взяткодатель, то есть действие закона распространяется на любых субъектов, имеющих какое-либо отношение к компании, в том числе ассоциированных лиц[16].

В соответствии с частью 3 статьи 12 УК РФ иностранные граждане, совершившие преступления против интересов РФ вне ее пределов, подлежат уголовной ответственности в случаях, если они не были осуждены в иностранном государстве и привлекаются к уголовной ответственности на территории РФ.

Как и в вышеприведенном гипотетическом примере с немецкой разведкой и ее агентом из числа российских граждан, можно сразу исключить практическое привлечение местными властями на территории Франции, США, Великобритании и их союзников по НАТО физических лиц к уголовной ответственности за проведение деятельности в ущерб безопасности России по заданию соответственно французских, американских или английских спецслужб. Однако такая возможность, прежде всего теоретически, возникает, если «торговцы влиянием» и коррупционеры действуют на территории Франции, США, Великобритании по заданию спецслужбы какой-либо другой страны (особенно недружественной НАТО) либо некоей террористической организации, например, «Аль-Каиды» или «Хезболлах». Таким образом, некоторые законы иностранных государств в отдельных случаях также применимы в противодействии иностранной теневой внешней политике.

Далее хотелось бы обратить внимание на следующий важный вопрос. Что касается российских граждан, то их ответственность за оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности РФ, в УК РФ предусмотрена. В то же время прямого запрета на проведение данной деятельности иностранцами уголовный закон не содержит (за исключением тех случаев, когда она связана с террористической деятельностью[17]).

В качестве примера можно привести деятельность гражданина Латвии, агента немецких спецслужб Ореста Берлинкса, которая оказала отрицательное влияние на формирование представлений советского руководства о намерениях Гитлера в мае — июне 1941 г. и нанесла колоссальный ущерб безопасности нашей страны. В соответствии с современным уголовным законом, однако, такая деятельность иностранца не наказуема.

Немецкие спецслужбы подставили Берлинкса резидентуре разведки НКВД в Берлине, которой он был завербован под псевдонимом «Лицеист». Он сообщал советским разведчикам, будто бы германское руководство планирует в ближайшее время напасть не на СССР, а на Великобританию. Сосредоточение немецких войск на советской границе, по уверениям «Лицеиста», было частью стратегической дезинформации, отвлекающей внимание от приготовлений к вторжению в Англию.

В мае 1947 г. на допросе бывший сотрудник гестапо З. Мюллер по данному делу дал следующие показания: «Нам удалось установить, что советник советского посольства Кобулов вел в Германии разведывательную работу. Кобулову в августе 1940 г. был подставлен агент германской разведки — латыш Берлинкс, который по нашему заданию длительное время снабжал его дезинформационными материалами. Берлинкс говорил мне, что ему удалось войти в доверие к Кобулову, что последний рассказывал Берлинксу даже о том, что свои доклады он направлял лично Сталину и Молотову. Очевидно, что все это позволило Гитлеру рассматривать Кобулова как удобную возможность для посылки дезинформации в Москву, в связи с чем он лично занимался этим вопросом и материалами, предназначавшимися для передачи Кобулову. Практика была такой: Риббентроп готовил эти материалы, затем докладывал их Гитлеру и только с его санкции материалы передавались агенту Берлинксу, который и доставлял их Кобулову» [8, с. 444—447].

Ответственность иностранцев за проведение деятельности в ущерб безопасности страны-объекта заложена в УК некоторых иностранных государств. Например, параграф 87 УК ФРГ устанавливает ответственность за подготовку актов саботажа, параграф 89 — за подрыв готовности чиновников бундестага и органов безопасности к защите ФРГ и ее конституционного строя. До 1968 года изменой стране признавалось противоречащее долгу ведение государственных дел[18]. Параграф 371 Свода законов США предусматривает ответственность за «сговор, направленный на совершение посягательства или обмана в отношении Соединенных Штатов», параграф 2386 — за уклонение от регистрации организаций, находящихся под иностранным финансовым, политическим и прочим контролем[19]. Статьи 102, 103, 105 УК КНР предусматривают ответственность за «сговор с иностранным государством в ущерб суверенитету, территориальной целостности

[16] Закон Великобритании «О взятках», 2010 год // Собрание законодательства Великобритании; 2010; глава 23 / Juris facto. Центр переводов. URL: https://perevodzakonov.ru/zakony/bribery-act-2010-ru.pdf (дата обращения: 06.09.2022).

[17] Статья 205.1. УК Содействие террористической деятельности запрещает финансирование терроризма — предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки или совершения преступления террористического характера, а также пособничество — умышленное содействие совершению преступления советами, указаниями, предоставлением информации, средств или орудий совершения преступления либо устранением препятствий к его совершению, а также обещание скрыть преступника, средства или орудия совершения преступления, следы преступления либо предметы, добытые преступным путем, а равно обещание приобрести или сбыть такие предметы. (Прим. авт.)

[18] См.: Гришаев П.И. Ответственность за государственные преступления по уголовному законодательству ФРГ. М.: Б.и., 1970. С. 35, 42, 48.

[19] См.: Уголовное право США : сборник нормативных актов / Сост. Козочкин И.Д. М. : Изд. УДН, 1986. С. 31, 42, 48, 59.

и безопасности КНР, … раскол страны, нарушение ее единства,… подрыв государственной власти, свержение социалистического строя»[20].

Видимо, назрела необходимость специально проработать вопрос о введении в УК РФ статьи, которая, наподобие статьи 276, специально предусматривала бы ответственность иностранцев и лиц без гражданства за участие в подрывных акциях влияния, направленных на ослабление безопасности РФ путем вмешательства в ее внутренние и внешние дела [1, с. 383].

Надо также обратить особое внимание на то, что в США для борьбы с подрывной деятельностью иностранных спецслужб и организаций успешно применяются регистрационные законы: Закон 1938 года о регистрации иностранных агентов, Закон Вурхиса 1940 года о регистрации американских организаций, находящихся под иностранным контролем, Закон 1940 года о регистрации иностранцев, Закон 1956 года о регистрации лиц, прошедших подготовку в системе разведки иностранного государства, Закон 1950 года о внутренней безопасности. Перечисленные законы устанавливают уголовную ответственность за уклонение либо за нарушение правил регистрации. С одной стороны, они имеют большое превентивное значение для общей профилактики антигосударственных преступлений, с другой — значительно облегчают деятельность контрразведки США по предупреждению и пресечению подрывной деятельности. ФБР имеет возможность в некоторых случаях не обременять себя сложным и подчас трудно осуществимым процессом сбора доказательств подрывной деятельности из процессуальных источников. Контрразведке США достаточно доказать лишь факт уклонения от регистрации в качестве лица, состоящего на службе у иностранного государства или организации, либо в качестве члена определенной организации, либо в качестве лица, проходившего обучение в зарубежной разведшколе [9, с. 228—242].

В России в 2012 г. также приняты правовые запреты на уклонение от регистрации лиц и организаций, находящихся под иностранным контролем, под угрозой административного наказания. Введен регистрационный режим для агентов иностранной власти и российских организаций, находящихся под иностранным контролем[21]. Данный режим стал правовым барьером, который вынужден преодолевать противник в процессе осуществления разведывательной и иной деятельности, направленной на нанесение ущерба России (подрывной деятельности). Отечественным правоохранительным органам достаточно привлечь, как это практикуется в США, субъектов проведения разведывательной и иной деятельности, направленной на нанесение ущерба России, к ответственности за нарушение данного режима, что гораздо проще привлечения к ответственности за проведение тайных операций и акций.

Кроме того, в России, по примеру США и других западных стран, внедрена практика составления списков юридических и физических лиц, с которыми не рекомендуется поддерживать отношения или поддержание отношений с которыми преследуется по закону. Например, ведется перечень иностранных и международных неправительственных организаций, деятельность которых признана нежелательной на территории РФ; реестр иностранных средств массовой информации, выполняющих функции иностранного агента; список некоммерческих организаций, выполняющих функции иностранного агента; список физических лиц, выполняющих функции иностранного агента[22]. Кроме того, ведется реестр недобросовестных поставщиков (подрядчиков, исполнителей) в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд[23].

Данный фактор создал более благоприятные условия для того, чтобы своевременно нейтрализовать подставные организации спецслужб и организаций иностранных государств, используемые в теневой внешней политике иностранного государства [10, с. 80—89].

В целях противодействия разведывательной и иной деятельности, направленной на нанесение ущерба России, могут также использоваться отдельные положения Кодекса Российской Федерации об административных правонарушениях. Например, Кодекс предусматривает административную ответственность за следующие виды правонарушений, которые могут входить как элементы в состав акций теневой внешней политики иностранного государства:

- ст. 5.19 (использование незаконной материальной поддержки кандидатом, зарегистрированным кандидатом, избирательным объединением, избирательным блоком, инициативной группой по проведению референдума);
- ст. 5.20 (финансирование избирательной кампании, проведения референдума помимо избирательных фондов, фондов для участия в референдуме и оказание иной запрещенной законом материальной помощи);

[20] Ахметшин Х.М., Ахметшин Н.Х., Петухов А.А. Современное уголовное законодательство КНР. М. : Муравей, 2000. С. 280–281.

[21] Федеральный закон «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» от 28.12.2012 № 272-ФЗ (последняя редакция) // СПС «КонсультантПлюс»; статья 19.34.1 КоАП РФ (нарушение порядка деятельности иностранного средства массовой информации, выполняющего функции иностранного агента, и (или) учрежденного им российского юридического лица, выполняющего функции иностранного агента) // СПС «КонсультантПлюс».

[22] Ст. 2.1, 3.1 Федерального закона «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» от 28.12.2012 № 272-ФЗ // СПС «КонсультантПлюс»; Федеральный закон от 14 июля 2022 г. № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием» // СПС «Гарант»; статья 13.1 Федерального закона от 12.01.1996 № 7-ФЗ (ред. от 02.07.2021, с изм. от 14.07.2022) «О некоммерческих организациях» // СПС «КонсультантПлюс».

[23] Статья 104 Федерального закона от 05.04.2013 № 44-ФЗ (ред. от 14.07.2022) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // СПС «КонсультантПлюс».

– ст. 16.3 (перемещение товаров и (или) транспортных средств с несоблюдением мер по защите экономических интересов Российской Федерации и других запретов и ограничений);
– ст. 18.8 (нарушение иностранным гражданином или лицом без гражданства режима пребывания в Российской Федерации) и т. п.

Кодекс предусматривает также такое взыскание, как дисквалификация (ст. 3.11), суть которого состоит в лишении физических лиц в судебном порядке лица права занимать руководящие должности в исполнительном органе юридического лица, входить в совет директоров (наблюдательный совет), осуществлять предпринимательскую деятельность по управлению юридическим лицом, а также осуществлять управление юридическим лицом.

Кроме того, как указывалось ранее, компетентные органы страны наделены правами выносить обязательные для исполнения представления о принятии мер по устранению причин, условий, обстоятельств, способствующих реализации угроз безопасности РФ, совершению преступлений, об устранении нарушений законов. Эти представления могут вноситься в государственные органы, администрацию предприятий, учреждений и организаций независимо от форм собственности, а также в общественные объединения, что также должно использоваться в интересах противодействия разведывательной и иной деятельности иностранных государств и организаций, направленной на нанесение ущерба России.

Выводы

Следует отметить, что латентная деятельность недружественных стран, направленная на нанесение ущерба РФ, наиболее полно отражается понятием теневой внешней политики. Спектр угроз, исходящих от теневой внешней политики недружественных государств, весьма широк. В него входят как преступные с точки зрения законодательства РФ деяния, так и непреступные. Например, получившие в последнее время известность санкции Запада в отношении России вряд ли нарушают законы России; создание враждебных России дипломатических союзов и альянсов также не может преследоваться по УК РФ. Можно привести множество других примеров недружественных, но не нарушающих УК деяний. Зачастую деструктивную деятельность граждан в пользу недружественных стран образуют действия, пока не криминализированные. Однако сердцевину недружественной деятельности иностранных государств и деструктивной деятельности отдельных лиц составляют деяния, преследуемые в уголовном порядке. Учитывая эти обстоятельства, значительная роль в противодействии теневой внешней политике отводится административным мерам предупреждения недружественной и деструктивной деятельности.

Подводя итог, обратим внимание на поднятый в работе вопрос о целесообразности установления прямого законодательного запрета на проведение иностранцами и лицами без гражданства иной (помимо разведывательной) деятельности, направленной на нанесение ущерба безопасности страны.

Литература

1. Агишев Р.Г. Теневая внешняя политика иностранных государств : монография. М. : Вече, 2023. 480 с.
2. Рябчук В.Н. Государственная измена и шпионаж: уголовно-правовое и криминологическое исследование. СПб. : Изд. Р. Асланова «Юридический центр Пресс», 2017. 1102 с.
3. Анин Б., Петрович А. Радиошпионаж. М. : Междунар. отношения, 1996. 448 с.
4. Красильников Р. Призраки с улицы Чайковского. М. : ГЕЯ итэрум, 1999. 299 с.
5. Филип Эйджи. За кулисами ЦРУ. Дневник сотрудника американской разведки. Пер. с англ. М. : Воениздат, 1979. 464 с.
6. Вейберт С.И. К вопросу о введении уголовной ответственности за торговлю влиянием в России: опыт регулирования и правоприменения во Франции // Вестник Омского университета. Серия «Право». 2013. № 2 (35). С. 167—172.
7. Трофимов Е.В. Закон США о зарубежной коррупционной практике 1977 г. и международно-правовые инициативы по глобальному противодействию коррупции: проблемы криминализации и администрирования сомнительных операций транснациональных корпораций в 1970-х гг. // Право и политика, 2019. № 2. С. 30—48.
8. Очерки истории российской внешней разведки. Т. 3: 1933—1941 годы. М. : Междунар. отношения, 1997. 496 с.
9. Дундуков М.Ю. Разведка в государственном механизме США. М. : Кучково поле, 2008. 448 с.
10. Фарои Т.В. Подрывная деятельность западных неправительственных организаций на постсоветском пространстве и в РФ: цели, методы и результаты // Всероссийский сборник научных трудов «Социально-гуманитарный вестник». Барнаул, 2023. С. 80—89.

CONSTITUTIONAL LAW MEASURES FOR COUNTERING SHADOW FOREIGN POLICY OF UNFRIENDLY COUNTRIES

Rishat Agishev, *Dr.Sc. (Economics), Academician at the Academy of Military Science, Professor at the Department of Public and International Legal Support for National Security of the Gubkin Russian State University of Oil and Gas, Moscow, Russian Federation.*
E-mail: *agish.gubkin@gmail.com*

Keywords: *inter-state relations, latent confrontation, bringing to liability, criminal and administrative responsibility.*

Abstract

Purpose of the work: identifying constitutional law approaches to countering harmful covert foreign policy of foreign countries.

Methods used in the study: dialectics, scientific methods of cognition based on it, and system approach.

Study findings: a system of legal measures used by the government to protect itself against threats emanating from shadow foreign policy of unfriendly countries is shown. Possibilities for using criminal and administrative law to that end are described. Gaps in the criminal law are noted as regards activities (other than intelligence gathering) carried out by foreign citizens and stateless persons and aimed at causing damage to the security of the Russian Federation.

Research novelty: the state of regulation of countering actions and operations of covert foreign policy of unfriendly countries from the standpoint of domestic law is examined. A systematisation is given of legal measures used by Russia and some other countries to protect themselves against actions and operations carried out latently by unfriendly countries. Problems occurring in this sphere in the Russian Federation are highlighted, and proposals for solving them are put forward.

References

1. Agishev R.G. Tenevaia vneshniaia politika inostrannykh gosudarstv : monografiia. M. : Veche, 2023. 480 pp.
2. Riabchuk V.N. Gosudarstvennaia izmena i shpionazh: ugolovno-pravovoe i kriminologicheskoe issledovanie. SPb. : Izd. R. Aslanova "Iuridicheskii tsentr Press", 2017. 1102 pp.
3. Anin B., Petrovich A. Radioshpionazh. M. : Mezhdunar. otnosheniia, 1996. 448 pp.
4. Krasil'nikov R. Prizraki s ulitsy Chaikovskogo. M. : GEIA iterum, 1999. 299 pp.
5. Filip Eidzhi. Za kulisami TsRU. Dnevnik sotrudnika amerikanskoi razvedki. Per. s angl. M. : Voenizdat, 1979. 464 pp.
6. Veibert S.I. K voprosu o vvedenii ugolovnoi otvetstvennosti za torgovliu vliianiem v Rossii: opyt regulirovaniia i pravoprimeneniia vo Frantsii. Vestnik Omskogo universiteta, seriia "Pravo", 2013, No. 2 (35), pp. 167–172.
7. Trofimov E.V. Zakon SShA o zarubezhnoi korruptsionnoi praktike 1977 g. i mezhdunarodno-pravovye initsiativy po global'nomu protivodeistviiu korruptsii: problemy kriminalizatsii i administrirovaniia somnitel'nykh operatsii transnatsional'nykh korporatsii v 1970-kh gg. Pravo i politika, 2019, No. 2, pp. 30–48.
8. Ocherki istorii rossiiskoi vneshnei razvedki. T. 3: 1933–1941 gody. M. : Mezhdunar. otnosheniia, 1997. 496 pp.
9. Dundukov M.Iu. Razvedka v gosudarstvennom mekhanizme SShA. M. : Kuchkovo pole, 2008. 448 pp.
10. Faroi T.V. Podryvnaia deiatel'nost' zapadnykh nepravitel'stvennykh organizatsii na postsovetskom prostranstve i v RF: tseli, metody i rezul'taty. Vserossiiskii sbornik nauchnykh trudov "Sotsial'no-gumanitarnyi vestnik". Barnaul, 2023, pp. 80–89.

ОБЩЕЕ КУЛЬТУРНОЕ ПРОСТРАНСТВО СТРАН СНГ: ПЕРСПЕКТИВА ГАРМОНИЗАЦИИ ЗАКОНОДАТЕЛЬСТВА

Савченко Е.А.[1]

Ключевые слова: *виртуальное пространство, гуманитарная политика, институциональные основы, цифровые права.*

Аннотация

Цель работы: рассмотреть институциональные основы культурного сотрудничества стран СНГ; определить перспективы гармонизации законодательства в целях формирования общего культурного пространства стран СНГ; рассмотреть соотношение понятия общего культурного пространства стран СНГ с правовым и виртуальным пространством.

Методы исследования: общенаучные и традиционные методы юридической науки.

Результаты исследования: сделан вывод, что основными инструментами формирования общего культурного пространства стран СНГ являются различные формы культурного обмена, при этом виртуальное пространство, являясь составной частью культурного пространства, меняет формат приобщения к культурным ценностям, появляются так называемые «цифровые права» в сфере культуры. В связи с этим необходимо констатировать, что в настоящее время проблема гармонизации законодательства стран СНГ особенно актуальна. В статье акцентируется внимание на том, что основным направлением гармонизации законодательства стран СНГ является правовая регламентация деятельности в виртуальном пространстве с точки зрения реализации права доступа к культурным ценностям на всём пространстве стран СНГ.

Практическая ценность исследования: впервые сформулирована необходимость правовой регламентации гарантированности права на доступ к цифровым информационным ресурсам о культуре, поскольку во всех странах СНГ реализуются программы по созданию национальных интернет-порталов о культуре. Представлена авторская позиция соотношения правового, культурного и виртуального пространства.

DOI:10.21681/1994-1404-2024-1-40-49

Введение и постановка задачи

Формирование общего культурного пространства государств — участников Содружества Независимых Государств (далее — стран СНГ) является одним из приоритетов гуманитарной политики Российской Федерации и направлено на сохранение общих культурных достижений советского времени, дальнейшее взаимодействие и взаимообогащение культур. Народы стран СНГ объединяет многовековая история, общий культурный и цивилизационный код, что предопределяет необходимость формирования общего культурного пространства в условиях современных вызовов. Культурное взаимодействие создаёт благоприятные условия и для взаимодействия стран СНГ по другим вопросам гуманитарной политики. В период трансформации мировой политической системы «общественное сознание, лишившись доктринального человеческого системообразующего начала, стало весьма уязвимым для проникновения чуждых нашей культуре жизненных смыслов»[2]. Поэтому в Концепции гуманитарной политики Российской Федерации за рубежом[3] особо отмечается необходимость многостороннего гуманитарного сотрудничества со странами СНГ. В этих целях особую важность представляет формирование единого культурного, образовательного и информационного пространства.

Хотя важнейшим для нашей страны интеграционным объединением является Евразийский экономический союз (далее — ЕАЭС), который за годы своего существования подтвердил свою жизнеспособность как механизм согласованного взаимодействия в решении

[2] Синюков В.Н. Личность в российской правовой системе: поиск новых подходов // Журнал российского права. 2023. № 5. С. 75—85.

[3] Указ Президента РФ от 05.09.2022 № 611 «Об утверждении Концепции гуманитарной политики Российской Федерации за рубежом».

[1] ***Савченко Елена Алексеевна,*** *кандидат юридических наук, научный сотрудник отдела социального законодательства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, г. Москва, Российская Федерация. ORCID: 0000-0001-8346-8829.*

E-mail: elen_savchenko@bk.ru

экономических и социальных задач, однако, рассматривая вопрос об общем культурном пространстве, всё же правильно рассматривать именно общее культурное пространство стран СНГ, поскольку, ограничиваясь рамками ЕАЭС, мы можем рассматривать только ситуационные вопросы, например «таможенный контроль в ходе перемещения культурных ценностей через таможенную границу ЕАЭС»[4].

Целями же формирования общего культурного пространства стран СНГ являются: укрепление единства народов стран СНГ посредством приоритетного культурного и гуманитарного развития; сохранение исторического и культурного наследия и его использование для воспитания и образования; передача от поколения к поколению традиционных норм, традиций, обычаев и образцов поведения; создание условий для реализации каждым человеком на пространстве СНГ его творческого потенциала и доступа к культурным ценностям и благам.

На заседании Совета глав правительств СНГ, который был посвящён вопросам развития культурно-гуманитарного сотрудничества, было отмечено, что «тесная культурная взаимосвязь и духовная близость наших народов» является «фундаментом, на котором выстраиваются интеграционные процессы в рамках СНГ»[5].

Поэтому планируется в ходе председательства России в СНГ, которое началось с 1 января 2024 года, «развивать практику проведения широкого круга совместных мероприятий по самым разным направлениям искусства, образования и науки»[6].

Правовой основой реализации культурной политики в рамках председательства России в СНГ, помимо основополагающих документов в сфере культуры в рамках СНГ[7], являются: План приоритетных мероприятий в сфере гуманитарного сотрудничества на 2023—2024 годы, перечень Основных мероприятий сотрудничества государств — участников СНГ в области культуры на 2021—2025 годы, Межгосударственная программа «Культурные столицы Содружества» и др.

Исходя из целей формирования общего культурного пространства стран СНГ, **задачами настоящего исследования являются:**

- установить инструменты и основополагающие акты, регулирующие вопросы формирования общего культурного пространства стран СНГ;
- рассмотреть институциональные основы культурного сотрудничества стран СНГ;
- определить перспективы гармонизации законодательства в целях формирования общего культурного пространства стран СНГ;
- рассмотреть соотношение понятия общего культурного пространства стран СНГ с правовым и виртуальным пространством.

Вопросы культурного пространства рассматривались многими учёными. Например, академик Д.С. Лихачёв под культурным пространством понимал «не просто определенную географическую территорию, а прежде всего пространство среды, имеющее не только протяженность, но и глубину»[8]. Культурное пространство, по мнению учёного, включает в себя и религию, и науку, и образование, а также нравственные и моральные нормы поведения людей и государства. При этом роль государства в формировании общего культурного пространства является превалирующей. Академик В.С. Стёпин исследовал «взаимодействие норм и ценностей различных культур в культурном пространстве России»[9] и определял культуру «как систему исторически развивающихся надбиологических программ»[10] человеческой жизнедеятельности». Член-корреспондент Российской академии наук Е.А. Лукашёва, рассматривая взаимодействие права и культуры, предложила свой подход к содержанию понятия культуры[11]. Ряд авторов исследовали вопросы культурной политики[12], цифровизации культурного пространства[13], полномочий органов публичной власти в системе культуры[14] и культурного сотрудничества на пространстве СНГ[15].

Основными инструментами формирования общего культурного пространства стран СНГ являются различные формы культурного обмена: фестивали, медиафорумы (например, XVII Международный медиафорум молодых журналистов «Диалог культур»[16]), культурно-образовательные форумы (например, «Дети Содружества»), научно-практические семинары (например, «Сохранение нематериального культурного наследия стран СНГ в контексте глобальных вызовов») и др.

---

[4] Михеева И.В., Логинова А.С. Вариативность нормативного закрепления понятия «культурные ценности» в законодательстве ЕАЭС // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 1. С. 69—74.

[5] URL: http://government.ru/news/50443/

[6] URL: http://government.ru/news/50443/

[7] Их подробный анализ будет рассмотрен ниже.

[8] Лихачёв Д.С. Русская культура. СПб. : Искусство, 2007.

[9] Стёпин В.С. Цивилизация и культура. СПб. : СПбГУП, 2011. С. 321.

[10] Программы представлены в культуре многообразием знаний, норм, навыков, идеалов, образцов деятельности и поведения, идей, гипотез, верований, целей, ценностных ориентаций и т. д.

[11] Лукашёва Е.А. Право и культура // Труды Института государства и права Российской академии наук. 2012. № 5. С. 26—42.

[12] Ивлиев Г.П. Культурная политика и развитие законодательства о культуре в Российской Федерации. М., 2012. С. 86.

[13] Дугужева М.Х., Симаева Е.П. Трансформация законодательства о культуре в условиях цифровизации // Вестник Пермского университета. Юридические науки. 2019. Вып. 44. С. 193.

[14] См., напр.: Жуков Д.В. Полномочия органов публичной власти по обеспечению конституционного права на доступ к культурным ценностям : дисс. … канд. юр. наук. М., Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. 2018. 159 с.

[15] Шульга С.В. Международно-правовое обеспечение межэтнического и межкультурного диалога на примере Содружества Независимых Государств (с. 33—38) // Материалы международной научно-практической конференции «Социальная справедливость и право: к упрочению мира и предотвращению кризисов», Московский гуманитарный университет, 17—18 февраля 2023 г.; Фокин В.И., Боголюбова Н.М., Николаева Ю.В. Культурное сотрудничество на пространстве СНГ // Управленческое консультирование. 2017. № 5 (101). С. 28—43.

[16] URL: https://mediacongress.ru/dialogcultur23_main

Одним из наиболее действенных инструментов по формированию общего культурного пространства стран СНГ являются фестивали. Например, наибольшую известность за время своего существования приобрели международный театральный фестиваль «Золотая маска» (с 1993 г.), фестиваль-симпозиум «Содружество академических искусств», который стал смотром национальных культур, фестиваль искусств «Славянский базар в Витебске», театральный фестиваль стран СНГ «Встречи в России». Появляются и новые инструменты, формирующие культурное пространство: например, в 2023 году была завершена работа по созданию Виртуального музея культурного наследия государств — участников СНГ, целью которого является объединение материального культурного наследия стран СНГ в едином виртуальном музее.

Рассматривая вопрос формирования общего культурного пространства стран СНГ в историческом ракурсе, нельзя не отметить, что после распада СССР произошло и разрушение единого пространства советской культуры. В первые годы существования СНГ «не удалось сохранить единое культурное пространство, где многонациональная культура сохранила бы свою целостность, следуя общей системе идеалов»[17]. Однако уже при обсуждении и принятии Устава СНГ была чётко обозначена необходимость тесного сотрудничества «в сохранении культурных ценностей и культурном обмене»[18] стран СНГ.

Правовой базой межгосударственных отношений в сфере культуры в рамках СНГ являются многосторонние и двусторонние соглашения. Среди основополагающих актов для формирования общего культурного пространства стран СНГ можно отметить:

- Соглашение о сотрудничестве в области культуры, подписанное 15 мая 1992 г. в Ташкенте[19],
- Соглашение о создании Совета по культурному сотрудничеству государств — участников Содружества Независимых Государств от 26 мая 1995 г.[20],
- Соглашение о гуманитарном сотрудничестве государств — участников Содружества Независимых Государств от 26 августа 2005 г. и
- Концепцию сотрудничества государств — участников Содружества Независимых Государств в сфере культуры от 19 мая 2011 г.[21]

В Концепции подчёркивается, что «сотрудничество в сфере культуры является одним из главных инструментов обеспечения устойчивого социально-экономического развития государств-участников СНГ»[22].

В этих целях необходимо рассмотреть **институциональные основы культурного сотрудничества стран СНГ.** Одним из первых институтов, отвечающих за организацию культурных обменов между государствами-членами, стал учрежденный 26 мая 1995 г. Совет по культурному сотрудничеству стран СНГ (далее — СКС).

В соответствии с Положением[23] Совет осуществляет в рамках своей компетенции такие функции, как организация взаимодействия государственных и общественных структур, осуществляющих культурные связи в рамках СНГ; подготовка проектов многосторонних международных договоров и организация мероприятий, относящихся к компетенции Совета; содействие органам государственной власти в сфере культуры в выработке согласованных действий и др.

В целях координации деятельности СНГ в гуманитарной сфере был создан Совет по гуманитарному сотрудничеству государств — участников СНГ (далее — СГС), соглашение о создании которого было подписано в Минске 28 ноября 2006 г.[24] Среди наиболее значимых функций Совета можно отметить такие, как: определение концептуальных направлений и форм сотрудничества в гуманитарной сфере; подготовку планов приоритетных межгосударственных мероприятий и проектов международно-правовых документов в сфере гуманитарного сотрудничества; организацию взаимодействия с Межгосударственным фондом гуманитарного сотрудничества государств-участников Содружества Независимых Государств (далее — МФГС)[25].

Анализируя компетенцию СГС и СКС, необходимо отметить, что, во-первых, «регуляторами компетенции» в данном случае «становятся соглашения, роль которых нельзя преувеличивать»[26], и, во-вторых, нельзя не отметить сходство некоторых функций, за исключением одного обстоятельства: компетенция СГС распространяется на более широкий круг субъектов, чем компетенция СКС, поскольку охватывает не только сферу культуры, но и сферу образования, науки, архивного

---

[17] Фокин В.И., Боголюбова Н.М., Николаева Ю.В. Культурное сотрудничество на пространстве СНГ // Управленческое консультирование. 2017. № 5 (101). С. 28—43.

[18] Устав Содружества Независимых Государств // Единый реестр правовых актов и других документов Содружества Независимых Государств. URL: http://cis. minsk.by/reestr/ru/index.html reestr/view/text?doc=187 (дата обращения: 25.12.2023).

[19] Соглашение о сотрудничестве в области культуры между Россией и СНГ от 15 мая 1992 г. URL: http://http://cis.minsk.by/main.aspx?uid=7602 (дата обращения: 19.12.2023).

[20] В редакции Протокола о внесении изменений и дополнений в Соглашение о создании Совета по культурному сотрудничеству государств — участников Содружества Независимых Государств от 26 мая 1995 г., подписанного 18 октября 2011 г.

[21] Решением Совета глав государств от 18.12.2020 Концепция изложена в новой редакции.

[22] Решение Совета глав правительств СНГ «О Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере культуры». Принято в г. Минске 19.05.2011.

[23] Протокол о внесении изменений и дополнений в Соглашение о создании Совета по культурному сотрудничеству государств-участников Содружества Независимых Государств от 26 мая 1995 года (вместе с Положением о Совете...). Подписан в г. Санкт-Петербурге 18.10.2011.

[24] Соглашение о Совете по гуманитарному сотрудничеству государств-участников Содружества Независимых Государств (вместе с «Положением...»).

[25] Договор о создании Межгосударственного фонда гуманитарного сотрудничества государств — участников СНГ (МФГС) от 25 мая 2006 г. Участниками являются Россия, Азербайджан (с июня 2008 г.), Армения, Белоруссия, Казахстан, Киргизия, Молдавия (с июля 2014 г.), Таджикистан и Узбекистан.

[26] Тихомиров Ю.А. Теория компетенции. М., 2001. С. 26.

дела, информации и массовых коммуникаций, спорта, туризма и работы с молодежью.

Одним из важных институтов в развитии общего культурно-гуманитарного пространства и активизации межкультурного диалога в СНГ является Межгосударственный фонд гуманитарного сотрудничества государств-участников СНГ[27]. Фонд является межгосударственной некоммерческой организацией и обеспечивает финансирование мероприятий в области гуманитарного сотрудничества. В Концепции гуманитарной политики Российской Федерации за рубежом[28] особо подчёркивается необходимость взаимодействия с СГС и МФГС.

Особое место в формировании общекультурного пространства занимает Межпарламентская Ассамблея (далее — МПА СНГ), которая является надгосударственным органом парламентского типа, и Экспертный совет МПА СНГ — Региональное содружество в области связи (далее ЭС МПА СНГ — РСС). МПА СНГ и РСС осуществляют функции по разработке согласованных подходов в целях сближения правовых систем стран СНГ и создания условий для всесторонней интеграции в рамках СНГ на основе принимаемых модельных законодательных актов.

Модельные акты МПА СНГ в сфере культуры носят рекомендательный характер и служат ориентиром в развитии и сближении законодательства стран СНГ[29] в целях формирования правовых основ общего культурного пространства СНГ. Сближение законодательства стран СНГ в процессе формирования общего культурного пространства получило свое развитие более чем в тридцати модельных законодательных актах[30]. Особое место среди модельных актов занимает модельный Кодекс о культуре для стран СНГ[31] (далее — Кодекс о культуре СНГ). Необходимость Кодекса была продиктована наличием большого количества различных актов в сфере культуры, принятых в странах СНГ, уже апробированных на практике, что создало условия для кодификации законодательства о культуре.

В Кодексе о культуре СНГ представлены нормы, которые уже нашли применение на практике и носят стабильный характер, унифицирована и уточнена терминология. Кодекс состоит из общей и особенной частей, которые включают пять разделов.

Основными направлениями регулирования являются: государственные гарантии прав человека в области культуры; правовой статус творческих работников и творческих союзов; порядок создания и деятельности организаций культуры; правовой режим объектов материального и нематериального культурного наследия народов СНГ; регулирование международного сотрудничества в области культуры и др.

Отметим, что при рассмотрении перспектив гармонизации[32] законодательства в целях формирования общего культурного пространства стран СНГ не стои́т вопрос об абсолютном единообразии в правовом регулировании, поскольку гармонизация законодательства является разновидностью международно-договорной унификации права, основанной на обязательстве государства при разработке национального законодательства следовать определенному направлению правового регулирования, сформулированному в международном соглашении. Однако единство определяющих понятий является необходимой составляющей для формирования общего культурного пространства.

В связи с этим проанализируем некоторые основополагающие понятия на примере Кодекса о культуре для стран СНГ, Основ законодательства Российской Федерации о культуре и Кодекса Республики Беларусь о культуре.

Основополагающий термин «культура» в Кодексе о культуре СНГ определяется как «совокупность культурных ценностей и культурной деятельности». В российском законодательстве новое определение термина «культура» предполагалось ввести законопроектом «О культуре в Российской Федерации»[33], дискуссии о принятии которого продолжаются и по сей день. Необходимо согласиться, что «вариант систематизации законодательства о культуре на федеральном уровне видится возможным, учитывая, что, например, его удалось реализовать в Беларуси, правовая система которой во многом схожа с российской»[34]. Однако в на-

---

[27] Фонд является юридическим лицом по законодательству государства его местопребывания. Место пребывания Фонда — город Москва.

[28] Указ Президента РФ от 05.09.2022 № 611 «Об утверждении Концепции гуманитарной политики Российской Федерации за рубежом».

[29] «Под рекомендательным (модельным) законодательным актом понимается типовой законодательный акт, разрабатываемый институтами СНГ в сфере их общих интересов, имеющий рекомендательный характер и направляемый Верховным Советам (парламентам) государств — участников СНГ для использования его в их законодательной деятельности»: Протокол Консультативного совещания председателей Верховных Советов (парламентов) Содружества Независимых Государств от 27 марта 1992 г. «О подготовке рекомендательных законодательных актов (модельных) государств — участников Содружества независимых государств» // Информационный бюллетень Межпарламентской Ассамблеи государств — участников СНГ. 1992. № 1. С. 76.

[30] Особо необходимо отметить в этой связи модельный Библиотечный кодекс для государств — участников СНГ, модельный закон «О культуре», «Модельный закон о творческих работниках и творческих союзах», «Конвенцию о сохранении объектов культурного наследия государств — участников СНГ.

[31] Постановление № 47-5 Межпарламентской Ассамблеи государств — участников СНГ «Межкультурный диалог стран Содружества: состояние, перспективы и правовое обеспечение» (вместе с Модельным кодексом о культуре). Принято в г. Санкт-Петербурге 13.04.2018.

[32] Н.Г. Доронина определяет гармонизацию права в качестве одного из методов унификации права. Сама же унификация определяется как гармоничное взаимодействие национальных правовых систем.

[33] В декабре 2017 года президент Российской Федерации Владимир Путин, выступая на заседании Совета по культуре и искусству, предложил членам совета, деятелям культуры и представителям профильных ведомств принять активное участие в работе над новым законом. Однако работа над законопроектом «О культуре в Российской Федерации» на сегодняшний день остается замороженной.

[34] Научные концепции развития российского законодательства : монография / В.Р. Авхадеев, Е.Г. Азарова, Л.В. Андриченко и др.; под ред. Т.Я. Хабриевой, Ю.А. Тихомирова; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. 8-е изд., перераб. и доп. М. : Норма, 2024.

стоящее время вопросы в сфере культуры регулируют принятые еще в 1992 году Основы законодательства о культуре (далее Основы)[35], а также ряд федеральных законов[36] и Указов Президента РФ[37].

В Основах определение термина «культура» не даётся. В Основах государственной культурной политики[38] под термином «культура» понимается совокупность

- формальных и неформальных институтов,
- явлений и факторов, влияющих на сохранение, производство, трансляцию и распространение духовных ценностей.

Анализируя данное определение культуры, следует вспомнить цитату из книги академика Д.С. Лихачёва о том, что «культура — это огромное целостное явление, которое делает людей, населяющих определенное пространство, из просто населения — народом, нацией»[39].

Стоит усомниться, что определение, в котором под культурой понимается совокупность формальных и неформальных институтов, можно считать соответствующим современным реалиям, поскольку такое определение является абстрактным и требующим корректировки, особенно учитывая то обстоятельство, что в настоящее время культура возведена в «ранг национальной ценности»[40].

На данное обстоятельство обращает внимание и В.Ю. Лукьянова, указывая, что «конституционная поправка в части культуры и принимающиеся законы, вносимые законопроекты отражают общую тенденцию усиления и укрепления институтов и инструментов сохранения и развития культуры как ценностного наследия»[41].

Вышесказанное подчёркивает необходимость комплексного изменения законодательства о культуре Российской Федерации, и, безусловно, начинать надо с гармонизации ключевых понятий.

Например, в Кодексе Республики Беларусь (далее Кодекс РБ) о культуре от 20 июля 2016 года № 413-З культура определяется именно как культурное наследие и культурная деятельность, где культурное наследие представлено как совокупность культурных ценностей. Культурные ценности Кодекс РБ определяет как предметы материального мира, а также нематериальные ценности, «созданные или преобразованные человеком или тесно связанные с его деятельностью материальные объекты и нематериальные проявления творчества человека, имеющие историческое, художественное, научное или иное значение».

Безусловно, такое определение культуры является более целостным, позволяющем говорить о культуре как о наследии ценностей конкретного культурного пространства.

Основы также дают более узкое определение понятия «культурная деятельность» по сравнению с Кодексом о культуре СНГ, определяя культурную деятельность как деятельность по сохранению, созданию, распространению и освоению культурных ценностей. Кодексом о культуре СНГ понятие «культурная деятельность» определяется как деятельность не только по сохранению, созданию, распространению и освоению культурных ценностей, но и по предоставлению культурных благ[42]. Различны и определения понятий «культурные ценности». В Кодексе о культуре СНГ в сравнении с Основами появляется уточнение, что культурные ценности — это объекты материальной[43] и нематериальной культуры, а также нравственные и эстетические идеалы, нормы и образцы поведения, языки, диалекты и говоры, национальные традиции и обычаи.

Понятие нематериального культурного наследия было определено в Модельном законе об охране нематериального культурного наследия 2013 г.[44] Под нематериальным культурным наследием понимается совокупность духовных, интеллектуальных и нравственно-этических ценностей, являющихся отражением культурной и национальной самобытности общества, которые охватывают образ жизни, традиции и формы их выражения[45].

---

[35] Основы законодательства Российской Федерации о культуре (утв. ВС РФ 09.10.1992 № 3612-1).

[36] Закон Российской Федерации от 15 апреля 1993 г. № 4804-1 «О ввозе и вывозе культурных ценностей», Федеральный закон от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле», Федеральный закон от 26 мая 1996 г. № 54-ФЗ «О Музейном фонде Российской Федерации и музеях в Российской Федерации», Федеральный закон от 22 августа 1996 г. № 126-ФЗ «О государственной поддержке кинематографии Российской Федерации», Федеральный закон от 6 января 1999 г. № 7-ФЗ «О народных художественных промыслах», Федеральный закон от 25 июня 2002 г. № 73-ФЗ «Об объектах культурного наследия (памятниках истории и культуры) народов Российской Федерации».

[37] См. например, Указ Президента РФ от 24.12.2014 № 808 «Об утверждении Основ государственной культурной политики», Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».

[38] Указ Президента РФ от 24.12.2014 № 808 «Об утверждении Основ государственной культурной политики».

[39] Лихачёв Д.С. Русская культура. СПб. : Искусство, 2007.

[40] Хабриева Т.Я., Клишас А.А. Тематический комментарий к Закону Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти». М. : Норма, ИНФРА-М, 2020.

[41] См.: Лукьянова В.Ю. Новый концепт соразмерности универсальных и национальных ценностей в российском законодательстве // Журнал российского права. 2022. № 9. С. 53—69.

[42] Культурные блага определяются как товары и услуги, предоставляемые физическими и юридическими лицами для удовлетворения культурных потребностей граждан и общества в целом.

[43] Объекты материальной культуры — имеющие историко-культурную значимость здания, сооружения и предметы, уникальные в историко-культурном отношении территории, объекты и т. д.

[44] Постановление № 39-17 Межпарламентской Ассамблеи государств — участников СНГ «О модельном законе «Об охране нематериального культурного наследия» применяется в части, не противоречащей модельному Кодексу о культуре от 13.04.2018. Принято в г. Санкт-Петербурге 29.11.2013.

[45] Включая язык, нормы и правила поведения, верования, обряды, обычаи, празднества, фольклор, технологии изготовления предметов народного декоративно-прикладного искусства, музыкальных инструментов, предметов быта и народные художественные каноны, реализующиеся в исторически сложившихся сюжетах и образах и стилистике их воплощения.

В российском законодательстве до принятия Федерального закона № 402-ФЗ[46] (далее — Закон о НЭД) категория «нематериальное наследие» не имела легитимации. В Основах используется только термин «культурное наследие народов Российской Федерации»[47]. Кроме того, в Законе о НЭД используется не термин «нематериальное культурное наследие»[48], который является признанным в международных правовых актах[49], а термин «нематериальное этнокультурное достояние».

Рассматривая роль модельного законодательства о культуре стран СНГ, нужно согласиться, что, хотя модельное законодательство не является обязательным для стран СНГ, но способно «оказывать унифицирующее влияние на развитие законодательства государств в соответствующей сфере»[50].

Пора навести здесь соответствующий нашему времени порядок, поскольку факт отсутствия единого определения основополагающих понятий «культура», «культурные ценности», «культурные блага», «нематериальное культурное наследие» и пр. позволяет лишь констатировать, что страны СНГ только в середине пути в части становления общего культурного пространства. Представляется, что упомянутое модельное законодательство может быть сформировано только при условии устранения всех препятствующих этому правовых факторов.

К таким, очевидно, относятся: коллизии между внутригосударственными правовыми системами и законодательством, действующим в разных странах СНГ в сфере культуры, а также остающиеся несоответствия внутренних правовых механизмов этих стран, регулирующих отношения в области культуры, и международно-правовыми инструментариями, функционирующими там же и принятыми как на субрегиональном и региональном, так и на универсальном уровнях.

Даже в том случае, если последние из упомянутых несоответствий международного права и внутригосударственного законодательства заинтересованных в этом государств в целом и в основной своей части будут или уже устранены, то модельное законодательство, которое является базисом общего культурного пространства стран СНГ, все равно не сможет эффективно функционировать из-за разной степени трансформации, инкорпорации или рецепции международного права в их внутригосударственные правовые системы и законодательства. В этой связи требуется гармонизация и, в конечном счете, унификация законодательств стран СНГ в рассматриваемой сфере.

Соотношение понятия общего культурного пространства стран СНГ с правовым и виртуальным пространством

Учёные Института законодательства и сравнительного правоведения при Правительстве Российской Федерации неоднократно обращались к вопросам научного понимания «пространства»[51]. Как отмечает профессор Ю.А. Тихомиров, правовое пространство различается «по сферам деятельности»[52], в том числе и культурное правовое пространство. По мнению автора, культурное пространство — это прежде всего пространство для реализации культурных прав человека; более подробно этот вопрос рассмотрим с помощью кругов Эйлера. Учёные выделяют также:

а) территориальные,

б) межтерриториальные,

в) экстерриториальные,

г) виртуальные пространства[53].

В контексте развития новых информационных технологий понятие «культурное пространство» приобретает новый смысл, поскольку включает в себя и ту часть, которую принято называть «виртуальное пространство»[54], при этом «информация позволяет

---

[46] Федеральный закон от 20 октября 2022 г. № 402-ФЗ «О нематериальном этнокультурном достоянии Российской Федерации».

[47] Материальные и духовные ценности, созданные в прошлом, а также памятники и историко-культурные территории и объекты, значимые для сохранения и развития самобытности Российской Федерации и всех ее народов, их вклада в мировую цивилизацию

[48] Конвенция ООН об охране нематериального культурного наследия 2003 г.

[49] URL: https://ru.unesco.org/ (дата обращения: 29.11.2023).

[50] Андриченко Л.В. Проблемы правового обеспечения сохранения культурного наследия коренных малочисленных народов: международный и национальный аспекты // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 4. С. 17—32.

[51] См.: Глобализация и интеграционные процессы в Азиатско-Тихоокеанском регионе (правовое и экономическое исследование) : монография / И.И. Шувалов, Т.Я. Хабриева, А.Я. Капустин и др.; под редакцией Т.Я. Хабриевой. М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2014; Правовое пространство и человек : монография / Отв. редакторы: Ю.А. Тихомиров, Е.В. Пуляева, Н.И. Хлуденева. М., 2012; Тихомиров Ю.А. Правовое пространство. Равновесие и отклонения // Право. 2017. № 4; Тихомиров Ю.А., Головина А.А., Плюгина И.В. и др. Правовое пространство: границы и динамика : монография / Отв. ред. Ю.А. Тихомиров. М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации : ИНФРА-М, 2019. С. 15.

[52] Авторы выделяют а) экономическое правовое пространство; б) социальное правовое пространство; в) образовательное правовое пространство; г) культурное правовое пространство; д) экономическое правовое пространство; е) политико-правовое пространство. См.: Тихомиров Ю.А., Головина А.А., Плюгина И.В. и др. Правовое пространство: границы и динамика : монография / Отв. ред. Ю.А. Тихомиров. М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации : ИНФРА-М, 2019.

[53] Виртуальное пространство, по определению эксперта ЮНЕСКО по правовым аспектам информационного общества Т. Фуентеса-Камачо, — это новая человеческая и технологическая среда, которая «включает в себя как людей всех стран, культур, языков, возрастов и профессий, поставляющих и обращающихся за информацией, так и всемирную сеть компьютеров, взаимосвязанных средствами коммуникационных инфраструктур, которые обеспечивают цифровую обработку и передачу информации».

[54] Например, по мнению профессора Ю.А. Тихомирова, «виртуальное пространство — не только государственные территории и международные зоны, но и предполагаемые и воображаемые обстоятельства, которые могут иметь место в будущем. Виртуальное пространство связано с правовым пространством и отражает регулирование не только в рамках государственной территории, но и за ее пределами»: Тихомиров Ю.А. Креативные регуляторы в правовом и виртуальном пространстве // Журнал российского права. 2023. № 3. С. 5—16.

формировать виртуальное пространство, где почти не видны правовые границы»[55].

Однако на сегодняшний день «виртуальное пространство представляет только дополнительные возможности для социальных коммуникаций, оставаясь в сфере общественных отношений, требующих актуализации правового регулирования»[56].

Рассматривая соотношение этих понятий с помощью кругов Эйлера, — большим кругом, по нашему мнению, будет понятие «правовое пространство». Правовое пространство, являясь особой сферой «правового регулирования территориального, межтерриториального и надтерриториального характера, формируемого с помощью системы национально-правовых и международно-правовых регуляторов и структурных институтов»[57], должно полностью включать понятие «культурное пространство». Между тем нельзя не согласиться, что «проведение цифровизации расширяет границы и объем правового регулирования внутри и вне государства»[58], поскольку появляется и так называемое виртуальное пространство, что ещё более актуализирует проблему гармонизации законодательства стран СНГ.

Цифровизация в сфере культуры позволяет гражданам стран СНГ удаленно участвовать в различных культурных мероприятиях, проводимых на пространстве СНГ. В Стратегии 2016 г.[59] в качестве основных направлений сотрудничества стран СНГ в построении и развитии информационного общества были определены

1) гармонизация законодательства,

2) формирование общего информационного пространства,

3) развитие экономической, социально-политической, культурной и духовной сфер жизни общества, и др.

Отдельное внимание в Стратегии 2016 г. уделено формированию электронной культуры, что предполагает увеличение проникновения объектов науки, культуры и искусства в повседневную жизнь граждан за счет оцифровки данных, развития средств обработки и предоставления удаленного доступа к цифровой информации. В этой связи особый акцент делается на создании национальных интернет-порталов о культуре, истории и науке. Например, в Российской Федерации во исполнение Указа Президента о национальных целях и стратегических задачах Министерством культуры разработан паспорт Национального проекта «Культура», который включает в себя три федеральных проекта: «Культурная среда», «Творческие люди», «Цифровая культура».

Целью данного национального проекта является создание единого информационного пространства в сфере культуры. Для оценки результатов достижения национальной цели развития Российской Федерации «Возможности для самореализации и развития талантов», определенной Указом Президента Российской Федерации от 22.07.2020 № 474 рассчитываются показатели национального проекта «Культура», например: целевой показатель «Число обращений к цифровым ресурсам», который определяется по данным счетчика «Цифровая культура». Так, число обращений к цифровым ресурсам в сфере культуры в 2022 году составило 264,23 млн[60].

Таким образом, изменяется формат приобщения к культурным ценностям, появляются так называемые цифровые права, например, право на доступ к цифровым информационным ресурсам о культуре[61], а также новые понятия, например «цифровая культура», «право владения уникальным цифровым объектом в сфере культуры», что требует своего правового регулирования и механизмов защиты «цифровых прав».

И здесь уместно вспомнить, что ещё в уставе СНГ (в статье 33) было регламентировано создание Комиссии по правам человека стран СНГ (далее — Комиссия), которая является консультативным органом СНГ. Основной задачей деятельности Комиссии является улучшение защиты прав человека на пространстве СНГ, а также разработка предложений по совершенствованию законодательства в области защиты прав человека, в том числе и с учётом культурной специфики стран СНГ. Предполагалось, что Комиссия будет наблюдать за международными обязательствами, принятыми на себя странами СНГ и содействовать диалогу граждан и государств.

Однако начало работы Комиссии по правам человека СНГ стало возможным после подписания в октябре 2022 г. в Астане[62] протокола о внесении изменений в конвенцию СНГ о правах и основных свободах человека, который изменил порядок утверждения положения о Комиссии[63].

---

[55] Тихомиров Ю.А., Головина А.А., Плюгина И.В. и др. Правовое пространство: границы и динамика : монография / Отв. ред. Ю.А. Тихомиров. М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации : ИНФРА-М, 2019. С. 13.

[56] Синицын С.А. Личные неимущественные права и безопасность человека в виртуальном пространстве // Журнал зарубежного законодательства и сравнительного правоведения. 2023. № 1. С. 13—24.

[57] Тихомиров Ю.А. Правовой суверенитет: сферы и гарантии // Журнал российского права. 2013. № 3 (195). С. 5—20.

[58] Тихомиров Ю.А. Креативные регуляторы в правовом и виртуальном пространстве // Журнал российского права. 2023. № 3. С. 5—16.

[59] Решение Совета глав правительств СНГ «О Стратегии сотрудничества государств — участников СНГ в построении и развитии информационного общества на период до 2025 года и Плане действий по ее реализации». Принято в г. Минске 28.10.2016.

[60] Распоряжение Правительства РФ от 11.12.2023 № 3550-р «Об утверждении стратегического направления в области цифровой трансформации отрасли культуры Российской Федерации на период до 2030 года».

[61] Автор уже обращала внимание на то, что виртуальное пространство, являясь составной частью культурного пространства, меняет формат приобщения к культурным ценностям, появляются так называемые цифровые права: право «на доступ, использование, создание и публикацию цифровых произведений», право на доступ к цифровым информационным ресурсам о культуре, а также право на использование NFT-токенов как аналога цифрового сертификата, который закрепляет право владения уникальным цифровым объектом в сфере культуры. См. Савченко Е.А. Культурные права человека в условиях цифровизации // Вестник Томского государственного университета. Право. 2023. № 49. С. 151—164.

[62] Подписано главами государств Белоруссии, Киргизии, Таджикистана и России.

[63] Изначально положение о Комиссии по правам человека СНГ было включено в Конвенцию СНГ о правах и основных свободах человека (статья 34). Поскольку 4 октября 2022 года Совет глав го-

В состав Комиссии по правам человека СНГ в настоящее время входят представители Армении, Белоруссии, Казахстана, Киргизии, России, Таджикистана и Узбекистана.

Возникновение так называемых цифровых прав, в том числе и в сфере культуры, делает особый акцент на актуализации деятельности Комиссии, поскольку «полноценное обеспечение прав человека возможно только в рамках определенного общества, конкретного культурного пространства, с которым эта личность идентифицируется»[64].

Однако мнения учёных по вопросу «цифровых прав» разнятся. Например, как отмечает Н.В. Варламова[65], «свобода функционирования в интернет-пространстве не является новым самостоятельным правом человека, а представляет собой реализацию традиционных прав в новых (виртуальных, цифровых) условиях» при этом, по её мнению, «в качестве нового права может рассматриваться только право на сам доступ к Интернету». Позволим себе не согласиться с такой постановкой вопроса, поскольку, по мнению автора, можно иметь доступ к Интернету, но не иметь информации, например, о цифровых информационных ресурсах о культуре, которые и были созданы в целях координации действий органов исполнительной власти, государственных, коммерческих и некоммерческих организаций по реализации конституционных прав граждан Российской Федерации по доступу к культурному наследию и участию в культурной жизни страны. Здесь необходимо согласиться с Э.В. Талапиной, которая выделяет «в праве на доступ к Интернету, как минимум, (1) право на подключение к Интернету, в рамках которого Интернет рассматривается как услуга, и (2) право на доступ к информации в Интернете»[66].

По мнению автора, право на доступ к информации в Интернете включает и «цифровые права» в сфере культуры. В целях повышения популяризации и доступности культурных ценностей как для граждан Российской Федерации, так и для граждан других стран, в том числе и стран СНГ, было утверждено стратегическое направление в области цифровой трансформации отрасли культуры Российской Федерации до 2030 года (далее — стратегическое направление)[67]. Стратегическое направление включает в себя шесть проектов, которые должны помочь инновационному развитию сферы культуры, что, безусловно, позволит пользоваться данными сервисами и гражданам других стран СНГ.

Аналогичные национальные проекты есть и в других странах СНГ[68]. Например, в Казахстане утверждён национальный проект «Национальное духовное возрождение», направленный на повышение уровня культуры, образования и национального духа казахстанского общества.

Основная цель проекта — сохранение национально-культурной самобытности и популяризация культурных продуктов, реализация художественного и творческого потенциала каждого казахстанца путем повышения их качества и разнообразия, сохранение национального кода и обновление культурной самобытности, повышение культурного уровня общества путем продвижения национальных ценностей.

Национальный проект реализуется по трем направлениям:

1) направление продвижения ценностей «духовного возрождения» и развития государственного языка — повышение интеллектуального потенциала страны и статуса государственного языка;

2) направление «Дух страны» включает в себя мероприятия по повышению доступности услуг в сфере культуры, а также продвижению отечественной культурной продукции, в том числе за рубежом;

3) направление «Поколения независимости» направлено на создание новых возможностей для молодежи.

Выводы

Формирование общего культурного пространства стран СНГ является одним из приоритетов гуманитарной политики Российской Федерации. Обмен опытом и совместные мероприятия в сфере культуры позволяют повышать уровень правосознания граждан стран СНГ, а также находить приемлемые решения и преодолевать возможные естественные разногласия. Это обогащает культурологический уровень взаимодействия стран СНГ и способствует укреплению их национальных правовых систем. Запрос на сохранение и защиту традиционных ценностей в странах СНГ становится всё более актуальным, что требует активизации деятельности Комиссии по правам человека стран СНГ, а также Совета по культурному сотрудничеству и Совета по гуманитарному сотрудничеству стран СНГ. Основными инструментами формирования общего культурного пространства стран СНГ являются различные формы культурного обмена, при этом виртуальное пространство, являясь составной частью культурного пространства, меняет формат приобщения к культурным ценностям, появляются так называемые цифровые права. Особо необходимо обратить внимание на возникающее право на доступ к цифровым информационным ресурсам

государств СНГ утвердил новое Положение о Комиссии по правам человека СНГ, статья 34 была исключена, что позволило расширить состав Комиссии за счет государств, не являющихся участниками Конвенции (Республика Армения, Республика Казахстан, Республика Узбекистан).

[64] Синюков В.Н. Личность в российской правовой системе: поиск новых подходов // Журнал российского права. 2023. № 5. С. 75—85.

[65] Варламова Н.В. Цифровые права — новое поколение прав человека? // Труды Института государства и права РАН. 2019. Т. 14. № 4. С. 9—46.

[66] Талапина Э.В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. 2019. Т. 14. № 3. С. 122—146.

[67] Распоряжение Правительства РФ от 11.12.2023 № 3550-р «Об утверждении стратегического направления в области цифровой трансформации отрасли культуры Российской Федерации на период до 2030 года».

[68] Перечень национальных проектов в соответствии с Указом Президента К.К. Токаева № 67 от 7 октября 2021 г.

о культуре, поскольку фактически во всех странах СНГ реализуются программы по созданию национальных интернет-порталов о культуре. Однако без гарантированного права доступности этих информационных ресурсов цифровизация просто теряет смысл [13]. Поэтому можно согласиться с необходимостью уточнения «права на доступ к культурным ценностям, в том числе благам, услугам, распространяемым (предоставляемым) посредством цифровых площадок» [4].

На активизацию развития общего культурного пространства указывается и в Стратегии сотрудничества государств — участников СНГ в построении и развитии информационного общества на период до 2025 года, что ещё более актуализирует проблему гармонизации законодательства стран СНГ.

Автор выражает благодарность за помощь в подготовке статьи профессору Юрию Александровичу Тихомирову и ведущему научному сотруднику отдела конституционного права Института законодательства и сравнительного правоведения при Правительстве Российской Федерации Сергею Витальевичу Шульге.

Литература

1. Синюков В.Н. Личность в российской правовой системе: поиск новых подходов // Журнал российского права. 2023. № 5. С. 75—85.
2. Талапина Э.В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. 2019. № 3.
3. Михеева И.В., Логинова А.С. Вариативность нормативного закрепления понятия «культурные ценности» в законодательстве ЕАЭС // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 1. С. 69—74.
4. Научные концепции развития российского законодательства : монография / В.Р. Авхадеев, Е.Г. Азарова, Л.В. Андриченко и др.; под ред. Т.Я. Хабриевой, Ю.А. Тихомирова; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. 8-е изд., перераб. и доп. М. : Норма, 2024.
5. Дугужева М.Х., Симаева Е.П. Трансформация законодательства о культуре в условиях цифровизации // Вестник Пермского университета. Юридические науки. 2019. Вып. 44. С. 193.
6. Хабриева Т.Я., Клишас А.А. Тематический комментарий к Закону Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти». М. : Норма, ИНФРА-М, 2020.
7. Лукьянова В.Ю. Новый концепт соразмерности универсальных и национальных ценностей в российском законодательстве // Журнал российского права. 2022. № 9. С. 53—69.
8. Андриченко Л.В. Проблемы правового обеспечения сохранения культурного наследия коренных малочисленных народов: международный и национальный аспекты // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 4. С. 17—32.
9. Тихомиров Ю.А., Головина А.А., Плюгина И.В. и др. Правовое пространство: границы и динамика : монография / Отв. ред. Ю.А. Тихомиров. М., 2019. С. 15.
10. Синицын С.А. Личные неимущественные права и безопасность человека в виртуальном пространстве // Журнал зарубежного законодательства и сравнительного правоведения. 2023. № 1. С. 13—24.
11. Тихомиров Ю.А. Креативные регуляторы в правовом и виртуальном пространстве // Журнал российского права. 2023. № 3. С. 5—16.
12. Шульга С.В. Международно-правовое обеспечение межэтнического и межкультурного диалога на примере Содружества Независимых Государств // Социальная справедливость и право: к упрочению мира и предотвращению кризисов : материалы международной научно-практической конференции, Московский гуманитарный университет, 17—18 февраля 2023 г. М. : МосГУ, 2023. 356 с. С. 33—38.
13. Савченко Е.А. Культурные права человека в условиях цифровизации // Вестник Томского государственного университета. Право. 2023. № 49. С. 151—164.

A COMMON CULTURAL SPACE OF CIS COUNTRIES: PROSPECTS FOR HARMONISATION OF LEGISLATION

Elena Savchenko, *Ph.D. (Law), Researcher at the Unit of Social Legislation of the Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, Russian Federation. ORCID: 0000-0001-8346-8829.*
E-mail: *elen_savchenko@bk.ru*

Keywords: *virtual space, humanitarian policy, institutional foundations, digital rights.*

Abstract

Purpose of the work: addressing the institutional foundations for cultural co-operation of the CIS countries, determining the prospects for harmonisation of legislation with a view to form a common cultural space of the CIS countries, and addressing the correspondence between the concept of the common cultural space of the CIS countries and their legal and virtual space.

Methods used in the study: general scientific and traditional methods of legal science.

Study findings: a conclusion is made that the main instruments for forming the common cultural space of the CIS countries are various forms of cultural exchange, and such a part of this cultural space as the virtual space changes the format of exposure to cultural values: the so-called digital rights are emerging in the sphere of culture. Therefore, it is necessary to state that the problem of harmonisation of legislation of the CIS countries is at present especially topical. The emphasis in the paper is put on that the main line of harmonisation of legislation of the CIS countries is legal regulation of activities in the virtual space from the viewpoint of exercising the right to access to cultural values over the whole CIS community.

Practical importance of the study: for the first time, the need is stated for legal regulation of guarantees for the right to access to digital cultural information resources because all CIS countries are implementing programmes for creating national web portals about culture. The author's position on the correspondence between the legal, cultural and virtual space is presented.

References

1. Siniukov V.N. Lichnost' v rossiiskoi pravovoi sisteme: poisk novykh podkhodov. Zhurnal rossiiskogo prava, 2023, No. 5, pp. 75–85.
2. Talapina E.V. Evoliutsiia prav cheloveka v tsifrovuiu epokhu. Trudy Instituta gosudarstva i prava RAN, 2019, No. 3.
3. Mikheeva I.V., Loginova A.S. Variativnost' normativnogo zakrepleniia poniatiia "kul'turnye tsennosti" v zakonodatel'stve EAES. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia, 2019, No. 1, pp. 69–74.
4. Nauchnye kontseptsii razvitiia rossiiskogo zakonodatel'stva : monografiia. V.R. Avkhadeev, E.G. Azarova, L.V. Andrichenko i dr.; pod red. T.Ia. Khabrievoi, Iu.A. Tikhomirova; Institut zakonodatel'stva i sravnitel'nogo pravovedeniia pri Pravitel'stve Rossiiskoi Federatsii. 8-e izd., pererab. i dop. M. : Norma, 2024.
5. Duguzheva M.Kh., Simaeva E.P. Transformatsiia zakonodatel'stva o kul'ture v usloviiakh tsifrovizatsii. Vestnik Permskogo universiteta, Iuridicheskie nauki, 2019, vyp. 44, p. 193.
6. Khabrieva T.Ia., Klishas A.A. Tematicheskii kommentarii k Zakonu Rossiiskoi Federatsii o popravke k Konstitutsii Rossiiskoi Federatsii ot 14 marta 2020 g. No. 1-FKZ "O sovershenstvovanii regulirovaniia otdel'nykh voprosov organizatsii i funktsionirovaniia publichnoi vlasti". M. : Norma, INFRA-M, 2020.
7. Luk'ianova V.Iu. Novyi kontsept sorazmernosti universal'nykh i natsional'nykh tsennostei v rossiiskom zakonodatel'stve. Zhurnal rossiiskogo prava, 2022, No. 9, pp. 53–69.
8. Andrichenko L.V. Problemy pravovogo obespecheniia sokhraneniia kul'turnogo naslediia korennykh malochislennykh narodov: mezhdunarodnyi i natsional'nyi aspekty. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia, 2019, No. 4, pp. 17–32.
9. Tikhomirov Iu.A., Golovina A.A., Pliugina I.V. i dr. Pravovoe prostranstvo: granitsy i dinamika : monografiia. Otv. red. Iu.A. Tikhomirov. M., 2019, p. 15.
10. Sinitsyn S.A. Lichnye neimushchestvennye prava i bezopasnost' cheloveka v virtual'nom prostranstve. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia, 2023, No. 1, pp. 13–24.
11. Tikhomirov Iu.A. Kreativnye reguliatory v pravovom i virtual'nom prostranstve. Zhurnal rossiiskogo prava, 2023, No. 3, pp. 5–16.
12. Shul'ga S.V. Mezhdunarodno-pravovoe obespechenie mezhetnicheskogo i mezhkul'turnogo dialoga na primere Sodruzhestva Nezavisimykh Gosudarstv. Sotsial'naia spravedlivost' i pravo: k uprocheniiu mira i predotvrashcheniiu krizisov : materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii, Moskovskii gumanitarnyi universitet, 17–18 fevralia 2023 g. M. : MosGU, 2023. 356 pp., pp. 33–38.
13. Savchenko E.A. Kul'turnye prava cheloveka v usloviiakh tsifrovizatsii. Vestnik Tomskogo gosudarstvennogo universiteta. Pravo, 2023, No. 49, pp. 151–164.

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ В СИСТЕМЕ МЕР ПРОФИЛАКТИКИ РАСПРОСТРАНЕНИЯ ИДЕОЛОГИИ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

Атагимова Э.И.[1]

Ключевые слова: *основы конституционного строя, терроризм, экстремизм, национальная безопасность, идеология, сознание, молодежь, правосознание, информационное пространство, информационная грамотность.*

Аннотация

В статье затронуты проблемные вопросы популяризации идеологии экстремизма и терроризма в молодежной среде посредством информационного пространства.

Методы: использованы методы анализа и синтеза, позволившие на теоретическом уровне обосновать предложения по повышению эффективности мер профилактики терроризма и экстремизма в молодежной среде, изучить и выявить особенности организационной работы в сфере формирования антитеррористического сознания.

Полученные результаты: обосновывается вывод, что формирование информационной грамотности молодого поколения выступает важным средством профилактики преступлений террористического характера и экстремистской направленности, совершаемых представителями молодого поколения. Сформулированы и обоснованы предложения по повышению эффективности мер, направленных на формирование антитеррористического сознания у молодежи.

Практическая значимость исследования: на основе сформулированных предложений возможно дальнейшее совершенствование профилактической деятельности в сфере распространения идеологии терроризма и экстремизма.

DOI:10.21681/1994-1404-2024-1-50-57

Введение

Распространение идеологии терроризма и экстремизма является одной из самых острых проблем для любого суверенного государства. Совершенно справедливо отмечено в Стратегии национальной безопасности Российской Федерации, что происходящие в современном мире изменения затрагивают не только межгосударственные отношения, но и общечеловеческие ценности. Достигнув высокого уровня социально-экономического и технологического развития, человечество столкнулось с угрозой утраты традиционных духовно-нравственных ориентиров и устойчивых моральных принципов. Насаждение чуждых идеалов и ценностей, осуществление без учета исторических традиций и опыта предшествующих поколений реформ в области образования, науки, культуры, религии, языка и информационной деятельности приводят к усилению разобщенности и поляризации национальных обществ, разрушают фундамент культурного суверенитета, подрывают основы политической стабильности и государственности. Пересмотр базовых норм морали, психологическое манипулирование наносят непоправимый ущерб нравственному здоровью человека, поощряют деструктивное поведение, формируют условия для саморазрушения общества. Увеличивается разрыв между поколениями. Одновременно нарастают проявления агрессивного национализма, ксенофобии, религиозного экстремизма и терроризма[2]. Предупреждение проявлений радикализма и профилактика экстремистских проявлений среди несовершеннолетних и молодежи обозначены в стратегическом документе в качестве основных задач, реализация которых способствует достижению целей обеспечения государственной и общественной безопасности.

В настоящее время действует обширный перечень нормативных правовых актов, регламентирующих во-

[2] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 03.06.2022).

[1] ***Атагимова Эльмира Исамудиновна****, кандидат юридических наук, Аппарат Государственной Думы Федерального Собрания Российской Федерации, г. Москва, Российская Федерация.*

E-mail: atagimovaei@duma.gov.ru

просы противодействия экстремизму и терроризму. Вместе с тем новые вызовы и угрозы, стремительное развитие информационно-коммуникационных технологий и широкое использование возможностей медиапространства обусловливают необходимость дальнейшего совершенствования правовой основы противодействия экстремизму и терроризму. Законодателем в течение последних лет внесено большое количество изменений и дополнений в различные законы и подзаконные нормативные правовые акты в части расширения перечня преступлений террористического характера и экстремистской направленности, а также ужесточения наказаний за такие преступления. В частности, приняты поправки, расширяющие перечень экстремистских материалов, направленные на оптимизацию порядка ведения перечней общественных, религиозных и иных объединений и организаций, деятельность которых запрещена или приостановлена в связи с ведением ими экстремистской деятельности, об ужесточении уголовной ответственности за диверсии и терроризм; Уголовный кодекс РФ дополнен новой статьей 217.3, предусматривающей ответственность за нарушение требований к антитеррористической защищенности объектов.

Многогранность, нестабильность, изменчивость и усложнение форм терроризма [13] и наметившаяся негативная динамика роста количества таких преступлений[3] актуализировали вопросы противодействия терроризму как общественно опасному криминальному проявлению.

По данным статистики МВД РФ в 2021 году за период январь — декабрь было зарегистрировано 2136 преступлений террористического характера, за аналогичный период 2022 года — 2233, в 2023 году — 2382.

Стоит отметить, что в 2023 г. было зарегистрировано рекордное количество террористических актов (ст. 205 УК РФ) — 410, что на 222,8% больше, чем за аналогичный период 2022 г. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ) — 548 преступлений, что составило увеличение количества совершенных преступлений на 11,8% по сравнению с аналогичным периодом 2022 г.[4]

Призывы к жестокости и насилию, исходящие от людей с иной системой ценностей, оформлены в идеологию экстремизма и терроризма — ориентированную на агрессию, разрушение и уничтожение. Злободневность исследуемой проблемы обусловлена вовлечением в террористические группировки и экстремистские сообщества преимущественно молодежь, поскольку, как правильно отмечается в Стратегии противодействия экстремизму в Российской Федерации до 2025 года (утв. Указом Президента Российской Федерации от 29.05.2020 № 344), она более мобильна и легче поддается идеологическому и психологическому воздействию.

Результаты исследования

Информационное пространство Интернета является для экстремистских сообществ идеальным инструментом пропаганды преступных идей[5]. Создание коммуникативной платформы в медиапространстве с целью пропаганды идей радикального характера нередко приводит молодежь к включению в ряды террористических структур [8, с. 193—198]. Данный факт подтверждается и выводами ученых-юристов, исследующих данную проблематику, которые отмечают, что «молодежь традиционно является наиболее активной социально-демографической группой населения, реализующей свои активности во всех сферах жизни общества» [11]; молодые люди наиболее активно пользуется социальными сетями, создают страницы в социальных сетях и общаются в блогах, ищут новых знакомств, обмениваются информацией через сервисы сообщений, читают новости, смотрят ролики и выставляют свои, участвуют в сетевых играх и сообществах игроков и т. д. Интернет становится средой, которая влияет на их поведение, действия, знания и мнения, установки и ценностные ориентиры, поведенческие навыки.

В силу остроты восприятия объективной действительности и неспособности критически воспринимать поступающую информацию молодежь как социальная группа является наиболее уязвимой для внешнего воздействия и распространения идеологии терроризма [2, с. 5]. Именно в молодежной среде (от 15 до 35 лет), отмечают авторы, «происходит накопление протестного потенциала в самых различных формах, что приводит к возникновению ксенофобии, разжиганию межнациональной розни, религиозным конфликтам, а также к случаям доведения несовершеннолетних до суицида. Некоторые представители молодежи примыкают к неформальным объединениям террористической направленности, где принуждаются к совершению противоправных действий, способных причинить тяжкий вред здоровью и жизни граждан». Д.И. Аминов и Р.Э. Оганян для основной возрастной группы приобщения к деятельности экстремистской направленности определяют возраст от 14 до 25 лет — 92%, в том числе от 14 до 16 лет — 24%, от 16 до 18 лет — 37% [3, с. 61].

Наиболее опасным с точки зрения вхождения в поле экстремистской активности ряд авторов (А.А. Клейменов, А.И. Григорьева и Т.В. Дьячкова) считают возраст от 14 до 22 лет. Как отмечается учеными, в это время происходит наложение двух важнейших психологических и социальных факторов. В психологическом плане подростковый возраст и юность характеризуются развити-

[3] Состояние преступности в Российской Федерации за январь — декабрь 2023 года // URL: https://мвд.рф/reports/item/47055751 (дата обращения: 13.03.2024).

[4] Состояние преступности в Российской Федерации за январь — декабрь 2023 года // URL: https://мвд.рф/reports/item/47055751 (дата обращения: 13.03.2024).

[5] Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утверждена Указом Президента Российской Федерации от 29.05.2020 № 344) // СПС «КонсультантПлюс».

ем самосознания, обострением чувства справедливости, определением смысла и ценности жизни. Именно в это время подросток озабочен желанием найти свою группу, поиском собственной идентичности, которая формируется по самой примитивной схеме: «мы» — «они» [10].

Данные Национального антитеррористического комитета также подтверждают, что молодежь в возрасте от 15 до 25 лет легче вовлечь в террористическую деятельность. Распространение данной тенденции в молодежной среде обусловлено комплексным воздействием негативных социальных и психологических факторов на социально незрелую личность, которые усугубляются возрастной спецификой социального развития личности: обостренной страстью к общению с эффектом группирования; склонностью к самоутверждению, приводящему к рискованному поведению; стремлением к самостоятельности и отрыву от семьи (школы, вуза); преодолением зависимости от взрослых; подверженностью манипулятивному влиянию и некритическому восприятию негативной информации; ростом общественной активности личности, что сопровождается возникновением кризиса в формировании духовно-нравственного сознания, ценностей, идеалов, установок, мировоззрения, гражданских позиций личности.

В последние годы в информационном пространстве стала регулярно появляться информация о диверсиях на железных дорогах. В частности, в разных регионах России фиксировались случаи поджогов релейных шкафов, предназначенных для размещения в них аппаратуры системы железнодорожной автоматики и телемеханики, позволяющей следить за движением поездов и обеспечивать безопасность их следования на конкретных перегонах. По сообщениям средств массовой информации, поджоги осуществляются по прямому указанию специальных служб иностранных государств в целях нарушения функционирования российской транспортной (железнодорожной) инфраструктуры. Среди задержанных правоохранительными органами поджигателей иногда оказывались подростки в возрасте 14—15 лет, которые через Интернет получали задания от неких лиц совершить акт диверсии за соответствующее вознаграждение.

Международные террористические и экстремистские организации, навязывающие идеологию терроризма и экстремизма, проводят пропагандистскую работу, оказывая психологическое воздействие на молодое поколение [6, с. 29—37], вербуют российскую молодежь для вовлечения в противоправную деятельность. Идеологические террористические установки — это мощнейший инструмент, которые используют террористы с целью втягивания в свою разрушительную деятельность целые группы людей, слои населения, этносы [8, с. 193—198]. Как правило, террористические организации применяют различные способы распространения идеологии терроризма: семинары по вербовке лиц, печатные брошюры, книги, статьи и т. д. Следует отметить, что в современных условиях манипулирование молодежью осуществляется преимущественно посредством Интернета и социальных сетей, где международные террористические организации пропагандируют свою идеологию. Интернет используется террористическими организациями не только для распространения своей идеологии, но и для поиска источников финансирования, вербовки сторонников, подготовки и совершения террористических актов [11, с. 30—34].

Чаще всего объектом вербовщиков становятся лица молодого возраста: романтики, идеалисты, изгои и просто не адаптировавшиеся ко взрослой жизни ребята, которые не хотят мириться с окружающим их социальным неравенством.

Существует множество методов вербовки в террористические и экстремистские организации [18, с. 61]. Вербовка осуществляется как при помощи непосредственного (личного) контакта вербовщика с вербуемым (что происходит реже), так и дистанционного, когда вербовщик входит в контакт при помощи сети Интернет и мобильной связи.

Следует понимать, что вербовщик находится практически вне досягаемости от правоохранительных органов, так как вербовка в террористические и экстремистские организации обычно происходит с территории других стран, а различного рода виртуальные террористические и экстремистские сообщества вообще не привязаны к какой-либо территории.

Составляющим элементом системы привлечения новых адептов, проповедников, боевиков, смертников-шахидов является высокопрофессиональная работа специалистов-психологов, находящихся на службе в террористических и экстремистских организациях.

Подавляющее большинство методов вербовки направлены на то, чтобы контролировать сознание и внушить что-либо. Чаще всего жертвами вербовщиков оказываются молодые люди. Всё начинается с дружелюбного незнакомца, который просто хочет помочь. Психофизиологические особенности подростка (несформированность способности критически анализировать текущую ситуацию, внушаемость, отсутствие доверия мнению родителей, педагогов, старших, отсутствие жизненного опыта, отсутствие адекватной самооценки, наличие ситуаций заражения и т. д.), с одной стороны, и профессионализм вербовщика — с другой, не позволяют подростку выявить истинную цель нового «хорошего, понимающего его друга».

В качестве примера приведем одну из схем вербовки: *«На первом этапе наводчик вычисляет потенциальную жертву, выявляет проблемы у члена коллектива. Затем в работу включается мотиватор, который сначала давит на существующие проблемы, преувеличивает их, а потом показывает «выход» — «прекрасный мир» «Исламского государства». Мотиватор заставляет поверить «клиента», что он может сделать нечто очень важное, внести вклад в общее дело, направленное на «спасение» человечества. Как «вдруг»*

появляется «уникальная возможность» встретиться с «очень важным человеком». Тогда и появляется вербовщик, рассказывающий сказки из серии: «Мы тебя заметили, признали твои способности и готовы тебе поручить важное дело» [12].

Таким образом, попадая в неконтролируемое интернет-пространство, открывающее свободный доступ к обширным информационным ресурсам, подросток, как правильно отмечают исследователи, оказывается в ситуации, сопряженной с определенными рисками и угрозами [16, с. 65—73]. Интернет является «идеальной ареной для незаконной деятельности из-за недостаточного законодательного регулирования отношений в киберсети, беспрепятственного распространения потока бесплатной информации, легкого доступа в онлайн-пространство практически из любой точки мира» [4, с. 167—177]. Распространяемая в сети Интернет информация далеко не всегда является достоверной, актуальной, порой «вбрасывается» с целью создания социальной напряженности, формирования агрессивных настроений в обществе, разрушения духовно-нравственных установок и ценностей. Фейковая информация, распространяемая, как правило, для манипулирования общественным мнением [7, с. 449—465], может привести к массовым беспорядкам, создать реальную опасность жизни и здоровью граждан, угрозу общественной и государственной безопасности.

Интернет-пространство обеспечивает большой охват аудитории, высокую скорость распространения информации, а в случае блокировки и удаления запрещенного контента — возможность его быстрого воспроизводства через множество других удаленных ресурсов [17, с. 113—131]. Воздействие на сознание современной молодежи с применением новых методик аудиовизуального представления информации, помноженное на возможности социальных сетей, приводит к многократному увеличению негативного воздействия на подрастающее поколение [5, с. 180—186], что, в свою очередь, способствуют привыканию к насилию, ожесточению нравов, уничтожению моральных критериев, распространению криминальной субкультуры, пропагандирующей преступный образ жизни среди молодежи.

Влияние цифровых технологий на распространение экстремистской и террористической деятельности неоднократно отмечалось экспертами Совета Безопасности Российской Федерации. Так, в феврале 2022 г. на заседании секции Научного совета при Совете Безопасности по проблемам нейтрализации внутренних угроз национальной безопасности было подчеркнуто, что «активное использование цифровых технологий и информационно-коммуникационных систем экстремистскими и террористическими структурами порождает угрозообразующие факторы, негативно влияющие на состояние национальной безопасности»[6]. Ранее Секретарь Совета Безопасности России Н.П. Патрушев в своем выступлении акцентировал внимание на том, что именно молодежь в первую очередь попадает под удар информационной агрессии, чем обусловлена необходимость «не только оградить молодежь от влияния деструктивных течений и организаций, но и сформировать у молодых людей активную гражданскую позицию»[7], с чем сложно не согласиться.

В связи с этим в рамках реализации мер по противодействию идеологии терроризма и формированию антитеррористического сознания граждан Российской Федерации первостепенную важность имеет информационно-пропагандистская работа с населением, прежде всего молодежью, предполагающая целенаправленную и систематическую деятельность по развитию активной гражданской позиции, направленной на неприятие идеологии терроризма и привитию молодому поколению иммунитета к попыткам вовлечения в террористическую деятельность.

Согласимся с мнением, что «успешная профилактика терроризма и экстремизма в подростковой и молодежной среде невозможна без действующей системы научно-методического сопровождения этой работы и создания соответствующих психолого-педагогических условий в образовательных организациях» [11].

Вышеизложенное свидетельствует о необходимости создания условий для социализации молодежи в информационном обществе, обучению их самостоятельности действий в информационной среде, эффективному использованию своих возможностей, умению защитить себя от негативного воздействия экстремистских организаций и опытных вербовщиков. Полагаем, что информационная грамотность молодого поколения выступает важным и необходимым элементом системы мер противодействия идеологии экстремизма и терроризма в информационном пространстве.

В формировании информационной грамотности ключевая роль, несомненно, принадлежит системе образования. Современным образовательным стандартам в эпоху цифровой глобализации и информационных технологий необходимо учитывать особенности развития современного информационного общества, требующие новых способов формирования мышления, приспособленного к быстро меняющемуся информационному миру. Целесообразно рассмотреть вопросы внедрения в программу основного общего и высшего образования учебных или факультативных курсов по формированию информационной грамотности обучающегося как участника информационных отношений в сети Интернет.

[6] Эксперты Совета Безопасности рассмотрели вопросы противодействия экстремистской и террористической деятельности в условиях развития цифровых технологий. URL: http://www.scrf.gov.ru/news/allnews/3179/ (дата обращения: 13.08.2023).

[7] Выступление секретаря Совета безопасности России Н.П. Патрушева во время видео-конференц-совещания по вопросам безопасности в Уральском федеральном округе. URL: https://rg.ru/2020/04/10/v-sovbeze-prizvali-sozdat-novuiu-mediapolitiku-povospitaniiu-molodezhi.html (дата обращения: 03.06.2022).

В эпоху цифровых и информационных технологий, образовательным организациям необходимо учитывать особенности развития информационного общества, требующие новые способа формирования мышления, приспособленного к быстро меняющемуся информационному миру. В сложившейся ситуации без информационной грамотности несовершеннолетним сложно будет ориентироваться в повседневной жизни. Информационная грамотность молодого поколения формируется повседневно под влиянием средств массовой коммуникации, поэтому образовательным организациям следует организовывать, структурировать и направлять процесс формирования информационной грамотности обучающихся. Таким образом задача, которая стоит перед образовательными организациями — это научить обучающихся получать, оценивать и распространять информацию; они должны знать и понимать свои права в области работы с информацией, функциональную роль поставщиков информации, а также условия реализации этих функций, уметь работать с поставщиками информации и СМИ [18, с. 287—290].

В завершение стоит отметить: несомненно, противодействие идеологии терроризма — это комплексный вопрос. Как уже было отмечено, именно молодежь выступает основным объектом вербовочной деятельности террористических и экстремистских организаций. Соответственно, она должна выступать приоритетным объектом профилактической работы со стороны государственных органов и иных субъектов профилактики правонарушений. Приоритетно важной является организация целенаправленного воздействия на формирование личностного развития представителей современной молодежи, соединяющего духовно-нравственные и правовые предписания в единую мировоззренческо-аксиологическую целостность [19].

Именно воспитательные меры являются основным инструментом общества и государства в профилактике любых правонарушений в молодежной среде. При этом образовательные организации как важнейший социальный институт являются центрами воспитательной работы, поскольку в них работают люди с педагогическим образованием, а целевая аудитория — дети, подростки, молодежь — принципиально доступна для воспитательного воздействия. Определенная часть молодежи, не получая ответов на свои жизненные проблемы, пытается найти их самым радикальным путем. С этой точки зрения формирование мировоззрения, устойчивого к разного рода проявлениям экстремизма, ксенофобии и нигилизма, остается актуальной потребностью педагогического сообщества. Учитель должен уметь правильно выстраивать коммуникацию с учеником, вовремя увидеть неприемлемые в современном обществе отношения среди подрастающего поколения [11].

На сегодняшний день важным требованием современного информационного общества к образовательной среде становится подготовка выпускника, который не только грамотно владеет знаниями, но и умеет работать с информацией в повседневной жизни. Знания и навыки позволят подросткам разбираться в сложнейших вызовах современности и адекватно действовать в экстремальных ситуациях.

Обучающийся должен осознавать, что все участники информационных отношений обладают правами и обязанностями, а за совершение определенных противоправных действий в медиапространстве может наступить и юридическая ответственность.

Таким образом, формирование информационной грамотности подрастающего поколения следует рассматривать как важную составляющую в системе мер профилактики распространения криминальной субкультуры и экстремистских проявлений в молодежной среде, а также преступлений террористической направленности, совершаемых представителями молодого поколения, в том числе с использованием интернет-пространства. Данная превентивная мера будет способствовать повышению уровня культуры безопасности у молодежи и, соответственно, предупреждению и устранению причин, порождающих вовлечение их в противоправную деятельность.

Литература

1. Rybakov O.J., Rybakova O.S. Principles of information security of a child on the Internet. Studies in Computational Intelligence. 2019. Vol. 826. Pp. 427–433.
2. Авакьян М.В. Методические рекомендации по профилактике распространения идеологии терроризма и экстремизма : учебное электронное издание / М.В. Авакьян, М.А. Болвачев, Т.С. Волчецкая, Е.В. Осипова. Калининград : Издательство БФУ им. И. Канта, 2023. 44 с.
3. Аминов Д.И., Оганян Р.Э. Молодежный экстремизм в России. М. : Academia, 2007. 200 с.
4. Антонян Е.А., Аминов И.И. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6 (103). С. 167—177.
5. Антонян Е.А., Борисов Е.А. К вопросу о популяризации криминальной субкультуры среди молодежи // Lex russica. 2017. № 12 (133). С. 180—186.
6. Атагимова Э.И., Рыбакова О.С. Информационная грамотность молодежи в системе мер противодействия идеологии терроризма и экстремизма в цифровом информационном пространстве // Мониторинг правоприменения. 2022. № 3 (44). С. 29—37. DOI: 10.21681/2226-0692-2022-3-29-37. EDN: BUDWMP.
7. Атагимова Э.И. Право человека на информацию: вопросы обеспечения ее достоверности в цифровом информационном пространстве // Права человека и политика права в XXI в.: перспективы и вызовы : сборник научных трудов по итогам Всероссийской научно-практической конференции с международным участием, Москва, 27—28 мая 2022 года. Саратов : Саратовский источник, 2022. С. 449—465. EDN: NCYRYS.
8. Брусенцева Д.М. Формирование современным медиапространством террористических установок в молодежной среде / Д.М. Брусенцева, Н.Х. Гафиатулина // Государственное и муниципальное управление. Ученые записки. 2019. № 1. С. 193—198. DOI: 10.22394/2079-1690-2019-1-1-193-198. EDN: ZAWVCH.
9. Габиева С.М. К вопросу о противодействии терроризму в средствах массовой информации // Юридический вестник ДГУ. 2017. Т. 22. № 2. С. 30—34.
10. Клейменов А.А., Григорьева А.И., Дьячкова Т.В. Формирование антитеррористического мировоззрения у молодежи // Вестник Национального антитеррористического комитета. 2022. № 1 (28). С. 20—24.
11. Кучукян А.В. Социоструктурные детерминанты влияния виртуальных сетей на протестную активность современной молодежи : дис. ... канд. социол. наук: 22.00.04. Ставрополь : СКФУ, 2017. 183 с.
12. Противодействие идеологии терроризма и экстремизма в образовательной сфере и молодежной среде : аналитич. доклад / Отв. ред. В.В. Каберник; Моск. гос. ин-т междунар. отношений (ун-т) МИД РФ. М. : МГИМО-Университет, 2015. 76 с.
13. Ростокинский А.В. Концепция противодействия терроризму в Российской Федерации: проблемы реализации и пути их решения // Образование и право. 2022. № 7. С. 297—302.
14. Рыбаков О.Ю., Тихонова С.В. Информационные риски и эффективность правовой политики // Журнал российского права. 2016. № 3 (231). С. 88—95.
15. Рыбакова О.С. Безопасность несовершеннолетних в информационном обществе: анализ киберрисков и угроз // Мониторинг правоприменения. 2020. № 2. С. 65—73.
16. Рыбакова О.С. Молодежный экстремизм как угроза национальной безопасности // Права молодежи и приоритеты государственной молодежной политики : сборник научных трудов / Под ред. О.С. Рыбаковой. М. : ООО «Русайнс», 2022. С. 113—131. EDN: UZAOHD.
17. Сергеева М.Г. Перевезенцева О.Н. Формирование информационной грамотности младших подростков средствами ИКТ // Проблемы современного педагогического образования. 2019. № 63-2. С. 287—290.
18. Терроризм — угроза человечеству / Э.И. Атагимова, А.В. Ростокинский, О.С. Рыбакова. Серия «Правовое просвещение населения». М. : ФБУ НЦПИ при Минюсте России, 2022. 132 с.
19. Федичев А.В., Танимов О.В. К вопросу об информационной безопасности современного государства // Правовая информатика. 2016. № 2. С. 4—11.

THE INFORMATION COMPONENT IN THE SYSTEM OF MEASURES FOR PREVENTING THE SPREAD OF TERRORIST IDEOLOGY IN THE YOUTH MEDIUM

El'mira Atagimova, *Ph.D. (Law), the Apparatus of the State Duma of the Federal Assembly of the Russian Federation, Moscow, Russian Federation.*
E-mail: *atagimovaei@duma.gov.ru*

Keywords: *foundations of constitutional order, terrorism, extremism, national security, ideology, consciousness, youth, legal consciousness, information space, information literacy.*

Abstract

The paper discusses problem questions of popularising terrorist and extremist ideology in the youth medium using the information space.

Methods used in the study: methods of analysis and synthesis making it possible to give a theoretical justification for proposals for increasing the efficiency of measures aimed at preventing terrorism and extremism in the youth medium, to examine and identify the specific features of organisational work in the field of forming anti-terrorist consciousness.

Study findings: a justification is given for the conclusion that forming information literacy of the young generation is an important tool for preventing terrorist and extremist offences committed by representatives of the young generation. Proposals for increasing the efficiency of measures aimed at forming anti-terrorist consciousness among youth are put forward and justified.

Practical importance of the study: based on the proposals set forth by the author, it is possible to further improve preventive activities in the field of spreading terrorist and extremist ideology.

References

1. Rybakov O.J., Rybakova O.S. Principles of information security of a child on the Internet. Studies in Computational Intelligence. 2019. Vol. 826. Pp. 427–433.
2. Avak'ian M.V. Metodicheskie rekomendatsii po profilaktike rasprostraneniia ideologii terrorizma i ekstremizma : uchebnoe elektronnoe izdanie. M.V. Avak'ian, M.A. Bolvachev, T.S. Volchetskaia, E.V. Osipova. Kaliningrad : Izdatel'stvo BFU im. I. Kanta, 2023. 44 pp.
3. Aminov D.I., Oganian R.E. Molodezhnyi ekstremizm v Rossii. M. : Academia, 2007. 200 pp.
4. Antonian E.A., Aminov I.I. Blokchein-tekhnologii v protivodeistvii kiberterrorizmu. Aktual'nye problemy rossiiskogo prava, 2019, No. 6 (103), pp. 167–177.
5. Antonian E.A., Borisov E.A. K voprosu o populiarizatsii kriminal'noi subkul'tury sredi molodezhi. Lex russica, 2017, No. 12 (133), pp. 180–186.
6. Atagimova E.I., Rybakova O.S. Informatsionnaia gramotnost' molodezhi v sisteme mer protivodeistviia ideologii terrorizma i ekstremizma v tsifrovom informatsionnom prostranstve. Monitoring pravoprimeneniia, 2022, No. 3 (44), pp. 29–37. DOI: 10.21681/2226-0692-2022-3-29-37. EDN: BUDWMP.
7. Atagimova E.I. Pravo cheloveka na informatsiiu: voprosy obespecheniia ee dostovernosti v tsifrovom informatsionnom prostranstve. Prava cheloveka i politika prava v XXI v.: perspektivy i vyzovy : sbornik nauchnykh trudov po itogam Vserossiiskoi nauchno-prakticheskoi konferentsii s mezhdunarodnym uchastiem, Moskva, 27–28 maia 2022 goda. Saratov : Saratovskii istochnik, 2022, pp. 449–465. EDN: NCYRYS.
8. Brusentseva D.M. Formirovanie sovremennym mediaprostranstvom terroristicheskikh ustanovok v molodezhnoi srede. D.M. Brusentseva, N.Kh. Gafiatulina. Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski, 2019, No. 1, pp. 193–198. DOI: 10.22394/2079-1690-2019-1-1-193-198. EDN: ZAWVCH.
9. Gabieva S.M. K voprosu o protivodeistvii terrorizmu v sredstvakh massovoi informatsii. Iuridicheskii vestnik DGU, 2017, t. 22, No. 2, pp. 30–34.
10. Kleimenov A.A., Grigor'eva A.I., D'iachkova T.V. Formirovanie antiterroristicheskogo mirovozzreniia u molodezhi. Vestnik Natsional'nogo antiterroristicheskogo komiteta, 2022, No. 1 (28), pp. 20–24.

11. Kuchukian A.V. Sotsiostrukturnye determinanty vliianiia virtual'nykh setei na protestnuiu aktivnost' sovremennoi molodezhi : dis. ... kand. sotsiol. nauk: 22.00.04. Stavropol' : SKFU, 2017. 183 pp.
12. Protivodeistvie ideologii terrorizma i ekstremizma v obrazovatel'noi sfere i molodezhnoi srede : analitich. doklad. Otv. red. V.V. Kabernik; Mosk. gos. in-t mezhdunar. otnoshenii (un-t) MID RF. M. : MGIMO-Universitet, 2015. 76 pp.
13. Rostokinskii A.V. Kontseptsiia protivodeistviia terrorizmu v Rossiiskoi Federatsii: problemy realizatsii i puti ikh resheniia. Obrazovanie i pravo, 2022, No. 7, pp. 297–302.
14. Rybakov O.Iu., Tikhonova S.V. Informatsionnye riski i effektivnost' pravovoi politiki. Zhurnal rossiiskogo prava, 2016, No. 3 (231), pp. 88–95.
15. Rybakova O.S. Bezopasnost' nesovershennoletnikh v informatsionnom obshchestve: analiz kiberriskov i ugroz. Monitoring pravoprimeneniia, 2020, No. 2, pp. 65–73.
16. Rybakova O.S. Molodezhnyi ekstremizm kak ugroza natsional'noi bezopasnosti. Prava molodezhi i prioritety gosudarstvennoi molodezhnoi politiki : sbornik nauchnykh trudov. Pod red. O.S. Rybakovoi. M. : OOO "Rusains", 2022, pp. 113–131. EDN: UZAOHD.
17. Sergeeva M.G. Perevezentseva O.N. Formirovanie informatsionnoi gramotnosti mladshikh podrostkov sredstvami IKT. Problemy sovremennogo pedagogicheskogo obrazovaniia, 2019, No. 63-2, pp. 287–290.
18. Terrorizm – ugroza chelovechestvu. E.I. Atagimova, A.V. Rostokinskii, O.S. Rybakova. Seriia "Pravovoe prosveshchenie naseleniia". M. : FBU NTsPI pri Miniuste Rossii, 2022. 132 pp.
19. Fedichev A.V., Tanimov O.V. K voprosu ob informatsionnoi bezopasnosti sovremennogo gosudarstva. Pravovaia informatika, 2016, No. 2, pp. 4–11.

СИСТЕМНЫЙ АНАЛИЗ АНОМАЛЬНЫХ СОБЫТИЙ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Сухов А.В.[1], Конюшев В.В.[2]

Ключевые слова: *эргатическая система (эргасистема), информационное пространство, детерминированный хаос, многопараметрическая эргасистема, аномальные события, признаки, сингулярность, отображение последования Пуанкаре, информационный ресурс, информационная орбита, странный аттрактор, энтропия покрытия.*

Аннотация

Цель работы: определение устойчивых аномалий на множествах сингулярных последовательностей признаков в информационном пространстве.

Методы: системный анализ, математическое и компьютерное моделирование информационных процессов с применением модифицированного аппарата оптимального управления на основе энтропии покрытия.

Результаты: исследованы отображения последования Пуанкаре сингулярных признаков аномальных событий в информационном пространстве многопараметрических эргасистем; использованы дискретные отображения непрерывных физических параметров на фазовое пространство в пределах односвязной информационной области, ограниченной пространственно-временными характеристиками наблюдения многопараметрических эргасистем; в качестве примера многопараметрической эргасистемы исследована криминалистическая информационная система (криминалистическая характеристика) серийного преступления, построенная на основе идентификационных признаков преступления.

EDN: BKPTEG

Введение

Системы принятия решений на основе информации *многопараметрических эргасистем* требуют структурирования и формализации идентификационных признаков. При этом процессы изменения характеристик этих признаков часто носят характер динамического хаоса[3].

Примером информационного проявления многопараметрической *динамической системы*[4] *такого рода является криминальная характеристика серийного преступления. Особенностью серийных преступлений является то, что задействованы все основные составляющие криминогенных ситуаций и процессов, между которыми существует неявная связь, объединяющая отдельные параметры в единую систему* [7]. Признаки серийности, как правило, не проявляются в виде, доступном для оперативного анализа. В связи с этим актуальным является разработка специальных методов и соответствующего математического аппарата для идентификации сингулярных последовательностей аномальных событий в информационном пространстве серийного преступления.

В ряде работ [1, 2, 13] представлены продуктивные методические подходы к разработке математических моделей системы идентификационных признаков, позволяющих осуществлять идентификацию сингулярных последовательностей признаков аномальных событий в *информационном пространстве* [1, 3, 6, 8] многопараметрических динамических систем[5].

Вопросам системно-информационного анализа многопараметрических эргасистем посвящен ряд работ [3—6, 10], в которых рассматриваются общие мето-

[3] Паркер Т.С., Чжуа Л.О. Введение в теорию хаотических систем для инженеров // ТИИЭР. 1997. Т. 75. № 8. С. 6—40.

[4] Hirsch M.W. and Smale S. Differential equations, dynamical systems, and linear algebra. New York, NY: Academic Press, 1974.

[5] Там же.

[1] ***Сухов Андрей Владимирович,*** *доктор технических наук, профессор, профессор Московского авиационного института (Национального исследовательского университета), г. Москва, Российская Федерация.*

E-mail: avs57@mail.ru

[2] ***Конюшев Валерий Вениаминович,*** *старший научный сотрудник Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, г. Москва, Российская Федерация.*

E-mail: klvvvk@mail.ru

дические подходы к описанию динамических эргасистем и процессов.

Идентификация сингулярных последовательностей

Динамику сингулярных последовательностей на признаковой решётке индексов можно представить отображением последования Пуанкаре. При этом узлами решётки будет являться набор признаков процесса[6] [1, 13]:

$$\Pi = \{x \in \boldsymbol{R}^m \times \boldsymbol{S}, z \in \boldsymbol{R} | x(0) = x_0\}, \quad (1)$$

где x — вектор признаков последовательности; $z = \sum_{i=1}^{m} z_i$ — наблюдаемый процесс; $\boldsymbol{R}^m$ — m-мерное пространство действительных чисел; $\boldsymbol{S}$ — гиперплоскость набора признаков.

Для идентификации сингулярных последовательностей аномальных признаков можно использовать известный авторский *алгоритм идентификации* [13]. Результативную идентификацию предлагается проводить по следующей уточненной схеме:

Шаг 1. Детализация признаков. Построение информационной модели эргасистемы на множестве признаков. Построение идентификационной решетки (ИР). Определение состава индексов ИР.

Шаг 2. Динамическое сопоставление цепей факторов ($C(T_1)$, $C(T_2)$…, $C(T_k)$) с индексами ИР для каждого периода T_1...T_k .

Шаг 3. Определение апостериорной плотности вероятности (АПВ) на каждом шаге идентификации признаков проявления сингулярности на цепях факторов.

Шаг 4. Сравнение АПВ с пороговым значением.

Шаг 5. Кластеризация.

Шаг 6. Формирование предикторных признаков.

Шаг 7. Вычисление *энтропии покрытия* [5, 16] на каждом шаге идентификации признаков проявления сингулярности на цепях факторов.

Шаг 8. Сравнение энтропии покрытия с пороговым значением.

Шаг 9. Определение факта проявления или непроявления сингулярности.

К качественным характеристикам серийного преступления, по которым строится *система предикторов*, отнесены следующие основные параметры: квалификация преступления; место совершения преступления; время совершения преступления; предмет преступного посягательства; способ совершения; использование орудий и средств, результат осмотра места происшествия; характеристика потерпевших; характеристика подозреваемых; территориальная принадлежность; дополнительная характеристика преступления; решение, принятое по уголовному делу и другие признаки, количество которых может составлять от нескольких единиц до нескольких десятков.

Системный анализ сингулярных признаков

Для выявления сингулярных признаков используется подход, основанный на минимизации среднего байесовского риска в сочетании с использованием *энтропии покрытия* для построения отношения правдоподобия для критерия определения принадлежности аномалии к определяемому типу сингулярных последовательностей [1, 13].

В рамках данного подхода может использоваться аппарат *оптимального оценивания* [9] и в качестве критерия оптимальности можно воспользоваться одним из следующих критериев[7]: критерий Неймана-Пирсона, критерий идеального наблюдателя, критерий последовательного наблюдателя.

Математическая структура модели наблюдения выглядит следующим образом [11]:

$$z(t) = \sum_{i=1}^{m} [a_i x_i(t) + n_i(t)], \quad (2)$$

где m — количество рассматриваемых признаков; $n_i(t)$ — шумовой фактор, характеризующий влияние внешней среды и субъективность экспертов [14], влияющий на результат наблюдения; a_i — весовой коэффициент i-го признака, выбор которого удовлетворяет требованиям *ортонормированности* [11].

Тогда при соответствии сингулярной последовательности синдрому сигнальное выражение в (2) будет выглядеть следующим образом:

$$S(x(t), t) = \sum_{i=1}^{m} a_i(t) x_i. \quad (3)$$

А при несоответствии сингулярной последовательности синдрому сигнальное выражение в (2) можно представить как:

$$S_0 = \sum_{i=1}^{m} a_i x_{0i}(t) \quad (4)$$

Энтропия покрытия для апостериорного распределения признаков $x(t)$ определяется следующим образом [11, 13]:

$$H^{\text{п}}(x(t), z(t)) = log\left[\Lambda\left(z(t), x(t)\right)\right] = log\left[\frac{p\left(z(t),\ x(t)\right)}{p(z(t), 0)}\right], \quad (5)$$

где $p\left(z(t),\ x(t)\right)$ — апостериорная плотность распределения наблюдаемого процесса; $p(z(t), 0)$ — апостериорная плотность распределения при отсутствии вектора признаков.

Поскольку серийное преступление представляет собой ряд преступлений, каждое из которых рассматривается на интервале Δt, то при переходе к дискретной форме интеграл по времени в представлении функции правдоподобия (5) переходит в сумму по k-м

[6] Паркер Т.С., Чжуа Л.О. Введение в теорию хаотических систем для инженеров // ТИИЭР. 1997. Т. 75. № 8. С. 6—40.

[7] Тихонов В.И. Оптимальный прием сигналов. М. : Радио и связь, 1983. 320 с.

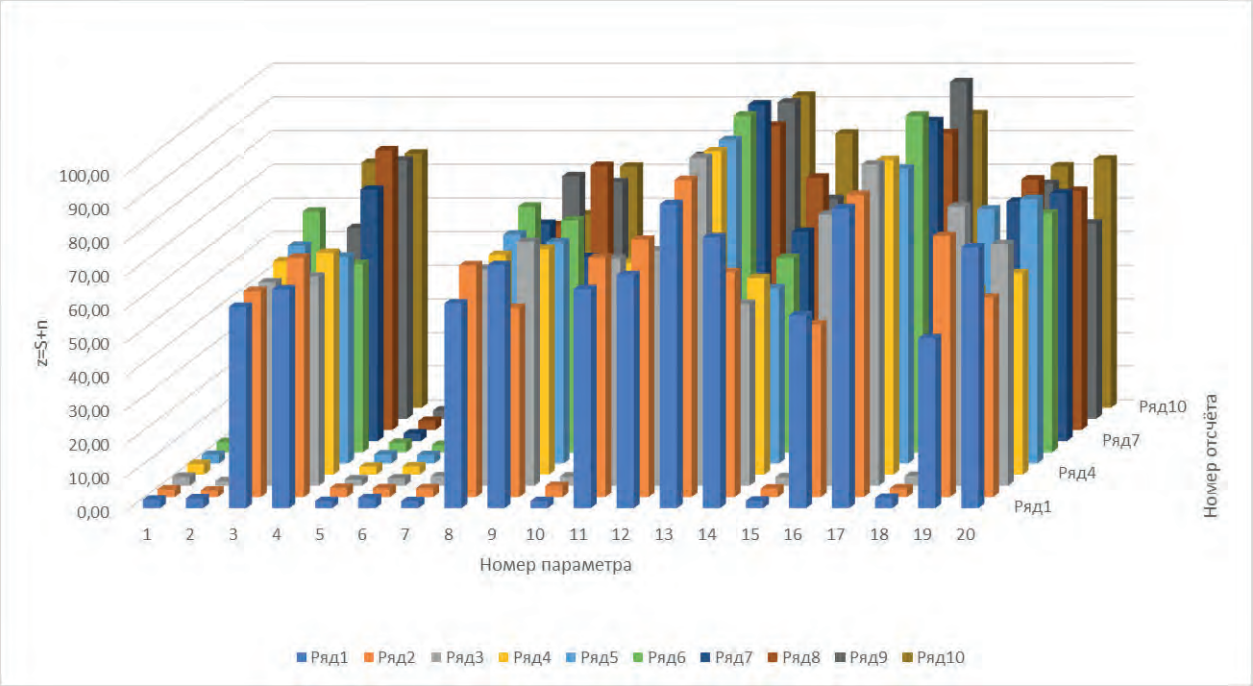


Рис. 1. Представление аномальной сингулярной последовательности на признаковой решётке индексов

слагаемым. При этом количество шагов при наблюдении на интервале времени от 0 до *T* равно:

$$M = T/\Delta t. \quad (6)$$

С учётом постоянности дискретного значения x_{ki} на интервале времени Δt_k значение для отношения правдоподобия:

$$H^{\text{п}}\big(z(t),x(t)\big) = \sum_{k=1}^{M}\sum_{i=1}^{m} z_k a_i x_{ki} - \\ -\frac{1}{2}\sum_{k=1}^{M}\sum_{i=1}^{m}(a_i x_{ki})^2 \lesseqgtr \text{NM}\ln\frac{p_{apr}(x_k=0)}{p_{apr}(x_k)} = \Lambda_{\text{пор}}, \quad (7).$$

где z_k — *k*-й отсчёт отображения последования Пуанкаре по результатам наблюдения; x_{ki} — *k*-й отсчёт *i*-го признака; *N* — дисперсия случайных факторов в модели наблюдения; $\Lambda_{\text{пор}}$ — пороговое значение критерия.

Отображение последования Пуанкаре аномальных признаков представляет собой *диффеоморфизм*[8] *на некоторой гиперплоскости* Σ*:*

$$\Sigma = \{x: h^t(x - x_\Sigma) = 0\}, \quad (8)$$

где *h* — вектор, нормальный к гиперплоскости Σ; x_Σ — некоторая точка, лежащая на гиперплоскости Σ.

В качестве точки x_Σ можно использовать математическое ожидание признака по результатам проведённого наблюдения.

Под *информационным ресурсом* серийного преступления понимается энтропия покрытия $H^{\text{п}}$, *нат* (*натуральных единиц*) для апостериорного распределения по результатам текущих наблюдений на интервале времени от 0 до *T*.

При наблюдении сингулярной аномалии, удовлетворяющей синдрому сингулярной последовательности, информационный ресурс будет возрастать, а когда сингулярная последовательность не будет соответствовать синдрому, уровень информационного ресурса наблюдений не будет превышать уровень порога.

Компьютерное моделирование аномалий на сингулярных последовательностях

Для примера рассмотрены последовательности, определённые на решётке 20-ти признаков (*m* = 20), количество дискретных отсчётов (шагов) равно десяти (*M* = 10). Результаты компьютерного моделирования реализации наблюдаемого процесса представлены в *табл.* 1.

Для идентификации аномальной сингулярной последовательности был использован признаковый синдром, который представлен в *табл.* 2.

Графическое представление динамики аномальной сингулярной последовательности 20-ти признаков за 10 шагов наблюдения, удовлетворяющей признаковому синдрому, показано на *рис.* 1.

Отображения последования Пуанкаре в информационном пространстве можно представить *информационными орбитами*, которые позволяют выделить области притяжения траекторий — *аттракторы*. На *рис.* 2, 3 и 4 представлены информационные орбиты

[8] Hirsch M. W. and Smale S. Differential Equations Dynamical Systems and Linear Algebra. New York, NY: Academic Press, 1974.

Таблица 1

Реализация наблюдаемого процесса на признаковой решётке индексов

Номер признака	$a_i x_{ki} + n_{ki}(t)$, *нат*									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	2,49	2,26	2,63	3,17	2,54	3,01	2,79	2,63	2,52	2,62
2	2,90	1,87	1,36	2,39	2,71	2,70	2,43	2,90	2,53	1,50
3	59,80	61,17	60,39	63,38	64,66	71,49	55,35	49,58	56,65	72,71
4	65,00	71,04	62,11	65,87	61,40	55,95	74,69	83,05	76,71	75,43
5	2,08	2,69	1,88	2,32	2,66	2,84	2,28	2,67	2,48	3,30
6	2,96	2,58	2,18	2,41	2,51	2,17	2,82	2,17	1,62	3,07
7	2,05	2,57	2,81	2,66	2,74	2,96	2,10	2,78	2,39	2,17
8	60,79	68,82	64,42	65,21	67,97	72,95	64,52	60,80	72,06	57,40
9	72,18	56,16	72,43	67,03	65,68	68,88	54,68	78,44	70,22	71,58
10	2,10	3,25	2,76	2,35	2,35	2,36	2,40	1,99	2,59	2,51
11	65,04	71,08	67,29	62,99	58,26	55,10	58,56	66,92	78,05	64,20
12	69,22	76,39	69,91	71,67	63,56	58,27	60,88	66,62	68,66	48,48
13	90,28	94,13	97,39	96,02	96,00	100,00	100,00	90,34	93,93	92,64
14	80,44	66,75	54,06	58,39	52,02	57,71	62,17	74,92	65,25	81,40
15	2,20	2,48	2,53	2,45	1,78	2,97	1,96	2,59	2,95	3,01
16	57,27	51,22	80,61	66,98	71,46	60,39	74,60	61,06	63,10	54,09
17	89,05	89,74	95,41	93,41	87,53	100,00	95,01	88,12	100,00	87,16
18	3,02	2,55	2,91	1,62	3,86	2,02	3,66	2,69	2,93	1,79
19	50,44	77,45	82,91	55,09	75,43	52,67	71,11	74,39	69,78	71,68
20	77,45	59,14	71,70	59,81	78,55	70,89	73,66	71,01	57,96	73,71

Таблица 2

Признаковый синдром аномальной сингулярной последовательности

Номер признака	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Синдром a_i	0	0	1	1	0	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1

отображения Пуанкаре для аномальной сингулярной последовательности, удовлетворяющей признаковому синдрому для шагов $k = 1…10$. При этом на *рис*. 2 представлены все информационные орбиты и для наглядности отображения использована логарифмическая шкала. На рис. 3 — орбиты, соответствующие синдрому по существенным признакам, а на *рис*. 4 — орбиты, соответствующие синдрому по несущественным признакам.

Информационные орбиты отображения Пуанкаре для аномальных последовательностей представляют собой детерминированный хаос. Эти орбиты, по существу, являются странными аттракторами и на *рис*. 2 и 3 видно, что эти аттракторы являются внешними областями траекторий отображений Пуанкаре.

В соответствии с выражением (8) было представлено отображение последования Пуанкаре для аномальной сингулярной последовательности относительно точки на $\sum$-гиперплоскости, в качестве которой выбрано математическое ожидание функции правдоподобия признаков на *k*-м шаге ($k = 1…10$) по результатам наблюдения:

$$\Phi_{\Sigma k} = M(\Phi_k = z_k a_i x_{ki} - \\ -\frac{1}{2}(a_i x_{ki})^2 | i = 1 \dots m) \quad (9)$$

На *рис*. 6 представлена *динамика информации покрытия* [10] (информационные орбиты отображения последования Пуанкаре), которая представляет разность энтропии покрытия функции правдоподобия признаков на *k*-м шаге Φ_k (k=1…10) по результатам наблюдения с математическим ожиданием этой функции $\Phi_{\Sigma k}$. Динамика информационного потока образует детерминированный хаос для аномальных сингулярных последовательностей, удовлетворяющих признаковому синдрому.

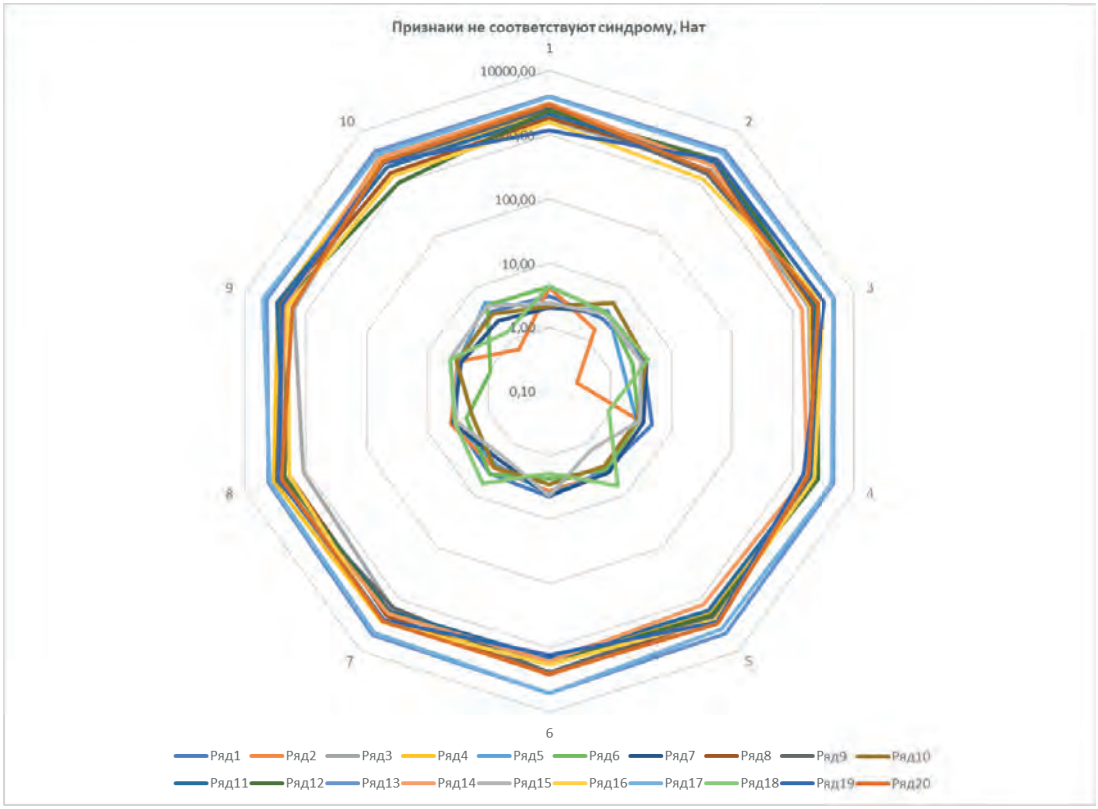


Рис. 2. Информационные орбиты отображения Пуанкаре для аномальной сингулярной последовательности, удовлетворяющей признаковому синдрому

Рис. 3. Информационные орбиты отображения Пуанкаре для аномальной сингулярной последовательности (по существенным признакам)

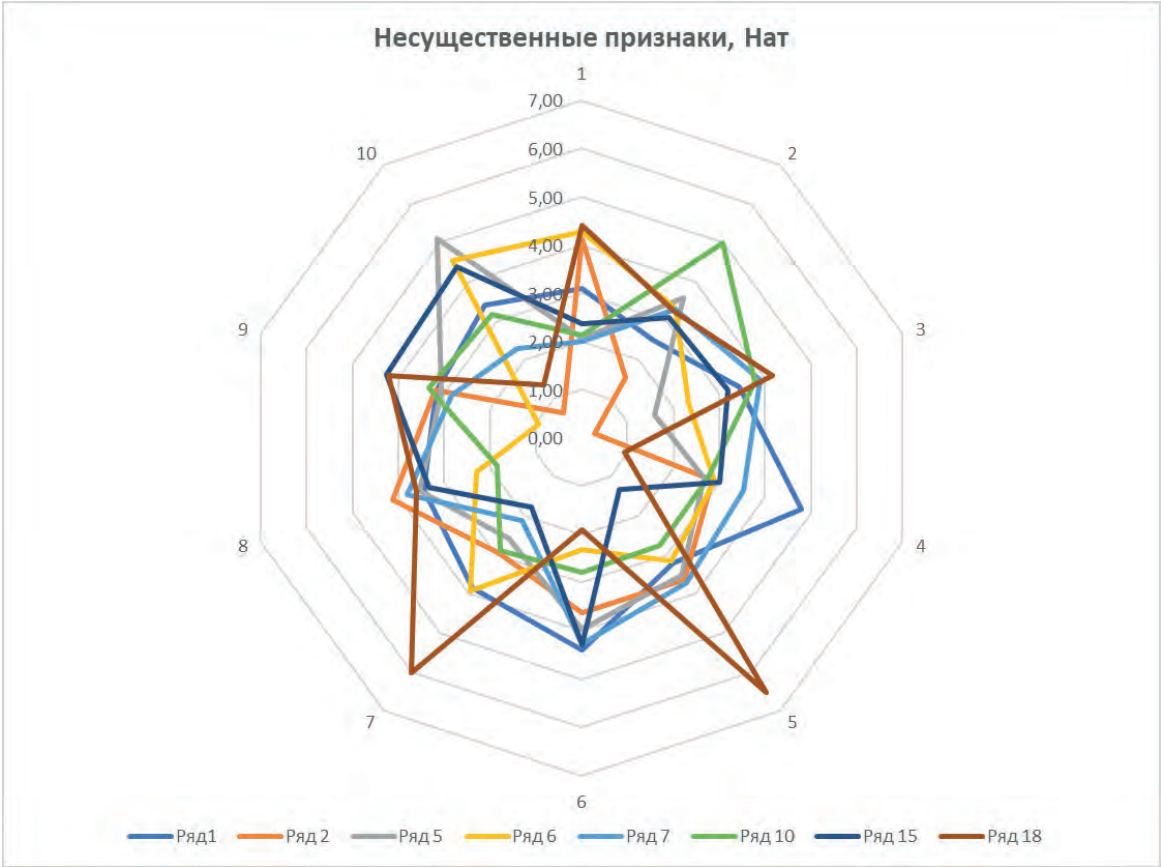


Рис. 4. Информационные орбиты отображения Пуанкаре для аномальной сингулярной последовательности (по несущественным признакам)

Для сравнения на *рис.* 5 представлены информационные орбиты отображения Пуанкаре для аномальной сингулярной последовательности, не соответствующей признаковому синдрому для шагов $k = 1…10$.

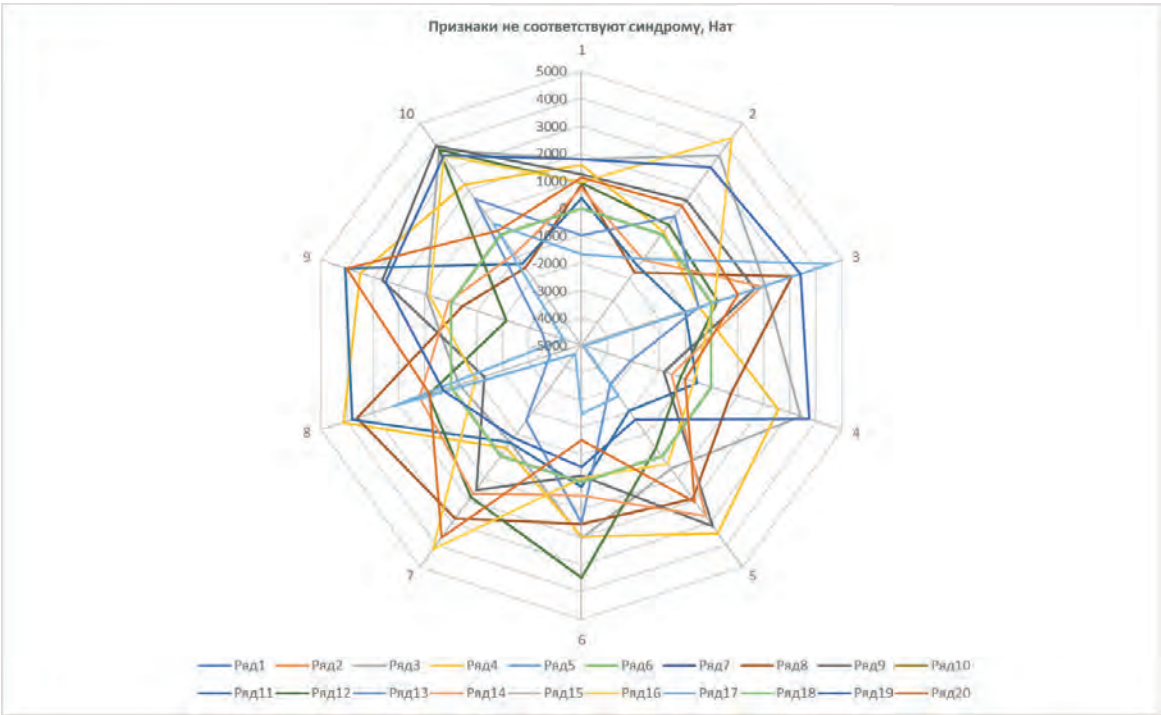


Рис. 5. Информационные орбиты отображения Пуанкаре для аномальной сингулярной последовательности, не соответствующей признаковому синдрому

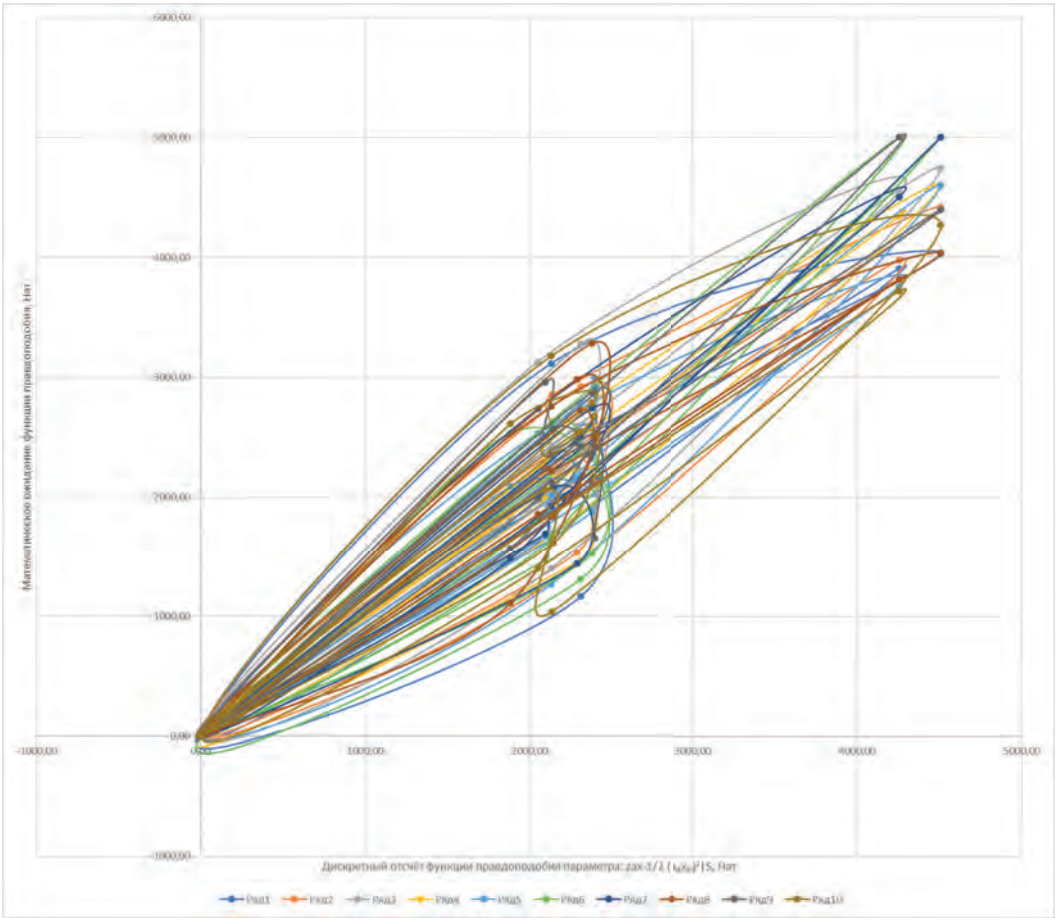


Рис. 6. Информационные орбиты отображения последования Пуанкаре для аномальных сингулярных последовательностей, удовлетворяющих признаковому синдрому (для S{x(t), t})

Для сравнения на *рис*. 7 представлены информационные орбиты отображения последования Пуанкаре для аномальных сингулярных последовательностей, не удовлетворяющих признаковому синдрому.

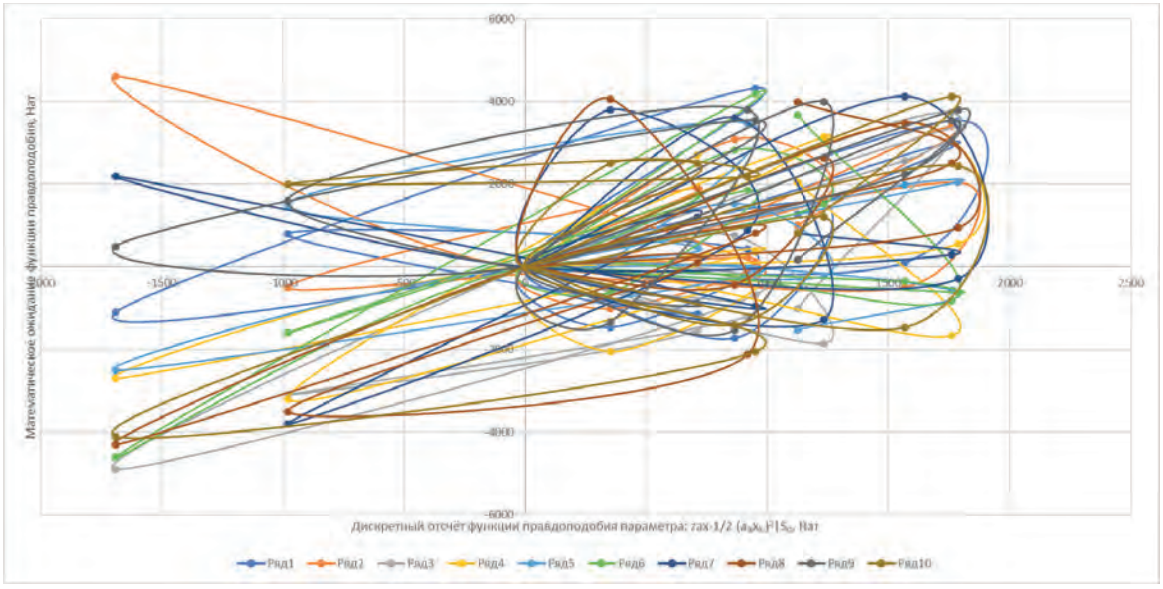


Рис. 7. Информационные орбиты отображения последования Пуанкаре для аномальных сингулярных последовательностей, не удовлетворяющих признаковому синдрому (для S_0)

Информационные орбиты отображения последования Пуанкаре позволяют выявлять странные аттракторы, определяющие *устойчивость* идентификации сингулярных последовательностей аномальных факторов.

В результате проведённого моделирования были получены графики динамики энтропии покрытия для информационных последовательностей, удовлетворяющих и не удовлетворяющих признаковому синдрому. Эти графики представлены на *рис*. 8.

На графиках видно, что порогового уровня для аномальной сингулярной последовательности, соответствующей признаковому синдрому, энтропия покрытия достигает на 8-м шаге. А энтропия покрытия сингулярной последовательности, не соответствующей признаковому синдрому, на рассматриваемом интервале наблюдения не достигает порогового значения.

При этом идентификацию соответствия сингулярной аномальной последовательности при достижении энтропией покрытия можно прекратить. Такая постановка вопроса идентификации принадлежности соответствует критерию последовательного наблюдателя.

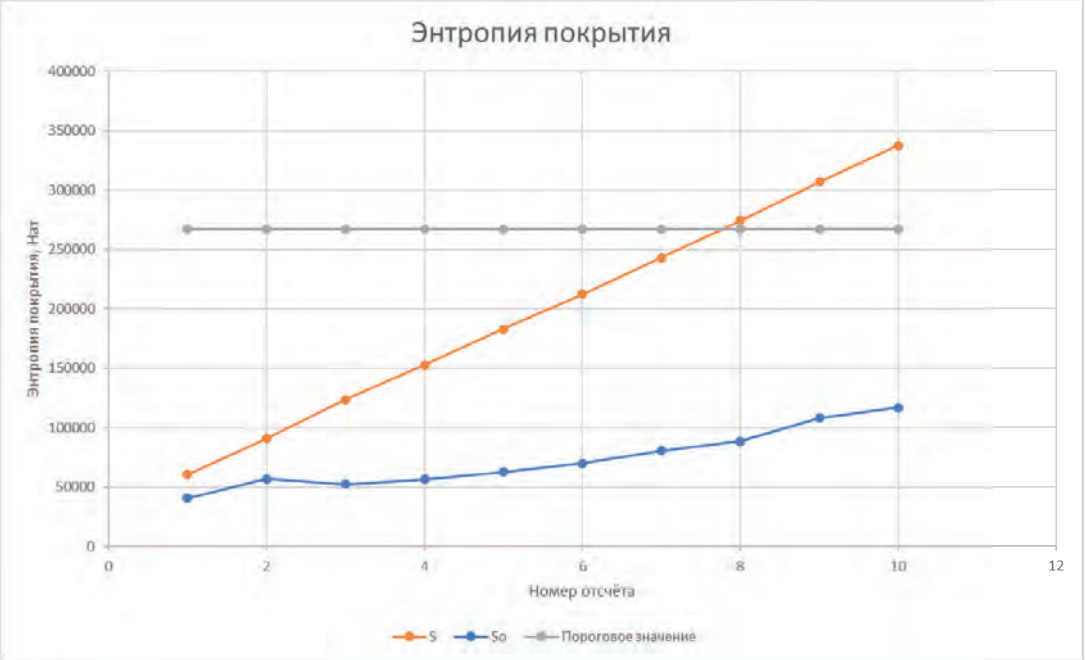


Рис. 8. Динамика энтропии покрытия для информационных последовательностей, удовлетворяющих (S) и не удовлетворяющих (S_0) признаковому синдрому

Заключение и выводы

Таким образом, рассмотрено формальное описание практического применения метода отображения последования Пуанкаре для распознавания сингулярных последовательностей на примере признаков серийности в информационном пространстве преступления. Исследование указанного направления проводится с точки зрения теории *хаотических систем*[9], которые представляют собой детерминированные системы, проявляющие себя в информационном пространстве случайным образом. Хаос в данном случае называется также странным поведением, что представляет собой важную сторону исследования нелинейных систем. При этом используется один из основополагающих научных принципов, заключающийся в том, что детерминированные системы по своей сути являются предсказуемыми при заданных уравнениях, описывающих некоторую систему, и начальных информационных условий [16] для этих уравнений, поведение системы может быть предсказано (прогнозировано) на любой интервал времени.

Проведённый системный анализ динамики аномальных сингулярных последовательностей позволяет определять области устойчивости динамики информационных орбит этих последовательностей. При этом информационные орбиты последовательностей представляют собой детерминированный хаос. Но по этим орбитам возможно на основании странных аттракторов проводить анализ устойчивости динамики аномальных последовательностей.

В то же время в случае получения информационных орбит отображения последования Пуанкаре с недетерминированным хаосом сразу можно сделать вывод о непринадлежности последовательностей к классу, соответствующему признаковому синдрому.

[9] Паркер Т. С., Чжуа Л. О. Введение в теорию хаотических систем для инженеров // ТИИЭР. 1997. Т. 75. № 8. P. 6—40.

Рецензент: ***Омельченко Виктор Валентинович,*** *доктор технических наук, профессор, заслуженный деятель науки и техники РСФСР, советник секретариата научно-технического совета ВПК «НПО Машиностроения», г. Москва, Российская Федерация.*
E-mail: omvv@yandex.ru

Литература

1. Бурый А.С., Сухов А.В. Оптимальное управление сложным техническим комплексом в информационном пространстве // Автоматика и телемеханика. 2003. № 7. С. 145—162.
2. Величко П.С., Конюшев В.В., Лёвин А.И., Сухов А.В. Применение технологий анализа больших данных и информационного подхода в целях выявления признаков серийности преступлений // Труды Межд. науч.-прак. конф. «Развитие учения о противодействии расследованию преступлений в условиях цифровой трансформации» (21 мая 2021 г.). Академия управления МВД России. М. : Академия управления МВД России, 2021. С. 142—145.
3. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
4. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
5. Ловцов Д.А. Информационная теория эргасистем. Тезаурус : монография. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
6. Ловцов Д.А. Системология информационного права // Правосудие/Justice. 2022. Т. 4. № 1. С. 41—70. DOI: 10.37399/2686-9241.2022.1.41-70 .
7. Ловцов Д.А. Системный анализ. Часть. 1. Теоретические основы. М. : РГУП, 2018. 224 с. ISBN 978-5-93916-701-7.
8. Ловцов Д.А., Ниесов В.А. Формирование единого информационного пространства судебной системы России // Российское правосудие. 2008. № 11 (31). С. 78—88.
9. Перов А.И. Статистическая теория радиотехнических систем. М. : Радиотехника, 2003. 400 с. ISBN 5-93108-047-3.
10. Сухов А.В. Динамика информационных потоков в системе управления сложным техническим комплексом // Теория и системы управления. 2000. № 4. С. 111—120.
11. Сухов А.В., Конюшев В.В., Калилец А.А. Информационное моделирование идентификации серийного преступления // Правовая информатика. 2022. № 1. С. 24—31. DOI: 10.21681/1994-1404-2022-1-24-31 .
12. Сухов А.В., Конюшев В.В. Разработка моделей оперативно-служебной деятельности цифровой полиции в информационном пространстве // Правовая информатика. 2022. № 4. С. 49—58. DOI: 10.21681/1994-1404-2022-4-49-58 .
13. Сухов А.В., Конюшев В.В. Идентификация сингулярных последовательностей признаков аномальных явлений в информационном пространстве // Правовая информатика. 2023. № 2. С. 26—33. DOI: 10.21681/1994-1404-2023-2-26-33 .
14. Федосеев С.В. Применение математических методов теории нечетких множеств при проведении судебно-экспертных исследований // Правовая информатика. 2020. № 4. С. 38—45. DOI: 10.21681/1994-1404-2020-4-38-45 .
15. Lovtsov D.A. Models for Measuring the Information Resource of a Computerized Control System. Automation and Remote Control. 1996. V. 57. No. 9, Part 1. Pp. 1221–1232.
16. Lovtsov D.A. Information Indices of Functioning Efficiency of MIS for Control Complex Dynamic Plants // Avtomatika i telemekhanika. 1994. № 12. С. 143—150.

SYSTEM ANALYSIS OF ABNORMAL EVENTS IN INFORMATION SPACE

Andrei Sukhov, *Dr.Sc. (Technology), Professor at the Moscow Aviation Institute (National Research University), Moscow, Russian Federation.*
E-mail: avs57@mail.ru

Valerii Koniushev, *Senior Researcher at the Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Moscow, Russian Federation.*
E-mail: *klvvvk@mail.ru*

Keywords: *ergatic system (ergasystem), information space, deterministic chaos, multiparametric ergasystem, abnormal events, indicators, singularity, Poincare sequence mapping, information resource, information orbit, strange attractor, entropy of coverage.*

Abstract

Purpose of the work: identifying stable anomalies on sets of singular sequences of indicators in information space.

Methods used in the study: system analysis, mathematical modelling and computer simulation of information processes using a modified optimal control apparatus based on coverage entropy.

Study findings: Poincare sequence mappings of singular indicators of abnormal events in the information space of multiparametric ergasystems are examined. Discrete mappings of continuous physical parameters onto the phase space within a single-connected information domain limited by the spatio-temporal characteristics of observation of multiparametric ergatic systems are used. A criminalistic information system (criminalistic characterisation) of a serial offence built on the basis of identification indicators of the offence is studied as an example of a multiparametric ergasystem.

References

1. Buryi A.S., Sukhov A.V. Optimal'noe upravlenie slozhnym tekhnicheskim kompleksom v informatsionnom prostranstve. Avtomatika i telemekhanika, 2003, No. 7, pp. 145–162.
2. Velichko P.S., Koniushev V.V., Levin A.I., Sukhov A.V. Primenenie tekhnologii analiza bol'shikh dannykh i informatsionnogo podkhoda v tseliakh vyiavleniia priznakov seriinosti prestuplenii. Trudy Mezhd. nauch.-prak. konf. "Razvitie ucheniia o protivodeistvii rassledovaniiu prestuplenii v usloviiakh tsifrovoi transformatsii" (21 maia 2021 g.). Akademiia upravleniia MVD Rossii. M. : Akademiia upravleniia MVD Rossii, 2021, pp. 142–145.
3. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
4. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
5. Lovtsov D.A. Informatsionnaia teoriia ergasistem. Tezaurus : monografiia. M. : Nauka, 2005. 248 pp. ISBN 5-02-033779-Kh.
6. Lovtsov D.A. Sistemologiia informatsionnogo prava. Pravosudie/Justice, 2022, t. 4, No. 1, pp. 41–70. DOI: 10.37399/2686-9241.2022.1.41-70 .
7. Lovtsov D.A. Sistemnyi analiz. Chast'. 1. Teoreticheskie osnovy. M. : RGUP, 2018. 224 pp. ISBN 978-5-93916-701-7.
8. Lovtsov D.A., Niesov V.A. Formirovanie edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii. Rossiiskoe pravosudie, 2008, No. 11 (31), pp. 78–88.
9. Perov A.I. Statisticheskaia teoriia radiotekhnicheskikh sistem. M. : Radiotekhnika, 2003. 400 pp. ISBN 5-93108-047-3.
10. Sukhov A.V. Dinamika informatsionnykh potokov v sisteme upravleniia slozhnym tekhnicheskim kompleksom. Teoriia i sistemy upravleniia, 2000, No. 4, pp. 111–120.
11. Sukhov A.V., Koniushev V.V., Kalilets A.A. Informatsionnoe modelirovanie identifikatsii seriinogo prestupleniia. Pravovaia informatika, 2022, No. 1, pp. 24–31. DOI: 10.21681/1994-1404-2022-1-24-31 .
12. Sukhov A.V., Koniushev V.V. Razrabotka modelei operativno-sluzhebnoi deiatel'nosti tsifrovoi politsii v informatsionnom prostranstve. Pravovaia informatika, 2022, No. 4, pp. 49–58. DOI: 10.21681/1994-1404-2022-4-49-58 .
13. Sukhov A.V., Koniushev V.V. Identifikatsiia singuliarnykh posledovatel'nostei priznakov anomal'nykh iavlenii v informatsionnom prostranstve. Pravovaia informatika, 2023, No. 2, pp. 26–33. DOI: 10.21681/1994-1404-2023-2-26-33 .
14. Fedoseev S.V. Primenenie matematicheskikh metodov teorii nechetkikh mnozhestv pri provedenii sudebno-ekspertnykh issledovanii. Pravovaia informatika, 2020, No. 4, pp. 38–45. DOI: 10.21681/1994-1404-2020-4-38-45 .
15. Lovtsov D.A. Models for Measuring the Information Resource of a Computerized Control System. Automation and Remote Control. 1996. V. 57. No. 9, Part 1. Pp. 1221–1232.
16. Lovtsov D.A. Information Indices of Functioning Efficiency of MIS for Control Complex Dynamic Plants. Avtomatika i telemekhanika, 1994, No. 12, pp. 143–150.

МЕТОДИКА АНАЛИЗА ЦИФРОВЫХ ПОЛЕЙ, ГЕНЕРИРУЕМЫХ СПРАВОЧНЫМИ ПРАВОВЫМИ СИСТЕМАМИ

Ващекин А.Н.[1], Ващекина И.В.[2], Квачко В.Ю.[3]

Ключевые слова: *информационное пространство, цифровые поля, функциональная идентичность, математические модели, методика, графы, матрицы, нечеткие множества, структура, изоморфизм.*

Аннотация

Цель работы: обоснование принципов анализа элементов цифрового пространства и алгоритмизации его проведения на основе математических методов.

Методы исследования: системный анализ, математическое моделирование, экспертное оценивание, теория графов, теория нечетких множеств.

Результаты: выявлена высокая степень самоорганизации в информационных взаимодействиях между деятелями цифровых полей на фоне несовершенства правового регулирования информационных отношений между деятелями цифрового пространства; предложена общая методика определения функциональной идентичности некоторых цифровых полей с использованием моделей, построенных на основе потенциально изоморфных алгебраических структур, например, графов (ориентированных графов) и сопряженных с ними матриц (смежности, инцидентности и др.), характеризующих информационные взаимодействия на этих полях; в качестве частного примера проведен сравнительный анализ цифровых полей, генерируемых образовательными сайтами трех наиболее распространенных в России справочных правовых систем; обоснован вывод о функциональной идентичности цифровых полей для образовательных систем «КонсультантПлюс» и «Гарант», а также о неидентичности им цифрового поля, генерируемого системой «Кодекс».

EDN: NWRRUD

Введение

Цифровое пространство на современном технологическом этапе образует наиболее весомую часть пространства *информационного* [6]. Оно порождается цифровым компонентом информационной среды, в некоторой степени совпадающей с территориальными границами определенного государства или союза государств, и включает в себя образования нового, до сих пор малоизученного типа — *цифровые поля* (англ. *digital fields*) и *цифровые площадки* (англ. *digital grounds*) [4].

Цифровое пространство базируется на соответствующей инфраструктуре и характеризуется набором своеобразных отличительных свойств. Изучение этой совокупности цифровых норм и социальных практик, а также правовых и иных отношений между разнообразными деятелями различных цифровых полей, в том числе *просьюмерами* (англ. *prosumers*), владельцами интернет-сайтов, государством, представляет собой на данный момент не до конца разрешенную методологическую *проблему* [5], работа над которой тем не менее активно ведется в отечественном научном сообществе [1].

Современное информационное пространство базируется на новых элементах цифровой среды — цифровых площадках, включающих в себя различные социальные группы, нередко формирующихся на основе одного сайта, способного обеспечить информационное взаимодействие в рамках конкретного форума, файлообменника, онлайн-магазина по продаже товаров определенного типа, оказания услуг определенной направленности, новостного ресурса, справочной системы. Цифровые площадки порождают более крупные структурные элементы цифрового пространства — *цифровые поля*, соответствующие совокупности деятелей с одинаковыми цифровыми интересами.

[1] ***Ващекин Андрей Николаевич,*** *кандидат экономических наук, доцент, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: vaschekin@mail.ru

[2] ***Ващекина Ирина Викторовна,*** *кандидат экономических наук, доцент, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: vaschekina@mail.ru

[3] ***Квачко Вячеслав Юрьевич****, кандидат физико-математических наук, доцент, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: k3v9@list.ru

Способ исследования

В статье рассмотрен способ анализа цифровых полей и их взаимного сравнения для возможного установления их функциональной идентичности. Комплекс информационных взаимодействий между цифровыми полями подчиняется общим законам развития и координации элементов сложных самоорганизующихся систем — логистических, финансовых, правовых. Поэтому исследование информационного взаимодействия в цифровом поле следует производить на основе воспроизведения структуры порождающей его цифровой площадки (или нескольких, если поле генерируется их совокупностью).

Для формального анализа функционирования цифровой площадки наилучшим образом подходит представление ее структуры в виде графа. В этом случае смысловые разделы площадки могут быть представлены вершинами графа, а цифровые потоки — ребрами.

Весовые характеристики логично задавать как результат нечеткой оценки, проводимой экспертом (группой экспертов). И уже после выявления структурных закономерностей следует вводить в модели факторы, отражающие специфику конкретной системы — наличие управления, воздействие субъекта, открытость информации, безопасность ее транслирования.

Внешний облик цифровых полей

Для конкретизации исследования рассмотрены в сравнении цифровые поля, генерируемые справочными правовыми системами (СПС). Сразу оговоримся, что поскольку количество их даже в российском сегменте Интернета довольно велико, а функционал их может быть довольно разнонаправленным, мы сосредоточимся только на тех, которые порождаются взаимодействием пользователей внутри систем обучения, созданных для самостоятельного или группового освоения наиболее распространенных в России СПС: «КонсультантПлюс», «Гарант» и «Кодекс».

Пользователями СПС являются коммерческие компании, разнообразные организации, госструктуры, библиотеки, вузы, а также простые граждане, нуждающиеся в решении тех или иных проблем через доступ к правовой информации разного рода. Постоянно пополняемые информационные базы современных СПС, включающие не только нормативные правовые акты, но и материалы судебной практики, аналитические обзоры, научные статьи и учебную литературу, дают опытным пользователям наиболее широкий спектр возможностей для получения правовой информации и оперативной работы с ней.

Как правило, материалы СПС предлагают в готовом виде решения по типовым правовым ситуациям, включают в себя путеводители, помогающие найти ответ практически на любой профессиональный вопрос и понять, как действовать в конкретной ситуации, как применять нововведения, указывают на возможные риски. В них могут быть встроены особые инструменты. Например, в системе «КонсультантПлюс» имеются онлайн-сервисы «Конструктор договоров» и «Конструктор учетной политики» [9], которые позволяют составлять и анализировать договоры и учетную политику компании на принципиально новом уровне.

Каждая современная СПС предоставляет доступ к видеосеминарам для специалистов по актуальным практическим вопросам, которые ведут авторитетные эксперты, в том числе из профильных министерств и ведомств. Эти семинары могут носить как общий характер, так и предлагать пользователю исчерпывающий ответ на вопрос со ссылками на правовые акты, инструкции и практические материалы.

Все нормативные акты снабжены актуальной информацией об их применении: указано, действует документ или нет, имеется доступ к предыдущим версиям документа в зависимости от указанного периода времени. Как правило, параллельно с предоставлением самого документа даются ссылки на важную практику по его применению, позиции судов, ведомств, образцы заполнения документов и другие готовые решения.

СПС обеспечивают разные виды поиска информации, как правило, простые и быстрые, учитывающие профессиональную лексику, распространенные сокращения и другие особенности обработки правовой информации. Для облегчения работы пользователя в СПС создаются персональные профили для каждого специалиста (бухгалтера, юриста, специалиста бюджетной организации, специалиста по закупкам, специалиста по кадрам). Свой профиль обеспечивает уникальную стартовую страницу, ленту новостей, подборку видеосеминаров, набор специальных подсказок; результаты поиска также настраиваются под задачи специалиста.

Эти преимущества обеспечивают многочисленным цифровым полям, образуемым разнообразными площадками СПС, огромное количество пользователей (как указано выше, разного уровня). Как правило, каждый из этих пользователей начинает осваиваться на этих цифровых полях с посещения сайтов учебных центров СПС, на которых он рассчитывает приобрести первоначальные навыки. Однако каждая из подобных площадок на деле давно ушла от примитивного обеспечения процесса обучения и, обрастая по мере своего развития все более разнообразным функционалом, стала основой для собственного цифрового поля.

Очевидно, что чем более привлекательным и полезным для пользователей окажется образовательная площадка конкретной СПС, тем больше шансов, что этот пользователь задержится на ней, станет ее завсегдатаем, и в дальнейшем станет профессиональным пользователем именно этой СПС. Поэтому создателям образовательных сайтов имеет смысл проводить сравнение своей площадки с конкурентами, чтобы усилить имеющиеся преимущества и устранить недостатки своей системы. Мы же, как незаинтересованные исследователи, можем провести сравнительный анализ непредвзято.

Начнем с обзора общей структуры сайтов. На рис. 1 показана схема образовательного сайта СПС «КонсультантПлюс». Надо заметить, что структура этого сайта динамично меняется, при этом появляются новые разделы. Так, например, относительно недавно у пользователей появилась возможность использовать систему для составления плана курсовой работы по наиболее значимым научным направлениям, число которых создатели системы намерены постепенно увеличивать. Несколько ранее на сайте появились разделы с классической и современной научной литературой по праву и экономике. Очевидно, создатели в настоящее время активно развивают раздел, предоставляющий студентам, изучающим СПС, новые возможности для творческой работы, написанию научных статей, подготовке докладов, рефератов, курсовых работ и дипломов. При достаточном пересечении темы студенческой работы с материалами, имеющимися в СПС, система предоставляет потенциальному автору план работы и составляет библиографический список, оформленный по стандарту. Поэтому схема, иллюстрирующая нашу статью, может до некоторой степени отличаться от того, что увидит пользователь, зайдя на сайт https://www.consultant.ru/edu/. Это соображение справедливо и в отношении общих схем двух других образовательных сайтов, рассматриваемых нами.

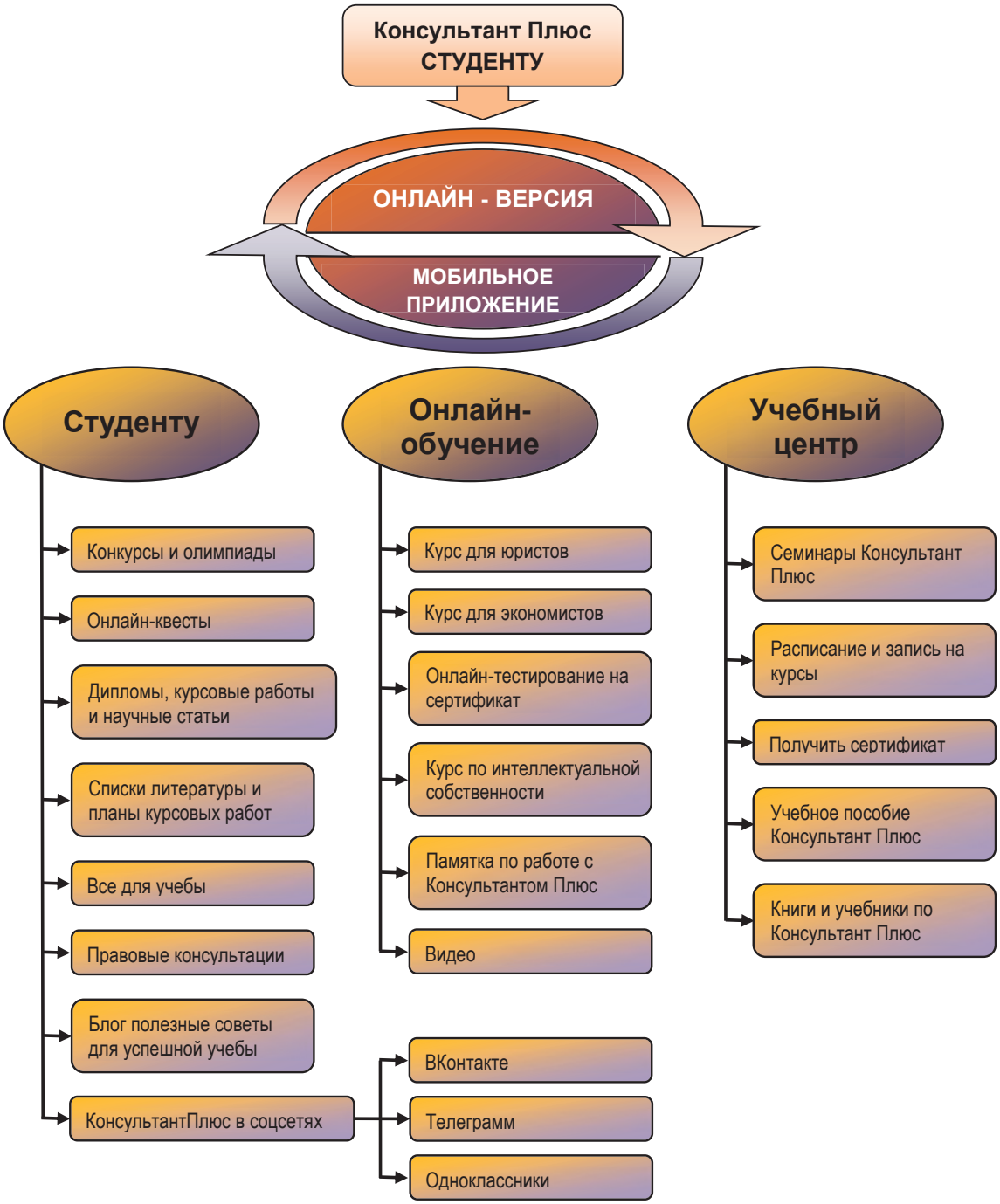


Рис. 1. Схема образовательного сайта СПС «КонсультантПлюс»

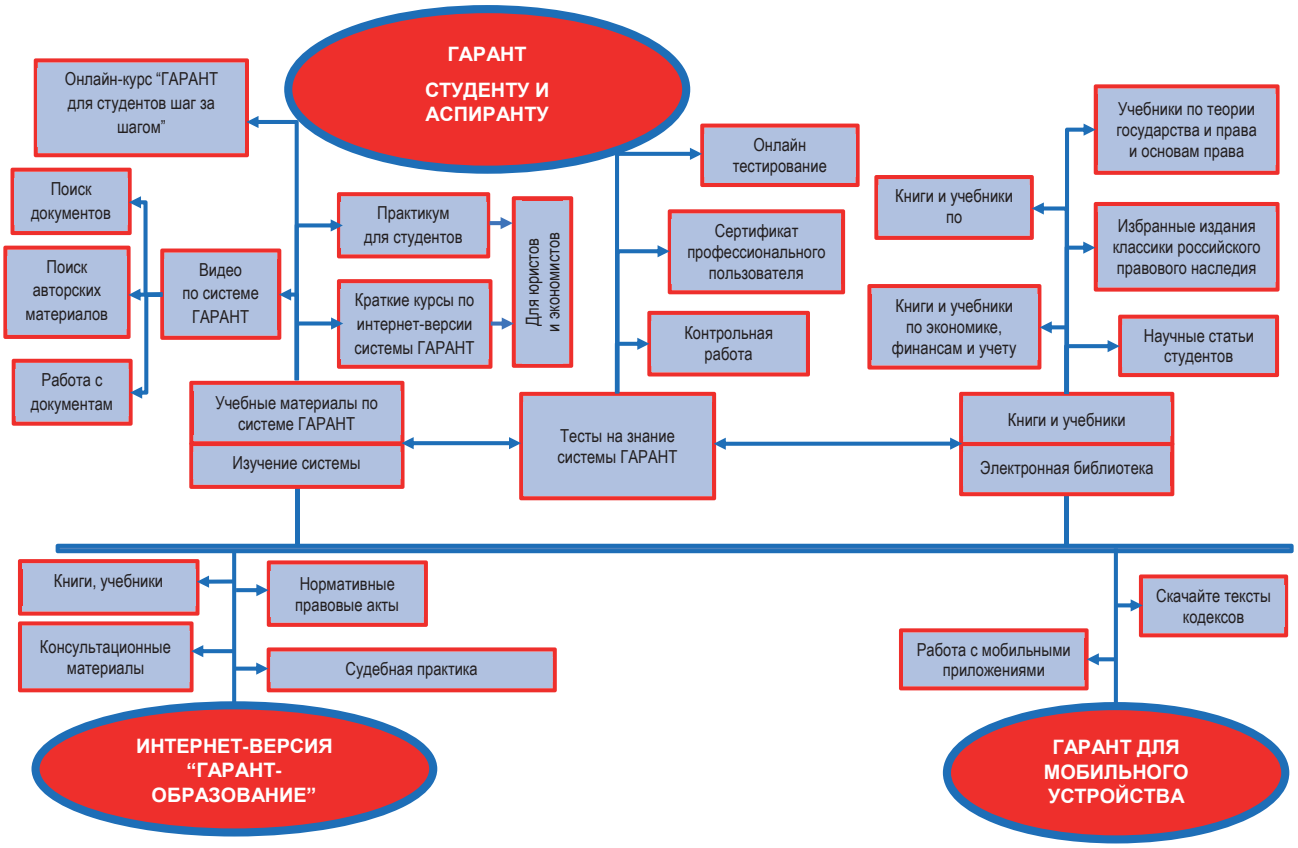


Рис. 2. Схема образовательного сайта СПС «Гарант»

На рис. 2 аналогичным образом проиллюстрирована общая структура образовательного сайта СПС «Гарант». Здесь разделы, обеспечивающие научное творчество пользователей (в первую очередь — обучающихся) также занимают немалое место, хотя перечисленными выше возможностями по формированию плана работы и списка литературы система пока не обладает. Тем не менее на сайте есть большая библиотека разнообразной научной литературы по разным направлениям, обеспечивается доступ к многочисленным студенческим публикациям (заметим, что материалы, размещаемые пользователями на этой и других изучаемых нами образовательных цифровых площадках, имеют статус публикации в средствах массовой информации, что побуждает немалое количество обучающихся к активной творческой работе).

Процесс обучения облегчается многочисленными средствами усвоения и закрепления материала: учебные пособия в различных форматах, содержащие теоретический материал, разобранные примеры и задания для самостоятельного выполнения, видеоролики, различные формы организации контрольных работ, включая квесты.

Однако наиболее заметными на этих цифровых площадках являются ссылки, предоставляющие доступ к слегка редуцированным, но вполне функциональным средствам получения правовой информации: интернет или, иначе, онлайн-версии соответствующей СПС и мобильному приложению, обеспечивающему максимально удобный интерфейс пользователям смартфонов.

Представленная на рис. 3 общая структура образовательного сайта СПС «Кодекс» на первый взгляд отличается тем, что в ней предоставляется доступ к одновременному обучению в системе «Техэксперт», однако в той части, которая касается доступа к правовой информации, возможности пользователя достаточно велики.

Функциональная идентичность цифровых полей

Для изучения функциональной идентичности исследуемых нами объектов следует обратиться к исследованию изоморфизма их структуры, которая наилучшим образом может быть представлена в виде простейших моделей — графов [3]. Сразу оговоримся, что внешний облик сайтов, генерирующих цифровые поля, рассмотренных в предыдущем разделе статьи, не является буквальным слепком их структуры. Фактическая структура цифрового поля определяется весом каждого его раздела, представляющего собой вершину графа. Весовая характеристика может задаваться различными способами, наиболее адекватным из которых является нечеткий алгоритм оценки [10, 11].

Авторы имели в своем распоряжении большое количество экспертов, активно задействовавших ис-

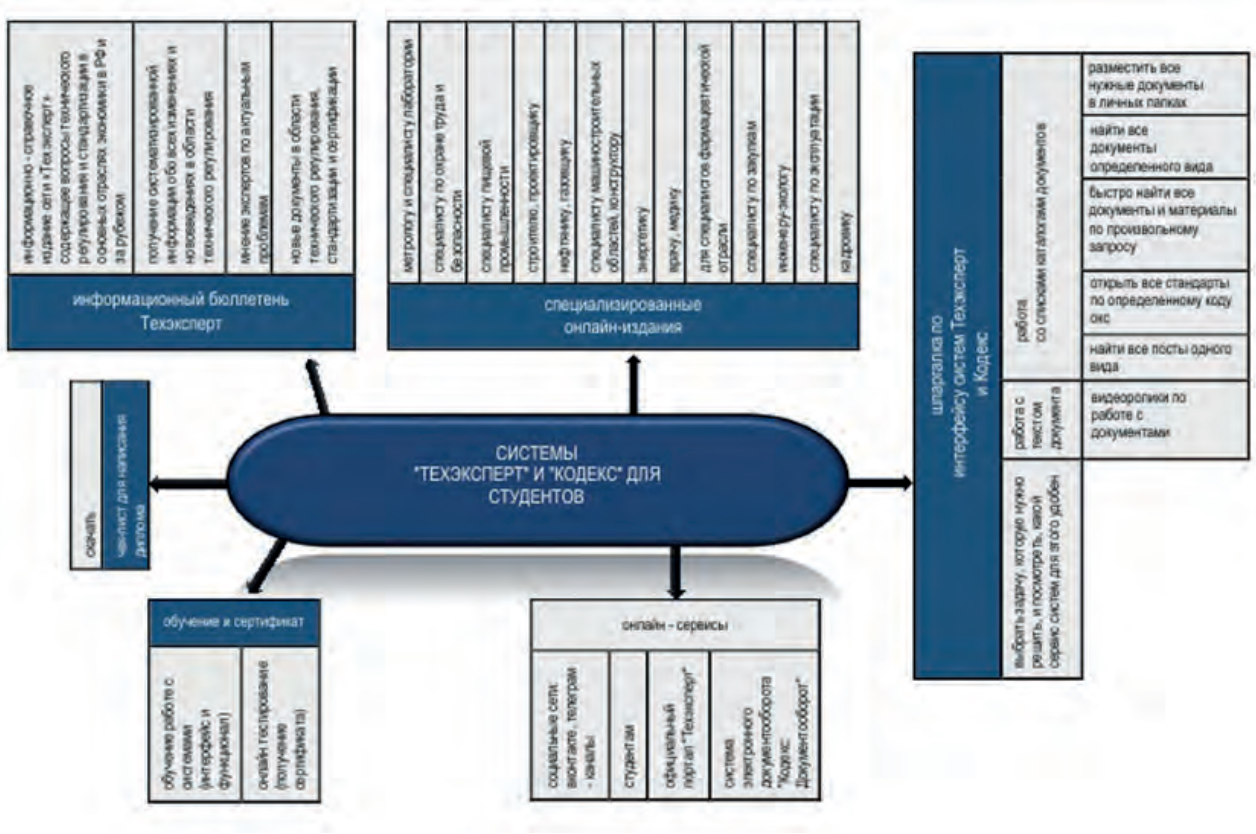


Рис. 3. Схема образовательного сайта СПС «Кодекс»

следуемые в статье цифровые площадки — более ста студентов Российского государственного университета правосудия.

Согласованность мнений этих экспертов проводилась с помощью метода анализа иерархий [2, 7].

В нескольких словах он выглядит следующим образом. За $X = \{x_1 ... x_n\}$ возьмем множество разделов (вершин составляемого графа). Эксперту для выбора весовых значений $C_1,\ldots,C_n$ этих вершин необходимо найти вектор приоритетов $\omega = (\omega_1,\ldots,\omega_n)^T$, где T — операция транспонирования, который определит степень их «важности» для пользователя.

Обозначим через a_{ij} число, соответствующее значимости элемента C_i по сравнению с C_j по мнению эксперта. Эти числа составляют квадратную матрицу размера $n \times n$, которую обозначим через A: $A = a_{ij}$.

Эта матрица A является обратно-симметричной, т. е. $a_{ij} = \frac{1}{a_{ji}}$.

Если суждение эксперта совершенно при всех сравнениях, то $a_{ik} = a_{ij}a_{jk}$ для всех i, j, k и матрица A называется согласованной.

Очевидным для согласованной матрицы является случай, когда сравнения основаны на точных измерениях, т. е. известен вектор приоритетов $\omega = (\omega_1,\ldots,\omega_n)^T$. В этом случае $\sum_{j=1}^{n} a_{ij}\omega_j = n\omega_i, i = 1,\ldots,n$, что эквивалентно выражению $A\omega = n\omega$.

В теории матриц эта формула отражает тот факт, что ω является собственным вектором матрицы A с собственным значением n.

Однако если a_{ij} основаны не на точных измерениях, а на субъективных суждениях — уравнение $A\omega = n\omega$ не выполняется.

В связи с этим приемлемое значение вектора приоритетов ω находится так: если A — матрица значений парных сравнений, то для нахождения вектора приоритетов нужно найти такой ω, который удовлетворяет $A\omega = \lambda_{max}\omega$ (т.е. вектор ω, представляющий собой собственный вектор матрицы A, соответствующий максимальному собственному значению λ_{max}).

Для нормализации решения «слегка» изменим ω, полагая $\alpha = \sum_{i=1}^{n} \omega_i$ и заменяя ω на $\frac{1}{\alpha}\omega$. Это обеспечивает единственность, а также то, что $\sum_{i=1}^{n} \omega_i = 1$.

Заметим следующее: так как малые изменения в a_{ij} вызывают малое изменение λ_{max}, отклонение последнего от n является мерой согласованности. Поэ-

тому индекс согласованности $\delta = \frac{\lambda_{max} - n}{n-1}$ можно рассматривать как показатель «близости к согласованности». Если этот индекс достаточно мал, например $\delta \le 0{,}1$, суждения эксперта считаются удовлетворительными.

Заметим, что примененный нами в данной работе нечеткий подход обеспечивает адекватную оцифровку субъективных экспертных мнений и позволяет решать широкий спектр задач, в том числе экономических [12].

Опираясь на эту методику, были сформированы три графа: *Ct* для образовательной системы «КонсультантПлюс», *Gt* для системы «Гарант» и *Cd* для системы «Кодекс» (рис. 4). Графы показаны как неориентированные, поскольку перемещение между их вершинами осуществляется в обе стороны. Для цифровых полей с более развитыми структурами, очевидно, возможно и даже целесообразно отображение их в виде ориентированных графов, но в нашем случае осложнять модель не требуется.

Граф *Ct* образован следующими вершинами (разделами цифрового поля): Ct_1 — Мобильное приложение, Ct_2 — Онлайн-версия, Ct_3 —Онлайн-обучение, Ct_4 — Конкурсы (включая квест), Ct_5 — Курсы, Ct_6 — Получение сертификата, Ct_0 — Творческая работа.

Граф *Gt* больше развернут по горизонтали (как и общая схема сайта) и сформирован вершинами: Gt_1 — Мобильное приложение, Gt_0 — Интернет-версия, Gt_2 — Изучение системы «Гарант», Gt_3 — Курсы, Gt_4 — Получение сертификата, Gt_6 — Творческая работа.

Граф *Cd* соединяет вершины Cd_1 — Система «Технэксперт», Cd_2 — Информационный бюллетень и другие издания, Cd_3 — Обучение, Cd_4 — Онлайн-сервисы, Cd_5 — Шпаргалка, Cd_6 — Сертификат.

Проверка объектов на изоморфизм

Изоморфизм разнообразных алгебраических структур хорошо исследован в современной математике. В отношении графов он выражается в наличии взаимно однозначного соответствия (биекции) между множествами их вершин, такого, что любая пара вершин в одном графе соединена тогда и только тогда, когда соответствующая им пара вершин в другом графе тоже соединена.

Простейшим способом проверки графов на изоморфизм является сравнение их матриц смежности. Если при рассмотрении всех возможных перестановок строк и столбцов хотя бы одна приведет из матрицы смежности одного к матрице другого, изоморфизм будет установлен, а задача функциональной идентичности решена. Для определения изоморфизма более сложных структур также разработаны надежные алгоритмы, опирающиеся на свойства графов (ориентированных графов) и сопряженных с ними матриц (смежности, инцидентности и др.), позволяющих однозначно охарактеризовать информационные взаимодействия на исследуемых цифровых полях.

В нашем случае граф *Cd* сразу следует исключить из процесса взаимной проверки, поскольку число его вершин не совпадает с числом вершин первых двух графов. Смысловая нагрузка некоторых из этих вершин

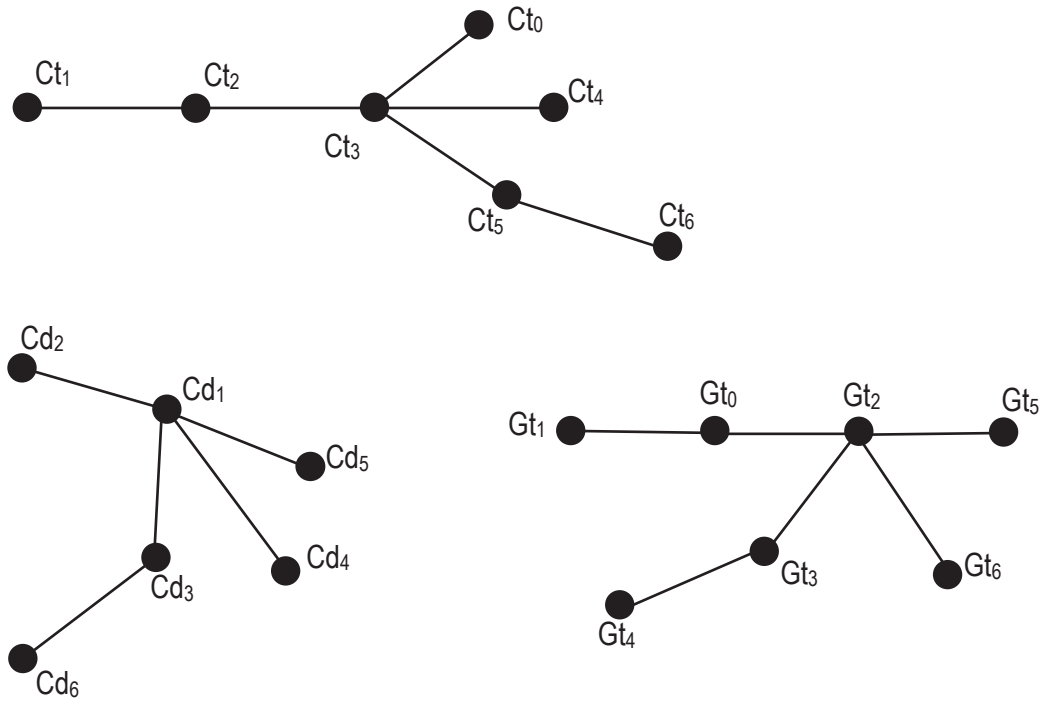


Рис. 4. Структуры графов рассматриваемых цифровых полей

(разделов) также заметно отличается, по крайней мере для вершины Cd_1 — Система «Техноэксперт» совершенно не находятся смысловые аналоги в графах *Ct* и *Gt*.

При рассмотрении этих двух последних графов, напротив, легко находится взаимное соответствие вершин: $Gt_6 \rightarrow Ct_0$, $Gt_1 \rightarrow Ct_1$, $Gt_0 \rightarrow Ct_2$, $Gt_2 \rightarrow Ct_3$, $Gt_5 \rightarrow Ct_4$, $Gt_3 \rightarrow Ct_5$, $Gt_4 \rightarrow Ct_6$, что избавляет нас от необходимости строить матрицы смежности. Получается, что графы изоморфны. К тому же в этих цифровых полях наблюдается практически полная смысловая идентичность разделов, различающихся только в деталях.

Заключение

Таким образом, можно заключить, что цифровые поля, генерируемые образовательными системами «КонсультантПлюс» и «Гарант», функционально идентичны, а поле, генерируемое образовательной системой «Кодекс», неидентично обоим этим полям.

Воспроизведение структуры цифровых полей с помощью графов позволяет производить взаимное сравнение организации информационных потоков внутри каждого из них, а выявление их функциональной идентичности может способствовать решению множества прикладных задач. К примеру, в последние годы наблюдается рост влияния цензуры на формирование интернет-контента, в результате которого происходит заметное переформатирование аудиторий различных социальных сетей, которые могут, например, фактически аккумулировать сторонников различных кандидатов в президенты США, с оттоком деятелей определенных цифровых полей с привычных ресурсов и концентрацией их на новых площадках. Заметные изменения происходят и на международном уровне: предвзятость формально независимого *Youtube* к материалам «пророссийских» информационных агентств и лавина блокировок частных ютубканалов заметна невооруженным глазом. Подобные примеры тенденциозной демонстрации администрациями социальных сетевых ресурсов своих политических предпочтений свидетельствуют о фактическом превращении этих ресурсов в средства массовой информации.

При ведении такого рода информационной борьбы [8] в цифровом пространстве представленная в работе методика может дать ответ на вопрос: являются ли различные поля функционально идентичными, могут ли определенные цифровые поля функционально заменить какие-либо другие, а если не могут, то каким образом можно модифицировать их структуру, чтобы они справились с этой задачей в случае введения ограничительных мер?

Рецензент: ***Цимбал Владимир Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки РФ, профессор кафедры автоматизированных систем боевого управления Филиала Военной академии им. Петра Великого, г. Серпухов, Российская Федерация.*
E-mail: tsimbalva@mail.ru

Литература

1. Борисов Р.С. Эффективный алгоритм управления переработкой судебной статистической информации // Правовая информатика. 2018. № 1. С. 15—22. DOI: 10.21681/1994-1404-2018-1-15-22 .
2. Ващекин А.Н. Оценка согласованности нормативно-правовых актов в процессе консолидации и кодификации законодательства // Информационные отношения и право : сб. науч. тр. Вып. 2. М. : РАП, 2007. С. 51—58.
3. Ващекин А.Н., Ващекина И.В. Математическое обеспечение анализа цифровых площадок в информационном пространстве // Тр. III Междунар. науч.-прак. конф. «Трансформация национальной социально-экономической системы России, тренд цифровые технологии» (4 декабря 2020 г.), РГУП. М. : РГУП, 2021. С. 196—201.
4. Ващекин А.Н., Дзедзинский А.В. Проблемы правового регулирования отношений в цифровом пространстве // Правосудие/Justice. 2020. Т. 2. № 2. С. 126—147. DOI: 10.37399/ issn2686-9241.2020.2.126-147 .
5. Ловцов Д.А. Информационно-правовые основы правоприменения в цифровой сфере // Мониторинг правоприменения. 2020. № 2 (35). С. 44—52. DOI: 10.21681/2226-0692-2020-2-44-52 .
6. Ловцов Д.А. Системологическая база регулирования информационных правоотношений в инфосфере // Российское правосудие. 2023. № S1. С. 154—165. DOI: 10.37399/issn2072-909X.2023.S1.154-165 .
7. Ловцов Д.А. Системный анализ. Часть. 1. Теоретические основы. М. : РГУП, 2018. 224 с. ISBN 978-5-93916-701-7.
8. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
9. Пальянова Н.В. Развитие отрасли Legal Tech в России // Правовая информатика. 2022. № 4. С. 27—38. DOI: 10.21681/1994-1404-2022-4-27-38 .
10. Федосеев С.В. Методика проведения экспертных исследований с использованием методов теории нечетких множеств // Тр. XIX Междунар. науч.-практ. конф. «Инновационные, информационные и коммуникационные технологии» (1—10 октября 2022 г.), МИРЭА. Сочи : ВВИА им. Н.Е. Жуковского, 2022. С. 20—23.

11. Федосеев С.В. Применение математических методов теории нечетких множеств при проведении судебно-экспертных исследований // Правовая информатика. 2020. № 4. С. 38—45. DOI: 10.21681/1994-1404-2020-4-38-45 .
12. Царькова Е.В. Информационно-математическое обеспечение задач «цифровой» экономики в нечетких условиях // Правовая информатика. 2019. № 1. С. 18—28. DOI: 10.21681/1994-1404-2019-1-18-28 .

A METHOD FOR ANALYSING DIGITAL FIELDS GENERATED BY LEGAL INFORMATION SYSTEMS

Andrei Vashchekin, *Ph.D. (Economics), Associate Professor, Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: vaschekin@mail.ru

Irina Vashchekina, *Ph.D. (Economics), Associate Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: *vaschekina@mail.ru*

Viacheslav Kvachko*, Ph.D. (Physics & Mathematics), Associate Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: k3v9@list.ru

Keywords: *information space, digital fields, functional identity, mathematical models, method, graphs, matrices, fuzzy sets, structure, isomorphism.*

Abstract

Purpose of the work: justifying the principles of analysing the digital space elements and algorithmisation of carrying it out based on mathematical methods.

Methods used in the study: system analysis, mathematical modelling, expert evaluation, graph theory, fuzzy set theory.

Study findings: a high degree of self-organisation is identified in information interactions between digital fields actors against a background of imperfect legal regulation of information relations between digital space actors. A general method is put forward for determining the functional identity of some digital fields using models built on the basis of potentially isomorphic algebraic structures, e.g. graphs (directed graphs) and associated matrices (adjacency and incidence matrices, etc.) describing information interactions in this fields. A comparative analysis of digital fields generated by education websites of three legal information systems most used in Russia is carried out as a specific example of applying the method. A justification is given for the conclusion that the digital fields for education systems used by Consultant Plus and Garant are functionally identical but the digital field generated by the Codex system is not identical to both of these.

References

1. Borisov R.S. Effektivnyi algoritm upravleniia pererabotkoi sudebnoi statisticheskoi informatsii. Pravovaia informatika, 2018, No. 1, pp. 15–22. DOI: 10.21681/1994-1404-2018-1-15-22 .
2. Vashchekin A.N. Otsenka soglasovannosti normativno-pravovykh aktov v protsesse konsolidatsii i kodifikatsii zakonodatel'stva. Informatsionnye otnosheniia i pravo : sb. nauch. tr., vyp. 2. M. : RAP, 2007, pp. 51–58.
3. Vashchekin A.N., Vashchekina I.V. Matematicheskoe obespechenie analiza tsifrovykh ploshchadok v informatsionnom prostranstve. Tr. III Mezhdunar. nauch.-prak. konf. "Transformatsiia natsional'noi sotsial'no-ekonomicheskoi sistemy Rossii, trend tsifrovye tekhnologii" (4 dekabria 2020 g.), RGUP. M. : RGUP, 2021, pp. 196–201.
4. Vashchekin A.N., Dzedzinskii A.V. Problemy pravovogo regulirovaniia otnoshenii v tsifrovom prostranstve. Pravosudie/Justice, 2020, t. 2, No. 2, pp. 126–147. DOI: 10.37399/ issn2686-9241.2020.2.126-147 .

5. Lovtsov D.A. Informatsionno-pravovye osnovy pravoprimeneniia v tsifrovoi sfere. Monitoring pravoprimeneniia, 2020, No. 2 (35), pp. 44–52. DOI: 10.21681/2226-0692-2020-2-44-52 .
6. Lovtsov D.A. Sistemologicheskaia baza regulirovaniia informatsionnykh pravootnoshenii v infosfere. Rossiiskoe pravosudie, 2023, No. S1, pp. 154–165. DOI: 10.37399/issn2072-909X.2023.S1.154-165 .
7. Lovtsov D.A. Sistemnyi analiz. Chast'. 1. Teoreticheskie osnovy. M. : RGUP, 2018. 224 pp. ISBN 978-5-93916-896-0, ISBN 978-5-93916-701-7.
8. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
9. Pal'ianova N.V. Razvitie otrasli Legal Tech v Rossii. Pravovaia informatika, 2022, No. 4, pp. 27–38. DOI: 10.21681/1994-1404-2022-4-27-38 .
10. Fedoseev S.V. Metodika provedeniia ekspertnykh issledovanii s ispol'zovaniem metodov teorii nechetkikh mnozhestv. Tr. XIX Mezhdunar. nauch.-prakt. konf. "Innovatsionnye, informatsionnye i kommunikatsionnye tekhnologii" (1–10 oktiabria 2022 g.), MIREA. Sochi : VVIA im. N.E. Zhukovskogo, 2022, pp. 20–23.
11. Fedoseev S.V. Primenenie matematicheskikh metodov teorii nechetkikh mnozhestv pri provedenii sudebno-ekspertnykh issledovanii. Pravovaia informatika, 2020, No. 4, pp. 38–45. DOI: 10.21681/1994-1404-2020-4-38-45 .
12. Tsar'kova E.V. Informatsionno-matematicheskoe obespechenie zadach "tsifrovoi" ekonomiki v nechetkikh usloviiakh. Pravovaia informatika, 2019, No. 1, pp. 18–28. DOI: 10.21681/1994-1404-2019-1-18-28 .

ЭКСПЕРТНОЕ ОЦЕНИВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В БАЗЕ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Алексеев В.В.[1], Дидрих В.Е.[2], Белевитин В.А.[3], Дерябин А.С.[4]

Ключевые слова: *информационная система, база данных, привилегированная информация, защищенность, несанкционированный доступ, экспертная оценка, достоверность, оперативность, веб-приложение, методические рекомендации, коэффициент конкордации, экспертная информация.*

Аннотация

Цель работы: повысить достоверность и оперативность экспертного оценивания защищенности привилегированной информации от несанкционированного доступа в базе данных информационной системы.

Методы исследования: системный анализ, математическое и компьютерное моделирование, экспертное оценивание, программирование.

Результаты: разработаны методические рекомендации по анализу экспертных оценок защищенности информации от несанкционированного доступа в базе данных информационной системы с учетом требований нормативных правовых актов в сфере информационной безопасности; разработанная компьютерная программа и обоснованный порядок проведения экспертного оценивания обеспечивают его необходимую достоверность за счет устранения нерелевантных оценок экспертов, имеющих низкие значения коэффициента конкордации; использование экспертных анкет в веб-приложении, позволяющее уменьшить время от постановки задачи до выполнения ее экспертом, а также автоматизация процессов сбора и обработки экспертной информации позволяют также повысить оперативность экспертной оценки защищенности информации.

EDN: XNKLBE

Введение

В настоящее время *своевременное* получение *достоверных* экспертных оценок *защищенности* [12] информации от несанкционированного доступа (НСД) в базе данных информационной системы представляется особенно актуальным по следующим причинам.

1. *Увеличение угроз кибербезопасности.* Современные информационные системы сталкиваются с растущими угрозами кибербезопасности, такими как хакерские атаки, вредоносное программное обеспечение, киберпреступления и др. [5, 7]. Базы данных, содержащие привилегированную (ценную) информацию, становятся приоритетными целями для злоумышленников. Оценка степени защищенности информации позволяет идентифицировать уязвимости и риски, связанные с базой данных PostgreSQL, и предпринять соответствующие меры по укреплению ее безопасности. Кроме того, современное состояние развития и использования сетевых технологий на базе совершенной импортной компьютерной техники обеспечивает возможность осуществления НСД по *«нетрадиционным информационным каналам»* (*скрытым, англ. covert channel*), «невидимым» для современных средств защиты информации[5] [15, 16] даже при условии использова-

[5] См.: ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. М. : Стандартинформ, 2008; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, ИТ и АС от атак с использованием скрытых каналов. М. : Стандартинформ, 2009.

[1] ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: vvalex1961@mail.ru

[2] ***Дидрих Валерий Евгеньевич,*** *доктор технических наук, профессор, профессор кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: dve54@mail.ru

[3] ***Белевитин Виктор Андреевич,*** *аспирант кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: adamunt@mail.ru

[4] ***Дерябин Андрей Сергеевич,*** *кандидат технических наук, доцент кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: 799980@mail.ru

Таблица 1

Результат обобщения правовых особенностей проведения экспертной оценки

№	Наименование	Содержание
1	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Основные положения о защите информации, включая требования к проведению экспертизы информационной безопасности
2	Постановление Правительства РФ от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»	Порядок проведения работ по обеспечению информационной безопасности, включая формирование экспертных групп
3	Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 21 октября 2021 г. № 1085 «Об утверждении Административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий»	Требования к аккредитации организаций, осуществляющих работы в области защиты информации государственной тайны, включая экспертные группы
4	ГОСТ Р ИСО/МЭК 27004-2021. Национальный стандарт РФ. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание»*	Требования к системам менеджмента информационной безопасности, включая оценку рисков и уязвимостей

* Приказ Росстандарта от 19 мая 2021 г. № 388-ст // СПС «КонсультантПлюс».

ния в эргасистеме сертифицированных и проверенных компонентов.

2. *Несовершенство нормативных правовых актов*. Многие страны и отрасли имеют законодательные требования и регуляторные стандарты, касающиеся защиты информации. Некоторые из них требуют проведения регулярных оценок информационной безопасности, включая базы данных. Соблюдение этих требований обязательно для соответствия закону и предотвращения штрафов или юридических последствий [6].

3. *Недостаточность защиты личных данных*. Базы данных могут содержать конфиденциальные и личные данные пользователей, клиентов или сотрудников. Оценка защиты информации помогает обнаружить уязвимости, которые могут привести к незаконному доступу к этим данным или их утечке. Это позволяет принять меры по защите конфиденциальности и личных данных, соблюдая требования закона и устанавливая доверие среди пользователей [11].

4. *Проблема доверительного взаимодействия*. Нарушение безопасности базы данных может негативно сказаться на бизнес-репутации и доверии клиентов и партнеров. Регулярная (периодическая) оценка степени защищенности привилегированной информации помогает предотвращать нарушения безопасности, минимизирует риски раскрытия конфиденциальной информации и подтверждает готовность организации защищать данные своих клиентов и партнеров [1].

В целом проведение оценки защищенности информации в базе данных информационных систем является важной мерой по обеспечению безопасности данных, соблюдению законодательных требований и защите интересов бизнеса и пользователей информационной системы. При этом одним из основных этапов оценки защищенности информации в базе данных информационной системы является сбор и анализ профессиональных экспертных оценок [8].

Существующие на данный момент системы сбора экспертных оценок обладают рядом *недостатков*, таких как отсутствие возможности детальной настройки анкеты эксперта, блокирования и удаления нерелевантных ответов в зависимости от степени согласованности экспертов, настройки сбора статистики и др. [22]. В связи с этим представляется целесообразным разработать *методические рекомендации по системному анализу* [13] экспертных оценок степени защищенности привилегированной информации в базе данных информационной системы от НСД, которые позволят устранить имеющиеся недостатки и автоматизировать проведение экспертного оценивания.

Особенности экспертного оценивания защищенности информации

При формировании экспертной группы для оценки защищенности информации рекомендуется[6] руководствоваться существующими правовыми актами и регламентами, основные из которых приведены в табл. 1. Важно заметить, что данные правовые документы предоставляют общую основу для формирования экспертной группы и проведения оценки защищенности информации. При конкретном формировании группы и проведении оценки рекомендуется дополнительно учитывать также профильные нормативные правовые акты, руководства и инструкции [17], выпущенные соответствующими регулирующими органами.

При проведении экспертной оценки принимаются меры, направленные на снижение уровня *субъективности* и *неопределенности* при определении каждой из угроз безопасности информации. В связи с этим экспертную оценку рекомендуется проводить в отношении следующих факторов [25]:

- негативного последствия от реализации угроз безопасности информации;
- целей нарушителей по реализации угроз безопасности информации;
- набора сценариев действий нарушителей при реализации угроз безопасности информации.

Оценку факторов рекомендуется проводить опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений («*низкий*», «*средний*», «*высокий*» или «*да*», «*нет*», или иные шкалы). При этом вопросы должны быть четкими и однозначно трактуемыми и предполагать однозначные ответы [25].

Процесс экспертного оценивания включает, как правило, следующие основные этапы [4]:

1. Каждый эксперт проводит оценку оцениваемого параметра (рекомендуется не менее двух раундов оценки), результаты которой заносятся в таблицу.

2. После оценки каждым из экспертов отбрасываются минимальные и максимальные значения.

3. Определяется среднее значение оцениваемого параметра в каждом раунде.

4. Определяется итоговое среднее значение оцениваемого параметра.

Качественное формирование экспертной группы способствует снижению субъективных факторов при оценке угроз безопасности информации [9, 19].

Занижение (ослабление) экспертами прогнозов и предположений при оценке угроз может повлечь наступление непрогнозируемого (неожиданного) ущерба в результате их реализации. *Завышение* экспертами прогнозов и предположений при моделировании угроз безопасности информации может повлечь за собой неоправданные расходы на нейтрализацию (блокирование) угроз, являющихся неактуальными [10].

Независимо от результата формирования экспертной группы существуют субъективные факторы, связанные с особенностью процесса принятия решений при оценке степени защищенности информации в базе данных информационной системы. Это также может приводить как к занижению (ослаблению), так и к завышению (усилению) экспертами прогнозов и предположений при оценке угроз безопасности информации, что в свою очередь может привести к *пропуску* отдельных угроз безопасности информации или к неоправданным затратам на нейтрализацию неактуальных угроз. Любое решение, принимаемое экспертами при оценке угроз безопасности информации, должно исходить из *правил*, при которых нарушитель находится в наилучших условиях для реализации угрозы безопасности («*концепция гарантированной защищенности информации*» [12, 14]).

В состав экспертной группы рекомендуется включать специалистов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций) от подразделения, ответственного за [2]: защиту информации (обеспечение информационной безопасности); цифровую трансформацию (ИТ-специалистов); эксплуатацию сетей связи; эксплуатацию автоматизированных систем управления, а также обладателя информации или оператора, ответственного за выполнение основных (критических) процессов (бизнес-процессов). При этом специалисты должны иметь опыт работы не менее одного года по соответствующему направлению деятельности, в котором проводится оценка угроз безопасности информации [18].

Мнения экспертов часто совпадают не полностью, поэтому необходимо количественно оценивать меру согласованности экспертов и устанавливать причины несовпадения их решений. Для оценки меры согласованности мнений экспертов используются, как правило, коэффициенты конкордации (согласия) [20, 27].

Количественная мера согласованности определяется на основе статистических данных всей группы экспертов. Так, согласованность мнений компетентных экспертов при использовании всех указанных экспертных методов, где определяются ранги объектов, рассчитываются с помощью коэффициента конкордации по формуле [5]:

$$W = \frac{S}{\frac{1}{12}m^2(n^3 - n) - m\sum T_i}, \quad (1)$$

где $T_i = \frac{1}{12}\sum(t_l^3 - t^3)$ — число связок (видов повторяющихся элементов) в оценках i-го эксперта (если нет связанных рангов, то T_i равно нулю); t_l — количество элементов в l-й связке для i-го эксперта (количество повторяющихся элементов); m — число анализируемых порядковых переменных; n — количество экспертов, S — сумма квадратов отклонений, рассчитываемая по формуле (2):

[6] Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).

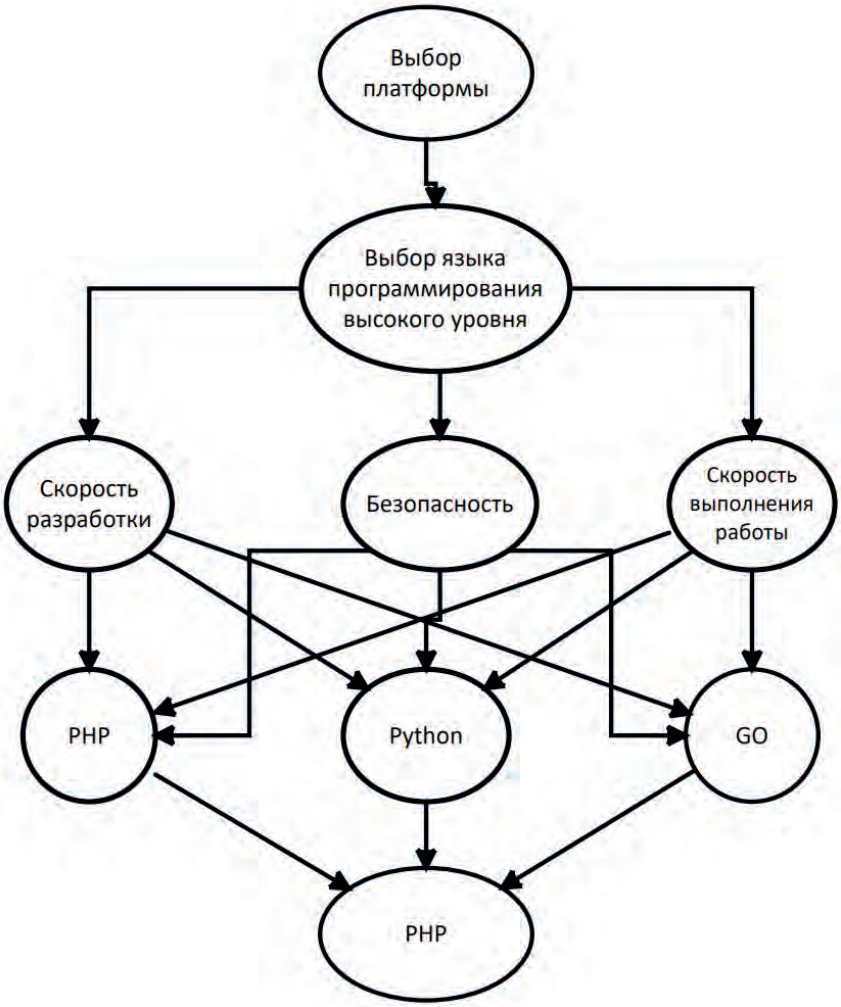


Рис. 1. Структура процесса принятия решения при выборе языка программирования высокого уровня

$$S = \sum_{i=1}^{n} r_{ij}^2 - \frac{(\sum_{i=1}^{n} r_{ij})^2}{n}, \quad (2)$$

где r_{ij} — расставленные ранги суждений группы экспертов; j — номер задания.

Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения. Не рекомендуется формировать экспертную группу из участников, находящихся в прямом подчинении, из-за возможного наличия психологического давления, так как это может негативным образом повлиять на результат определения угроз безопасности информации. В состав экспертной группы должны входить не менее трех экспертов [3].

Методические рекомендации по анализу экспертных оценок защищенности информации

При разработке методических рекомендаций были обоснованно учтены следующие основные требования и ограничения:

- возможность исключать оценки экспертов из статистики в зависимости от значения коэффициента конкордации;
- обеспечение требований кроссплатформенности;
- отсутствие территориальных ограничений при взаимодействии с приложением.

Разработанные методические рекомендации базируются на следующей логической последовательности основных этапов:

1. Обоснование платформы для создания автоматизированной системы сбора и анализа экспертной информации.
2. Разработка системы сбора и анализа экспертной информации.
3. Получение экспертной оценки.
4. Верификация полученной оценки.

На *первом* этапе реализации методических рекомендаций определяется возможный набор технологий для разработки системы сбора и анализа экспертных оценок. Для начала необходимо выбрать тип будущего приложения. Существует два основных вида — это дес-

ктопное приложение и веб-приложение [21]. В соответствии с обоснованными требованиями и принятыми ограничениями выбрана разработка веб-приложения вместо десктопного решения.

На *втором* этапе определяется основной язык программирования, используемый для веб-разработок. Одним из основных факторов определения приемлемого языка программирования является возможность поддержки созданного продукта в течение долгого периода времени. Столь же важным является наличие проверенных библиотек, которые позволят как сократить время разработки, так и повысить безопасность данного решения [23].

Выбор языка программирования высокого уровня можно осуществить с применением системы поддержки принятия решений «Выбор»[7]. На рис. 1 представлена структура процесса принятия решения при выборе приемлемого языка программирования высокого уровня с применением системологического *метода анализа иерархий* [13], включая уровень целей (определение языка программирования высокого уровня), уровень критериев (скорость разработки, безопасность, скорость выполнения программы) и уровень альтернатив (языки программирования PHP, Python, Go).

Например, скорость выполнения программы выше у языков Go и Python по сравнению с PHP. Скорость разработки и безопасность за счет большего количества проверенных библиотек выше у PHP по сравнению с Go и Python. После попарного сравнения всех критериев в программе «Выбор» было определено, что язык высокого уровня PHP набирает 0,778 балла, по сравнению с 0,145 у Python и 0,076 у Go, следовательно, язык PHP наиболее приемлем для разработки веб-приложения с обоснованными требованиями и принятыми ограничениями.

Для сокращения времени на разработку системы возможно использование фреймворка Laravel, который представляет широкий набор инструментов для быстрой и безопасной разработки. Для хранения результатов опросов в текстовом виде можно использовать (в соответствии с обоснованными требованиями и принятыми ограничениями) безопасную и быстродействующую реляционную СУБД PostgreSQL [21, 23].

Созданные опросы хранятся (рис. 2) в таблице surveys, вопросы к опросам и их части сохраняются в таблицах questions и sections. Такая схема позволяет просто добавлять и удалять вопросы в опросах. Пройденные опросы сохраняются в таблицу entries. Ответы на вопросы экспертов добавляются в таблицу answers. То есть база данных веб-приложения состоит из пяти взаимосвязанных таблиц.

Для прохождения опроса каждый эксперт должен авторизоваться на сайте. Если у эксперта нет аккаунта, он не сможет пройти опрос. Аккаунты могут создаваться как самими пользователями, так и только администратором для повышения безопасности. Вход осуществляется с помощью комбинации электронной почты и пароля.

Третий этап — получение экспертной оценки с помощью разработанной компьютерной программы. После входа в программу у каждого эксперта на экране выводится окно «Задания». В этом окне представлен перечень активных заданий. Эксперт, выбрав задание, осуществляет оценку.

Каждый добавленный опрос автоматически создает задание для всех активных экспертов. При необходимости имеется возможность выдавать задания только определенным пользователям.

В процессе выполнения одного из заданий на странице опроса эксперту достаточно в качестве оценки поставить число по 10-балльной шкале. Такой подход позволяет сократить время проведения экспертной оценки. Количество заданий, опросов и вопросов в них неограничено. Вопросы могут быть различного типа: числовые, текстовые, с одним или несколькими вариантами ответа.

В каждом опросе есть также возможность добавить проверку вводимых данных. Например, если пользователю необходимо оценить качество показателя по десятибалльной шкале, то правила валидации для ответа будут иметь следующий вид:

'rules' => [*'numeric'*, 'min:0', 'max:10'], (3)

где *'rules'* — массив правил валидации; 'numeric' — тип данных; min, max — минимальное и максимальное значение для данных типов данных соответственно.

При попытке эксперта ввести значения, выходящие за этот диапазон, система отобразит ошибку и не позволит завершить опрос. После валидации полученных ответов и завершения опроса эксперт попадает опять в личный кабинет. Завершенный опрос исчезает из заданий и считается выполненным. Каждый эксперт проходит опрос только один раз и в будущем не может изменить свои ответы.

Окно «Статистика» доступно только администратору (рис. 3).

Во вкладке «Статистика» отображается статистика по прохождению опросов: *среднее значение* каждого ответа, за исключением максимальных и минимальных значений в опросе, и *количество пользователей,* прошедших опрос. Статистика выводится в режиме реального времени. Если данных будет слишком много, есть возможность обновления статистики через определенные промежутки времени, что снизит нагрузку на базу данных. Но, как правило, экспертные команды относительно небольшие, что не создаст серьезной нагрузки на базу данных. Данные по статистике обезличены. Статистика об опросе появляется после того, как хотя бы один эксперт успешно прошел его, и выводится автоматически.

На *четвертом* этапе экспертные оценки верифицируются. Для верификации результатов оценки существует экран «Эксперты». На экране отображаются все

[7] Малтугуева Г.С., Юрин А.Ю., Дородных Н.О. Система поддержки принятия решений «Выбор» // Информационные технологии и системы. 2017. С. 163—166.

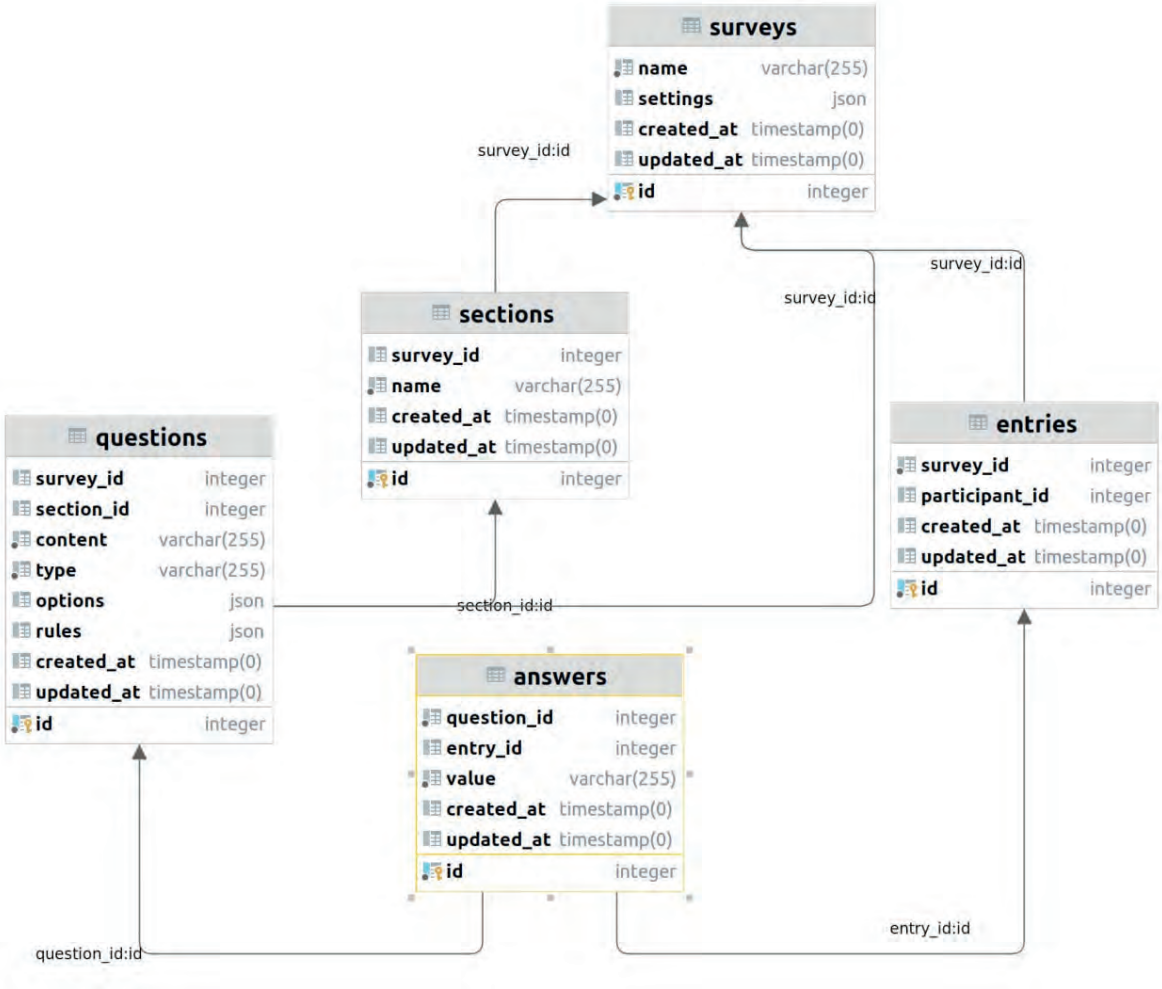


Рис. 2. Схема базы данных веб-приложения

пользователи системы (рис. 4). У каждого пользователя отображается также коэффициент согласованности. В зависимости от его значения администратор системы может принять решение о блокировании пользователя или его разблокировании. Результаты ответов экспертов с показателем конкордации, выходящим за пределы допустимых значений, установленным администратором, блокируются, и результаты их оценки не учитываются в статистике.

Численный пример

Приведем *численный пример* проведения экспертной оценки защищенности информации в информационной системе с помощью разработанных методических рекомендаций. Предположим, что необходимо провести оценку защищенности (уязвимости) информации от НСД в базе данных информационной системы. Имеется тест с пятью вопросами и пять экспертов, каждый из которых выставляет оценку от 1 до 10 баллов для каждого вопроса. Результат проведенных оценок экспертов представлен в табл. 2.

Рассчитаем число T_i связок в оценках i-го эксперта следующим образом:

$T_1 = [(2^3 — 2)]/12 = 0{,}5;$

$T_2 = [(3^3 — 3)]/12 = 2;$

$T_3 = [(2^3 — 2)]/12 = 0{,}5;$

$T_4 = [(2^3 — 2) + (2^3 — 2)]/12 = 1;$

$T_5 = [(2^3 — 2)]/12 = 0{,}5;$

$\Sigma T_i = 0{,}5 + 2 + 0{,}5 + 1 + 0{,}5 = 4{,}5.$

Так как в матрице имеются связанные ранги, произведем их переформирование. На основании переформирования рангов строится новая матрица рангов в табл. 3, используя формулу (4):

$$d = \sum r_{ij} — 15, \quad (4)$$

где $\sum r_{ij}$ — сумма рангов; 15 — сумма столбцов матрицы из табл. 3.

Исходя из матрицы рангов, сумма отклонений (S) для данных экспертов равняется 193,5.

Вычисляем коэффициент конкордации по формуле (1), используя данные из табл. 2 ($n = 5$, $m = 5$):

$$W = \frac{193.5}{\frac{1}{12}5^2(5^3 - 5) - 5 \times 4.5} = 0{,}85.$$

Название анкеты: "Защита базы данных"

Задание	Средняя оценка
1) Оцените защиту базы данных от sql-инъекций по 10 бальной шкале	4.4
2) Оцените защиту базы данных от физического проникновения по 10 бальной шкале	3.8

Количество респондентов: 5

Название анкеты: "Уязвимость информации"

Задание	Средняя оценка
1) Оцените защиту данных по 10 бальной шкале	4
2) Оцените риск прониковения в базу данных по 10 бальной шкале	5.33

Количество респондентов: 3

Название анкеты: "Оценка"

Задание	Средняя оценка
Оценка	7
Оценка	8

Количество респондентов: 2

Рис. 3. Вкладка «Статистика» в личном кабинете администратора

Активные эксперты

ФИО	Почта	Количество пройденных опросов	Оценка согласованности	Действия
Белевитин Виктор Андреевич	adamunt@mail.ru	2	0.67	Заблокировать
Иванова Диана Андреевна	adamunt2@mail.ru	1	0.67	Заблокировать

Неактивные эксперты

ФИО	Почта	Количество пройденных опросов	Оценка согласованности	Действия
Венедиктов Иван Алексеевич	dianamoiseeva56540@gmail.com	3	0.67	Разблокировать

Рис. 4. Список пользователей системы

Рассчитанное значение коэффициента конкордации $W = 0{,}85$ говорит о высокой согласованности мнений экспертов.

Рассчитаем также средний балл экспертной оценки для каждого вопроса, используя только оценки, которые остались после удаления максимальной и минимальной величин. Получаем окончательную оценку степени защищенности информации от НСД в базе данных информационной системы, усредняя средние баллы оценки экспертов по всем вопросам:

$O_c = (6{,}6 + 6{,}6 + 8{,}4 + 5 + 7{,}4) / 5 = 6{,}8$ балл.

Полученная оценка (6,8 *балл* из 10 возможных) степени защищенности информации в информационной системе — приемлемая. Эта оценка может служить показателем при сравнении степени информационной защищенности подобных систем. В дальнейшем целесообразно эту оценку использовать при анализе слабых сторон информационной системы и определения мер по ее повышению.

Заключение

Таким образом, рассмотрены результаты разработки и апробации методических рекомендаций по анализу экспертных оценок защищенности привилегированной информации в базе данных информационной системы от НСД с учетом требований существующих нормативных правовых актов в сфере информационной безопасности и необходимой степени согласованности экспертов на основе коэффициента конкордации.

Данные методические рекомендации позволяют в значительной степени сократить время сбора экс-

Таблица 3

Матрица рангов после переформирования

Факторы	Эксперты					Сумма рангов	*d*	d^2
	1	2	3	4	5			
r_{11}	3,5	3	2	1,5	3,5	13,5	-1,5	2,25
r_{21}	2	3	3	3	2	13	-2	4
r_{31}	5	5	4,5	4,5	5	24	9	81
r_{41}	1	1	1	1.5	1	5,5	-9,5	90,25
r_{51}	3,5	3	4,5	4,5	3,5	19	4	16
∑	15	15	15	15	15	75		**193,5**

пертных оценок в информационной системе за счет возможности гибкой настройки вариантов вопросов. Создание опросов для экспертов в веб-приложении позволяет уменьшить время от постановки задачи до выполнения ее экспертом. Уровень согласованности экспертов позволяет определить членов экспертной группы, которые обладают наименьшей степенью согласованности, и исключить результаты их оценки. Процесс исключения экспертов в зависимости от их коэффициента конкордации приводит к устранению нерелевантных оценок и повышает степень *достоверности* [12] общей оценки степени защищенности информации.

Встроенный интерфейс статистики позволяет в режиме реального времени анализировать полученные результаты и использовать их при оценке степени защищенности информации. Автоматизация расчета статистики также позволяет повысить *оперативность* и *экономичность* анализа экспертной информации.

Рецензент: ***Федосеев Сергей Витальевич,*** *кандидат технических наук, доцент, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*
E-mail: fedsergvit@mail.ru

Литература

1. Алексеева Ю.А., Смолькин А.С. Социальные аспекты риска: исследование риска информационных технологий // Управление рисками в экономике: проблемы и решения (РИСК'Э-2019). 2020. С. 38—41.
2. Антамошкин О.А., Пузанова Г.А., Онтужев В.В. Особенности проектирования автоматизированной системы экспертной оценки информационной безопасности организаций // Сибирский аэрокосмический журнал. 2013. № 3 (49). С. 4—8.
3. Белевитин В.А. Эффективность защиты информации на основе нечетких рисков // Мир науки без границ. 2022. С. 232—235.
4. Быков А.А., Киселева О.М., Кириллова М.А. Элементы оценки эффективности систем информационной безопасности предприятия // Труды V Юбил. Всеросс. науч.-прак. конф. с межд. участием «Вызовы цифровой экономики» (20 мая 2022 г.) / Брянский гос. инж.-технол. ун-т. Брянск : БГИТУ, 2022. С. 355—359.
5. Головань С.А., Русакова О.И. Анализ кибербезопасности в контексте современных угроз // Управленческий учет. 2022. № 10-2. С. 496—504.
6. Илларионова Т.М. Процесс нечёткого оценивания в многокритериальных экспертных оценках // Научный вестник МГТУ ГА. 2009. № 140. С. 1—3.
7. Ильин Д.Ю. Методика выбора компонентов стека технологий цифровых платформ на основе нечеткой логики // Вестник СибГУТИ. 2020. № 3 (51). С. 38—46.
8. Камалова Г.Г. Проблемы и приоритетные направления организационно-правового обеспечения конфиденциальности информации при использовании цифровых технологий // Вестник Университета им. О.Е. Кутафина. 2019. № 12 (64). С. 45—52.

9. Карасев О.И., Муканина Е.И. Метод экспертных оценок в форсайт-исследованиях // Статистика и экономика. 2019. № 4. С. 4—13.
10. Кузьмин И.Е., Баранова Е.М., Баранов А.Н., Борзенкова С.Ю. К вопросу рекомендаций оптимального качественного и количественного формирования экспертной рабочей группы для решения задач информационной безопасности // Изв. Тульского гос. ун-та. Технические науки. 2020. № 12. С. 103—107.
11. Кузьмин И.Е. Проблема значимости согласованности мнений экспертов рабочей группы при моделировании угроз безопасности информации // Изв. Тульского гос. ун-та. Технические науки. 2021. № 3. С. 254—260.
12. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
13. Ловцов Д.А. Системный анализ. Часть. 1. Теоретические основы. М. : РГУП, 2018. 224 с. ISBN 978-5-93916-701-7.
14. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74 .
15. Ловцов Д.А., Ермаков И.В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // Науч.-техн. инф. РАН. Сер. 3. Информ. процессы и системы. 2005. № 3. С. 1—7.
16. Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // Науч.-техн. инф. РАН. Сер. 3. Информ. процессы и системы. 2006. № 9. С. 1—9.
17. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54 .
18. Мамцов К.Г., Ачилов Н.Р. Киберпреступность как угроза национальной безопасности // Молодой исследователь Дона. 2022. № 1 (34). С. 42—45.
19. Милько Д.С., Данеев А.В., Горбылев А.Л. База знаний экспертной системы оценки угроз безопасности информации // Доклады Томского гос. ун-та систем управления и радиоэлектроники. 2022. Т. 25. № 1. С. 61—69.
20. Паршин И.И. Моделирование задачи определения зависимости согласованности мнения экспертов от численного состава экспертной группы // Вестник современных исследований. 2019. № 1.8 (28). С. 142—145.
21. Семенова З.В., Любич С.А., Кузнецов А.Г., Мальцев П.А. Система автоматизированной проверки правильности составления SQL-запросов: защита от уязвимостей // Динамика систем, механизмов и машин. 2017. № 4. С. 90—95.
22. Федосеев С.В. Инфологическая модель комплекса средств автоматизации компьютерных деловых игр в экспертной деятельности // Правовая информатика. 2019. № 4. С. 40—49. DOI: 10.21681/1994-1404-2019-4-40-49 .
23. Чернов А.Е. Основные требования и принципы, учитываемые при разработке и внедрении политики информационной безопасности // Вестник науки. 2023. Т. 2. № 6 (63). С. 693—699.
24. Erulanova A. et al. Expert system for assessing the efficiency of information security. 2020. 7th International Conference on Electrical and Electronics Engineering (ICEEE). IEEE, 2020. Pp. 355–359.
25. Haji S., Tan Q., Costa R.S. A hybrid model for information security risk assessment. Int. j. adv. trends comput. sci. eng. 2019. № ART-2019-111611. Pp. 100–106.
26. Schönig H.J. Mastering PostgreSQL 12: Advanced techniques to build and administer scalable and reliable PostgreSQL database applications. Packt Publishing Ltd, 2019. P. 56–67.
27. Seng L.K., Ithnin N., Said S.Z.M. The approaches to quantify web application security scanners quality: a review // International Journal of Advanced Computer Research. 2018. V. 8. No. 38. Pp. 285–312.

EXPERT EVALUATION OF INFORMATION PROTECTION IN AN INFORMATION SYSTEM DATABASE

Vladimir Alekseev, *Dr.Sc. (Technology), Professor, Head of the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: vvalex1961@mail.ru

Valerii Didrikh, *Dr.Sc. (Technology), Professor at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: dve54@mail.ru

Viktor Belevitin, *Ph.D. student at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: adamunt@mail.ru

Andrei Deriabin, *Ph.D. (Technology), Associate Professor at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: 799980@mail.ru

Keywords: *information system, database, privileged information, protection, unauthorised access, expert estimate, reliability, promptness, web application, methodological recommendations, concordance coefficient, expert information.*

Abstract

Purpose of the work: increasing the reliability and promptness of expert evaluation of protection of privileged information against unauthorised access in an information system database.

Methods used in the study: system analysis, mathematical modelling and computer simulation, expert evaluation, programming.

Study findings: methodological recommendations are worked out for analysing expert estimates of protection of information against unauthorised access in an information system database considering the requirements of legal regulations in the information security field. The developed software and a justified procedure for carrying out the expert evaluation ensure the needed reliability due to the elimination of irrelevant expert estimated with a low concordance coefficient value. Using expert questionnaires in a web application which allows to reduce the time from setting the task to its fulfilment by the expert as well as the automation of the processes of gathering and processing expert information makes it possible also to increase the promptitude of the expert evaluation of information protection.

References

1. Alekseeva Iu.A., Smol'kin A.S. Sotsial'nye aspekty riska: issledovanie riska informatsionnykh tekhnologii. Upravlenie riskami v ekonomike: problemy i resheniia (RISK'E-2019), 2020, pp. 38–41.
2. Antamoshkin O.A., Puzanova G.A., Ontuzhev V.V. Osobennosti proektirovaniia avtomatizirovannoi sistemy ekspertnoi otsenki informatsionnoi bezopasnosti organizatsii. Sibirskii aerokosmicheskii zhurnal, 2013, No. 3 (49), pp. 4–8.
3. Belevitin V.A. Effektivnost' zashchity informatsii na osnove nechetkikh riskov. Mir nauki bez granits, 2022, pp. 232–235.
4. Bykov A.A., Kiseleva O.M., Kirillova M.A. Elementy otsenki effektivnosti sistem informatsionnoi bezopasnosti predpriiatiia. Trudy V Iubil. Vseross. nauch.-prak. konf. s mezhd. uchastiem "Vyzovy tsifrovoi ekonomiki" (20 maia 2022 g.), Brianskii gos. inzh.-tekhnol. un-t. Briansk : BGITU, 2022, pp. 355–359.
5. Golovan' S.A., Rusakova O.I. Analiz kiberbezopasnosti v kontekste sovremennykh ugroz. Upravlencheskii uchet, 2022, No. 10-2, pp. 496–504.
6. Illarionova T.M. Protsess nechetkogo otsenivaniia v mnogokriterial'nykh ekspertnykh otsenkakh. Nauchnyi vestnik MGTU GA, 2009, No. 140, pp. 1–3.
7. Il'in D.Iu. Metodika vybora komponentov steka tekhnologii tsifrovykh platform na osnove nechetkoi logiki. Vestnik SibGUTI, 2020, No. 3 (51), pp. 38–46.
8. Kamalova G.G. Problemy i prioritetnye napravleniia organizatsionno-pravovogo obespecheniia konfidentsial'nosti informatsii pri ispol'zovanii tsifrovykh tekhnologii. Vestnik Universiteta im. O.E. Kutafina, 2019, No. 12 (64), pp. 45–52.
9. Karasev O.I., Mukanina E.I. Metod ekspertnykh otsenok v forsait-issledovaniiakh. Statistika i ekonomika, 2019, No. 4, pp. 4–13.
10. Kuz'min I.E., Baranova E.M., Baranov A.N., Borzenkova S.Iu. K voprosu rekomendatsii optimal'nogo kachestvennogo i kolichestvennogo formirovaniia ekspertnoi rabochei gruppy dlia resheniia zadach informatsionnoi bezopasnosti. Izv. Tul'skogo gos. un-ta. Tekhnicheskie nauki, 2020, No. 12, pp. 103–107.
11. Kuz'min I.E. Problema znachimosti soglasovannosti mnenii ekspertov rabochei gruppy pri modelirovanii ugroz bezopasnosti informatsii. Izv. Tul'skogo gos. un-ta. Tekhnicheskie nauki, 2021, No. 3, pp. 254–260.
12. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
13. Lovtsov D.A. Sistemnyi analiz. Chast'. 1. Teoreticheskie osnovy. M. : RGUP, 2018. 224 pp. ISBN 978-5-93916-701-7.
14. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66–74. DOI: 10.21681/1994-1404-2017-3-66-74 .
15. Lovtsov D.A., Ermakov I.V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme. Nauch.-tekhn. inf. RAN, ser. 3. Inform. protsessy i sistemy, 2005, No. 3, pp. 1–7.

16. Lovtsov D.A., Ermakov I.V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. Nauch.-tekhn. inf. RAN, ser. 3. Inform. protsessy i sistemy, 2006, No. 9, pp. 1–9.
17. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Pravovaia informatika, 2017, No. 2, pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .
18. Mamtsov K.G., Achilov N.R. Kiberprestupnost' kak ugroza natsional'noi bezopasnosti. Molodoi issledovatel' Dona, 2022, No. 1 (34), pp. 42–45.
19. Mil'ko D.S., Daneev A.V., Gorbylev A.L. Baza znanii ekspertnoi sistemy otsenki ugroz bezopasnosti informatsii. Doklady Tomskogo gos. un-ta sistem upravleniia i radioelektroniki, 2022, t. 25, No. 1, pp. 61–69.
20. Parshin I.I. Modelirovanie zadachi opredeleniia zavisimosti soglasovannosti mneniia ekspertov ot chislennogo sostava ekspertnoi gruppy. Vestnik sovremennykh issledovanii, 2019, No. 1.8 (28), pp. 142–145.
21. Semenova Z.V., Liubich S.A., Kuznetsov A.G., Mal'tsev P.A. Sistema avtomatizirovannoi proverki pravil'nosti sostavleniia SQL-zaprosov: zashchita ot uiazvimostei. Dinamika sistem, mekhanizmov i mashin, 2017, No. 4, pp. 90–95.
22. Fedoseev S.V. Infologicheskaia model' kompleksa sredstv avtomatizatsii komp'iuternykh delovykh igr v ekspertnoi deiatel'nosti. Pravovaia informatika, 2019, No. 4, pp. 40–49. DOI: 10.21681/1994-1404-2019-4-40-49 .
23. Chernov A.E. Osnovnye trebovaniia i printsipy, uchityvaemye pri razrabotke i vnedrenii politiki informatsionnoi bezopasnosti. Vestnik nauki, 2023, t. 2, No. 6 (63), pp. 693–699.
24. Erulanova A. et al. Expert system for assessing the efficiency of information security. 2020. 7th International Conference on Electrical and Electronics Engineering (ICEEE). IEEE, 2020. Pp. 355–359.
25. Haji S., Tan Q., Costa R.S. A hybrid model for information security risk assessment. Int. j. adv. trends comput. sci. eng. 2019, No. ART-2019-111611. Pp. 100–106.
26. Schönig H.J. Mastering PostgreSQL 12: Advanced techniques to build and administer scalable and reliable PostgreSQL database applications. Packt Publishing Ltd, 2019. P. 56–67.
27. Seng L.K., Ithnin N., Said S.Z.M. The approaches to quantify web application security scanners quality: a review. International Journal of Advanced Computer Research. 2018. V. 8. No. 38. Pp. 285–312.

РАЗВИТИЕ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ПРЕЦЕДЕНТОВ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СТРУКТУРАХ

Бурый А.С.[1], Усцелемов В.Н.[2]

Ключевые слова: *распределенная информационная система, прецедент, информационная безопасность, риск, поддержка принятия решений, система на основе рассуждений, классификатор, метод, модель, алгоритм, сходство.*

Аннотация

Цель работы: развитие адаптивных механизмов подсистемы информационной безопасности в организационных системах поддержки принятия решений на основе метода построения выводов по прецедентам, а также оценки динамики информационного конфликтного взаимодействия, отличающейся возможностью выработки управляющего воздействия для настройки (перенастройки) механизмов подсистемы информационного обмена.

Методы: комплексное использование системного и сравнительного анализа, методов обеспечения информационной безопасности, метода построения рассуждений на основе прецедентов, концептуально-логического обоснования структур построения распределенных информационных систем.

Результаты: обоснован концептуально-методический подход к построению гибридных процедур формирования баз прецедентов на основе метода рассуждений, сочетания метрических методов классификации инцидентов информационной безопасности и алгоритмов экспертного оценивания объектов классификации в задачах мониторинга информационных ресурсов интегрированных информационных структур заданной предметной области; разработана формально-логическая модель настройки подсистемы информационной безопасности на основе рассуждений по прецедентам с использованием модифицированного метода k-ближайших соседей; обоснована рациональная структура базы прецедентов и эффективный алгоритм поиска прецедентов.

EDN: XTRUMB

Введение

Одной из характерных особенностей информации является множество различных форм ее существования, проявления и представления [11]. С одной стороны, это позволяет использовать и развивать организационные подходы к построению *распределенных информационных систем*, совершенствовать их информационное, модельно-алгоритмическое, техническое и др. обеспечение, формировать *требования* к информационным ресурсам и технологиям. С другой стороны, появляется дополнительная опасность при обращении с информацией в контурах управления и принятия решений, связанная с необходимостью обеспечить ее *сохранность* в условиях различного рода воздействий (случайных и преднамеренных).

Процесс построения эффективной *подсистемы защиты* информационной системы часто представляет собой очень трудоемкий процесс. Это обусловлено тем, что необходимо предусмотреть широкий спектр возможных традиционных и *нетрадиционных*[3] *угроз и средств, способных им противодействовать [13].*

С появлением сетевых структур и внедрением интернет-технологий возможными причинами отказов и сбоев в работе аппаратно-программных средств стали не только неисправное техническое (программно-логическое) состояние, но и деструктивные действия злоумышленников с целью несанкционированного по-

[3] Начиная с 70-х гг. прошлого века несанкционированный доступ к привилегированной информации осуществляется, как правило, по так называемым скрытым каналам (covert channel), эффективная защита от которого представляется крайне затруднительной. См.: ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. М. : Ростехрегулирование, 2008. 24 с.; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 2. Рекомендации по организации защиты. М. : Ростехрегулирование, 2009. 26 с.

[1] ***Бурый Алексей Сергеевич,*** *доктор технических наук, эксперт Российской академии наук, директор департамента ФГБУ «Российский институт стандартизации», г. Москва, Российская Федерация.*

E-mail: a.s.burij@gostinfo.ru

[2] ***Усцелемов Вячеслав Николаевич,*** *научный сотрудник, соискатель ФГБУ «Российский институт стандартизации», г. Москва, Российская Федерация.*

E-mail: ustselemov@mail.ru

лучения информации или ее уничтожения, изменения и др. С этим связано обеспечение информационной безопасности как механизма «защиты конфиденциальности, целостности и доступности информации»[4]. Организационные и технические меры защиты информации, реализованные в рамках системы (подсистемы) информационной безопасности (ПИБ), например, АСУ технологическими процессами (ТП), должны быть направлены на обеспечение конфликтной устойчивости [9] и исключение [4]: неправомерного доступа, копирования, модифицирования информации, неправомерного блокирования информации.

Практически безграничные возможности глобальной телематической сети Интернет подтверждают глобальную угрозу виртуальных преступлений, кибертерроризма, а широкое использование информационно-коммуникационных технологий (ИКТ) делают информационные ресурсы наиболее привлекательной целью подобных действий [1].

Основываясь на целевых задачах информационных систем, будем понимать под *информационной безопасностью* свойство объекта (субъекта), характеризующее степень защищенности его потребностей и интересов в качественной (ценной) информации, необходимой ему для устойчивого функционирования и развития (обучения, анализа данных и др.) [13].

Наличие «противоречия» между требованиями по защите информации и открытостью государственных данных, обеспечения их целостности и доступности лишь на первый взгляд выступают в роли именно «противоречия». *Открытость* предполагает возможность при выполнении ряда пользовательских условий получения, внесения изменений и иных действий в открытых информационных ресурсах [15], осуществляя конфиденциальный *электронный документооборот* [12] с использованием электронной цифровой подписи и др., реализуемых в составе российского сегмента сети Интернет, обеспечения информационной безопасности государственных систем, например, Государственной автоматизированной системы РФ «Правосудие» [13].

Необходимость выявления действий злоумышленников на ранней стадии, предотвращая возможные атаки, привела к разработке *систем автоматизированного мониторинга* [2] событий информационной безопасности, ведения киберразведки, фиксации инцидентов безопасности для обучения ПИБ, основываясь в том числе и на *индикаторах компрометации*[5], сигнализирующих, что атака произошла и необходимо проверить ее последствия [16]. Создание базы ранее выявленных случаев преднамеренных воздействий (прецедентов) или атак и их попыток позволяет каждый раз анализировать новые воздействия на предмет того, являются ли они некоторым «повторением прошлого» [17, 21], повышая качество обнаружения атак и их предупреждения.

Интеграция данных и знаний в информационных системах выступают доминантой развития ИКТ, киберфизических систем как на уровне отдельной системы, например, локальной эргатической системы [3, 13], так и на уровне крупномасштабных систем (на примере «системы систем», в качестве которой можно рассматривать информационные структуры «умного города» [3, 4]), автоматизированных телематических сетей в контурах управления сложными динамическими объектами [13, 18] и поддержки принятия решений в них [22].

Предметной целью данного исследования является развитие адаптивных механизмов подсистемы информационной безопасности в организационных системах поддержки принятия решений на основе метода вывода по прецедентам, а также оценки динамики информационного конфликтного взаимодействия, отличающейся возможностью выработки управляющего воздействия для настройки (перенастройки) механизмов подсистемы информационного обмена, на основе оценки возможности сохранения целостности информационных ресурсов различного уровня.

Анализ угроз информационной безопасности

Для анализа угроз информационной безопасности будем исходить из того, что воздействие угроз изменяет состояние распределенной информационной системы (РИС), которое может проявляться в изменении ее количественных или качественных показателей.

Состояние информационной системы в каждый момент времени можно представить вектором $x(t)$ переменных. Разделим все множество состояний РИС на множество $D(t)$ безопасных состояний и множество $N(t)$ небезопасных состояний, т.е. $x(t) = D(t) \cup N(t)$.

Безопасное состояние РИС — это состояние[6], при котором значения параметров системы не выходят из диапазона значений, принятых как безопасные для конкретной РИС.

Небезопасное состояние РИС — это состояние РИС, характеризующееся критичными изменениями значений ее параметров, которые могут привести к преодолению нарушителем подсистемы защиты.

Тогда одной из основных функций подсистемы защиты является поддержание значений вектора $x(t)$ в области допустимых состояний $D(t)$. Появление пограничных и небезопасных состояний РИС, когда вектор $x(t) \notin D(t)$, связано с рисками деструктивных воздействий на РИС.

[4] ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов (Введ. 2015-05-29).

[5] Индикаторы компрометации (*indicators of compromise, IoC*) — технические данные, которые можно использовать для идентификации действий или инструментов атакующих (например, имена хостов, доменные имена, IP-адреса и др.).

[6] Пункт 3.1.2 ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения (Введ. 2009-01-10).

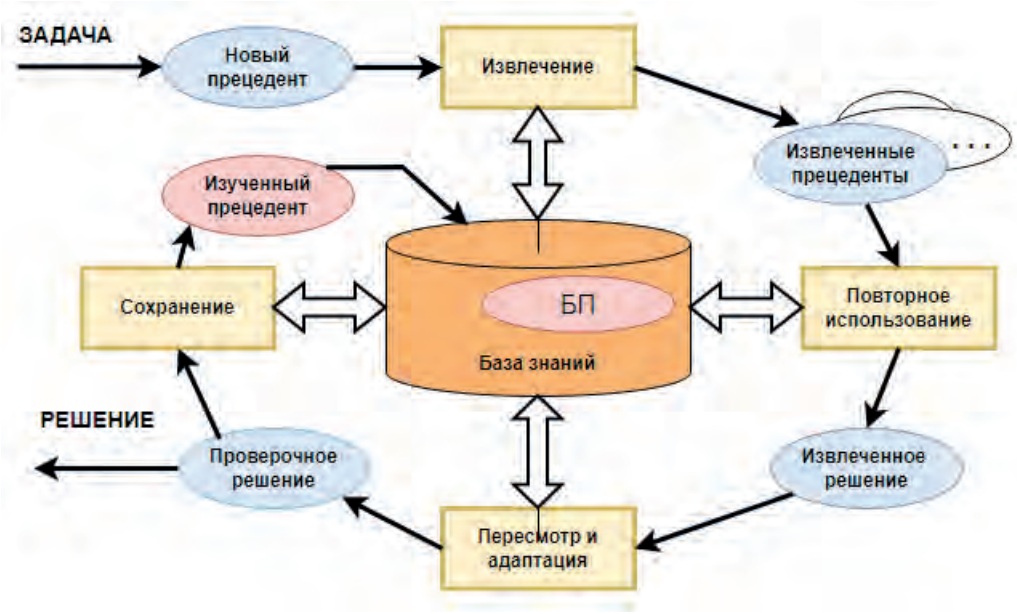


Рис. 1. Структура CBR- цикла рассуждений по прецедентам

Для повышения эффективности функционирования ПИБ целесообразно обеспечивать ее *адаптивную настройку*. Одним из решений указанной задачи является использование при построении и дальнейшей эксплуатации ПИБ формально-логических моделей, позволяющих на основе изменения значений ее параметров оценивать *риск* воздействия угрозы, на основе чего осуществлять настройку механизмов ПИБ.

Проведенный анализ показал [7, 17], что задачи рассматриваемого класса достаточно эффективно решаются на основе использования *методов правдоподобного вывода*, которые позволяют найти рациональное решение в условиях заданных ограничений. Достоинствами указанных методов являются: возможность использования опыта, накопленного системой без интенсивного привлечения экспертов, возможность сокращения времени поиска решения за счет использования уже имеющего решения подобной задачи, возможность применения эвристик, повышающих эффективность процесса поиска решений.

Оценка информационных рисков на основе рассуждений по прецедентам

В основе применения «методов правдоподобного вывода» лежит идея построения «модели рассуждений по прецедентам» (CBR — Case Based Reasoning) [7, 23]. Модели рассуждений являют собой развитие идей логического вывода, решавших подобные задачи в прошлом, применяемые в экспертных системах.

Данный *концептуально-методический подход* позволяет решать новую задачу на основе использования или адаптации решения известной подобной задачи, т. е. использовать опыт, накопленный в решении таких задач.

Методы рассуждений на основе прецедентов включают четыре основных этапа, образующих так называемый *CBR*-цикл, структура которого представлена на *рис*. 1.

Основными этапами *CBR*-цикла являются [20]:

- извлечение наиболее релевантных прецедентов для текущей ситуации из *библиотеки прецедентов* (БП);
- повторное использование извлеченного прецедента для попытки решения текущей задачи;
- пересмотр и адаптация в случае необходимости полученного решения применительно к условиям текущей проблемной ситуации;
- сохранение вновь принятого решения как части нового прецедента.

К *преимуществам* рассуждений на основе прецедентов можно отнести [7]:

- самостоятельность выработки решений в критической ситуации без участия эксперта на основе накопленного опыта;
- сокращение времени поиска решения путем использования уже имеющегося решения для аналогичной задачи;
- накопление ошибочного опыта и исключение подобных действий в будущем: за счет использования ключевых знаний и особенностей (из *базы данных и знаний* рассматриваемой предметной области [11]) можно избежать углубленного изучения всех имеющихся предметных знаний;
- возможность использования эвристик, способствующих росту эффективности поиска прецедентов (так решения, не уникальные для конкретной ситуации, могут быть использованы в других случаях);
- прецеденты представляются в различном виде: от записей в базах данных до предикатов и фреймов.

К *недостаткам* рассуждений на основе прецедентов можно отнести:

– снижение эффективности поиска при избыточном объеме базы прецедентов;
– сложность процесса определения критериев для индексации и сравнения прецедентов.

В большинстве источников под *прецедентом* понимают случай, который имел место ранее и служит примером или оправданием для подобных случаев в дальнейшем [7, 10, 21]. Поэтому представляется возможным использовать накопленный опыт экспертов при описании небезопасных состояний информационной системы.

Применительно к решаемой задаче *прецедент* — это небезопасное состояние подобной РИС в прошлом, которое могло способствовать преодолению рубежей защиты нарушителями.

Под решением задачи подразумевается определение совокупности таких действий, которые бы позволили снизить *риск* преодоления подсистемы защиты до приемлемого уровня. Указанные действия включают в себя шаги по настройке ПИБ, а также реализацию дополнительных рубежей защиты, если таковые не были реализованы ранее.

В качестве результата применения решения подразумевается снижение значения остаточного *риска* преодоления подсистемы защиты до допустимого уровня, а также возвращение значений параметров системы в поле допустимых (безопасных) значений.

Так как описание состояния информационной системы проводится по совокупности ее параметров, то предлагается прецеденты в базе прецедентов формировать по следующей структуре (*рис.* 2):

– описание задачи (метаданные 1—4, 7, 8);
– решение этой задачи (5, 6, 10);
– результат (обоснованность) применения решения (9, 11).

Следовательно, формальное представление прецедента возможно в следующем виде:

$$P_j = \{x_1, x_2, \dots, x_i, \dots, x_n, r, d, c\},$$

где P_j — прецедент из базы прецедентов; x_i, $i \in \overline{[1,n]}$ — значение i-го параметра информационной системы, описывающего ее состояние на момент сохранения прецедента; r — уровень риска преодоления подсистемы защиты нарушителем для указанных в прецеденте значений параметров РИС; d — управляющее воздействие по настройке ПИБ; c — затраты на реализацию управляющего воздействия.

Всё множество известных, а также новых прецедентов в базе прецедентов распределено по принадлежности между соответствующими классами угроз.

Формально можно определить библиотеку прецедентов (БП) в следующем виде:

$$BP = \langle K_1, K_2, \dots, K_m \rangle,$$

где $\{K_k\}$, $k \in \overline{[1,m]}$ — множества классов угроз.

При этом:

$$K_k = \{\langle P_1, P_2, \dots, P_j, \dots, P_n \rangle, do\},$$

где K_k — наименование класса k-й угрозы; P_j — подмножество прецедентов; do — совокупность настроек ПИБ.

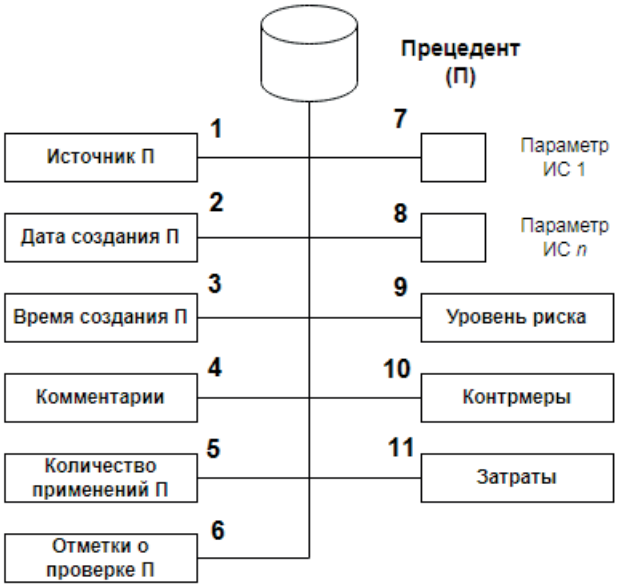


Рис. 2. Структура метаданных прецедента — события атаки на информационную систему

Тогда формальное описание оценки информационных рисков с использованием рассуждений на основе прецедентов можно представить следующим образом [7, 17]:

$$PS = \langle BP, A(p), I^p \rangle,$$

где BP — библиотека (база) прецедентов; $A(p)$ — алгоритм определения сходства прецедентов p; I^p — интерпретатор прецедентов.

Интерпретатор I^p, используя алгоритм $A(p)$, обрабатывает информацию, хранящуюся в базе прецедентов BP, и представляет последовательности процессов:

$$I^p = \langle I^{p1}, I^{p2}, I^{p3}, I^{p4} \rangle,$$

где индексы $p1, \dots, p4$ соответствуют последовательности алгоритмов обнаружения, адаптации, пересмотра и сохранения.

Известны следующие *методы поиска сходства* (подобия прецедентов) [7, 8]: метод ближайшего соседа, метод извлечения прецедентов на основе деревьев решений, метод извлечения прецедентов на основе знаний, метод извлечения прецедентов с учетом их применимости и др. [7, 19].

Проведенный анализ показал, что наиболее целесообразно для решения поставленной задачи использовать метод *k*-взвешенных ближайших соседей, который относится к метрическим методам *классификации* [14]. *Достоинством* метода является наличие более эффективных результатов поиска необходимого решения по сравнению с другими.

Формализация задачи классификации прецедентов

Математическую постановку задачи классификации в общем случае можно представить следующим образом.

Пусть X — множество описаний объектов, *Y* — конечное множество номеров классов. Существует неизвестная целевая зависимость — отображение

$$y^*: X \to Y, \quad (1)$$

значения которой известны только на объектах конечной обучающей выборки $X_m = \{(x_1, y_1), \ldots, (x_m, y_m)\}$.

Требуется построить алгоритм $a: X \to Y$, способный классифицировать, т. е. отнести произвольный объект $x \in X$ к классу $y \in Y$.

Для применения метода ближайшего соседа данная задача сводится к следующему виду (метод модифицирован применительно к решаемой задаче):

– пусть на множестве объектов X задана функция расстояния (метрика)

$$\rho: X \times X \to [0, \infty);$$

– существует целевая зависимость (1), значения которой известны только на объектах обучающей выборки $X^l = (x_1, y_1)_{i=1}^l, y_i = y^*(x_i)$.

Чтобы сгладить влияние выбросов, применяют алгоритм k-взвешенных ближайших соседей, тогда объект u относится к тому классу, элементы которого оказываются больше влияния среди k ближайших соседей $x_u^{(i)}, i = 1, \ldots, k$.

Тогда постановка задачи выглядит следующим образом:

$$w(i,u) = [i \le k];\ a(u; X^l, k) = \quad (2)$$
$$= arg \max_{y \in Y} \sum_{i=1}^k \left[y_u^{(i)} = y\right] w_i,$$

где u — исследуемый объект; $w(i,u)$ — весовая функция; $a(u; X^l, k)$ — алгоритм, строящий локальную аппроксимацию выборки X^l; $y_u^{(i)} = y^*$ — искомое решение.

Процесс поиска прецедентов с использованием модифицированного метода k-взвешенных ближайших соседей заключается в вычислении степени удаленности между значениями параметров, описывающих текущую ситуацию, и извлеченным прецедентом (или в определении степени их близости) [19]. В данной процедуре используется покоординатное сопоставление, так что каждый параметр, описывающий прецедент, рассматривается как одна из координат вектора x. Модификация метода состоит в учете (при поиске прецедентов) предпочтений L_s лица, принимающего решение (ЛПР).

В результате для поиска прецедента определяется расстояние ΔS между текущей ситуацией и прецедентом из базы прецедентов:

$$\Delta S = \left(\sum_{i=1}^n \left(w_i \times SIM\left(x_i^l; x_i^k\right) \times L_i\right)\right) / \sum_{i=1}^n w_i, \quad (3)$$

где w_i — весовое значение (значимость) *i*-го параметра; $SIM\left(x_i^l; x_i^k\right)$ — функция сходства; $x_i^l; x_i^k$ — значения *i*-го параметра в текущем *l* и прошлом *k* прецедентах соответственно; L_i — предпочтение ЛПР по *i*-му показателю прецедента.

Степень сходства прецедентов $x_i^l; x_i^k$ по общему числу параметров N вычисляется по метрике Евклида [19]:

$$SIM\left(x_i^l; x_i^k\right) = \sqrt{\sum_{i=1}^N \left(x_i^l - x_i^k\right)^2}.$$

Данный метод позволяет обеспечивать реализацию эффективного поиска с различной размерностью исходных данных. В случае отсутствия явных значений параметров x_i, описывающих прецедент, или отсутствия недостающих параметров в выбранном прецеденте используются оценки экспертов (после соответствующей обработки). Наиболее прагматичным экспертным методом в данном случае является метод конкордации, так как он позволяет учесть компетентность, ангажированность, взаимозависимость и другие характеристики экспертов, определяющих качество экспертизы. При этом выполнение любого эксперимента предполагает известными измеренные значения выходных параметров системы и перечень факторов, оказывающих влияние на величину выходного параметра.

Направлением развития методов классификации прецедентов является *сочетание* метрических методов с методами экспертного оценивания, что вполне допустимо при задействовании ряда метрик, отличных от евклидового расстояния. В частности, применение к оценке рисков информационной безопасности и настройки ПИБ *риск-ориентированного подхода* на основе ансамблевой нейросети позволяет повысить точность систем поддержки принятия решений по сравнению с ординарной нейросетью за счет использования для решения одной и той же задачи нескольких нейросетей с различными значениями погрешностей отклонений от истинного результата [17].

Заключение

Таким образом, в рамках предложенного концептуально-методического подхода к построению гибридных процедур формирования баз прецедентов разработана формально-логическая модель настройки подсистемы информационной безопасности на основе рассуждений по прецедентам с использованием модифицированного (применительно к решаемой задаче) метода *k*-ближайших соседей. Обоснована рациональная структура базы данных прецедентов и разработан эффективный алгоритм поиска прецедентов. Реализацию эффективного поиска с различной размерностью исходных данных позволил обеспечить модифицированный метод на основе применения процедур классификации на этапе идентификации прецедентов.

Одним из направлений дальнейших исследований предполагается разработка онтологических структур библиотек прецедентов на основе агентных управляющих систем, что позволит, по мнению авторов, существенно расширить возможности методов классификации прецедентов, обеспечивая кроссплатформенность построения баз прецедентов для междисциплинарных предметных областей.

Рецензент: ***Бетанов Владимир Вадимович,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, академик РАРАН, начальник центра АО «Российские космические системы», г. Москва, Российская Федерация.*
E-mail: vlavab@mail.ru

Литература

1. Емельянов В.А., Пастухова С.Е., Соболев А.С., Кучеренко В.А. Алгоритмы кибербезопасности правдоподобно дескрипционной логики в динамических системах // Изв. Тульского гос. ун-та. Технические науки. 2023. № 4. С. 15—22.
2. Бурый А.С. Структуризация систем мониторинга информационных ресурсов // Правовая информатика. 2023. № 1. С. 52—61. DOI: 10.21681/1994-1404-2023-1-52-61 .
3. Бурый А.С., Ловцов Д.А. Информационные структуры умного города на основе киберфизических систем // Правовая информатика. 2022. № 4. С. 15—26. DOI: 10.21681/1994-1404-2022-4-15-26 .
4. Бурый А.С., Ловцов Д.А. Информационные технологии цифровой трансформации умных городов // Правовая информатика. 2022. № 2. С. 4—13. DOI: 10.21681/1994-1404-2022-2-04-13 .
5. Бурый А.С., Усцелемов В.Н. Онтологический подход к формированию когнитивных моделей оценки кибербезопасности // Информационно-экономические аспекты стандартизации и технического регулирования. 2020. № 3 (55). С. 77—84.
6. Бурый А.С., Усцелемов В.Н. Информационная безопасность автоматизированных систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2023. № 2 (72). С. 31—37.
7. Варшавский П.Р., Ар Кар Мьо, Шункевич Д.В. Применение методов классификации и кластеризации для повышения эффективности работы прецедентных систем // Программные продукты и системы. 2017. № 4. С. 625—631.
8. Дойникова Е.В., Чечулин А.А., Котенко И.В. Оценка защищенности компьютерных сетей на основе метрик CVSS // Информационно-управляющие системы. 2017. № 6 (91). С. 76—87. DOI: 10.15217/issn1684-8853.2017.6.76 .
9. Жидко Е.А., Разиньков С.Н. Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта // Системы управления, связи и безопасности. 2018. № 1. С. 122—135.
10. Крылов А.В. Проблема извлечения знаний с использованием рассуждений на основе прецедентов // Изв. вузов. Приборостроение. 2018. Т. 61. № 11. С. 956—962.
11. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
12. Ловцов Д.А. Проблемы правового регулирования электронного документооборота // Информационное право. 2005. № 2. С. 28—31.
13. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 273 с. ISBN 978-5-93916-896-0.
14. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54 .
15. Марков А.С. Правоприменение открытых данных с учетом требований по информационной безопасности // Мониторинг правоприменения. 2017. № 3 (24). С. 86—96. DOI: 10.21681/2412-8163-2017-3-86-96 .
16. Мещеряков Р.В., Исхаков С.Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. 2022. № 5 (51). С. 82—99. DOI: 10.21681/2311-3456-2022-5-82-99 .
17. Усцелемов В.Н. Совершенствование подсистемы информационной безопасности на основе интеллектуальных технологий // Прикладная информатика. 2016. Т. 11. № 3 (63). С. 31—38.
18. Фомичева С.Г. Влияние ранжирования индикаторов атак на качество моделей машинного обучения в агентных системах непрерывной аутентификации // T-Comm: Телекоммуникации и транспорт. 2023. Т. 17. № 8. С. 45—55. DOI: 10.36724/2072-8735-2023-17-8-45-55 .
19. Шелухин О.И., Ерохин С.Д., Полковников М.В. Технологии машинного обучения и сетевой безопасности. М. : Горячая линия-Телеком, 2021. 360 с. ISBN 978-5-9912-0913-7.
20. Юдин В.Н., Карпов Л.Е. Модель поведения объектов, подверженных спонтанному изменению в прецедентном подходе к управлению // Труды ИСП РАН. 2016. Т. 28. Вып. 4. С. 183—192. DOI: 10.15514/ISPRAS-2016-28 (4)-11 .
21. Jung J. W., Lee S. W. Security requirement recommendation method using case-based reasoning to prevent advanced persistent threats. Applied Sciences. 2023. Vol. 13. No. 3. P. 1505.
22. Kim D., Jeong D., Seo Y. Intelligent Design for Simulation Models of Weapon Systems Using a Mathematical Structure and Case-Based Reasoning. Applied Sciences. 2020. No. 10 (21). P. 7642. DOI: 10.3390/app10217642 .
23. San Zaw K., Vasupongayya S. A case-based reasoning approach for automatic adaptation of classifiers in mobile phishing detection. Journal of Computer Networks and Communications. 2019. Vol. 2019. Art. ID 7198435. DOI: 10.1155/2019/7198435 .

DEVELOPING PRECEDENT-BASED DECISION SUPPORT SYSTEMS IN DISTRIBUTED INFORMATION STRUCTURES

Aleksei Buryi, *Dr.Sc. (Technology), expert at the Russian Academy of Sciences, Department Director at the Russian Standardisation Institute, Moscow, Russian Federation.*
E-mail: a.s.burij@gostinfo.ru

Viacheslav Ustselemov, *Researcher, external Ph.D. student at the Russian Standardisation Institute, Moscow, Russian Federation.*
E-mail: ustselemov@mail.ru

Keywords: *distributed information system, precedent, information security, risk, decision support, case-based reasoning system, classifier, method, model, algorithm, similarity.*

Abstract

Purpose of the work: developing adaptive mechanisms for the information security subsystem in organisational decision support systems using the precedent-based method for building conclusions as well as evaluating the dynamics of information conflict interaction with the ability to developing control actions for (re)adjusting the mechanisms of the information exchange subsystem.

Methods used: a complex use of system and comparative analysis, methods ensuring information security, the precedent-based method for building reasoning, and logical concept justification of structures for building distributed information systems.

Study findings: justification is given for a conceptual and methodological approach to building hybrid procedures for forming precedent databases based on the CBR (Case-Based Reasoning) method, a combination of metric methods for classifying information security incidents and algorithms for expert evaluation of classification objects in tasks of monitoring information resources of integrated information structures of a given subject area. A formal logic model is developed for adjusting the information security subsystem based on precedent-based reasoning using a modified k-nearest neighbours method. A rational structure for the precedent database and an efficient algorithm for precedent search are justified.

References

1. Emel'ianov V.A., Pastukhova S.E., Sobolev A.S., Kucherenko V.A. Algoritmy kiberbezopasnosti pravdopodobno deskriptsionnoi logiki v dinamicheskikh sistemakh. Izv. Tul'skogo gos. un-ta. Tekhnicheskie nauki, 2023, No. 4, pp. 15–22.
2. Buryi A.S. Strukturizatsiia sistem monitoringa informatsionnykh resursov. Pravovaia informatika, 2023, No. 1, pp. 52–61. DOI: 10.21681/1994-1404-2023-1-52-61 .
3. Buryi A.S., Lovtsov D.A. Informatsionnye struktury umnogo goroda na osnove kiberfizicheskikh sistem. Pravovaia informatika, 2022, No. 4, pp. 15–26. DOI: 10.21681/1994-1404-2022-4-15-26 .
4. Buryi A.S., Lovtsov D.A. Informatsionnye tekhnologii tsifrovoi transformatsii umnykh gorodov. Pravovaia informatika, 2022, No. 2, pp. 4–13. DOI: 10.21681/1994-1404-2022-2-04-13 .
5. Buryi A.S., Ustselemov V.N. Ontologicheskii podkhod k formirovaniiu kognitivnykh modelei otsenki kiberbezopasnosti. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia, 2020, No. 3 (55), pp. 77–84.
6. Buryi A.S., Ustselemov V.N. Informatsionnaia bezopasnost' avtomatizirovannykh sistem. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia, 2023, No. 2 (72), pp. 31–37.
7. Varshavskii P.R., Ar Kar M'o, Shunkevich D.V. Primenenie metodov klassifikatsii i klasterizatsii dlia povysheniia effektivnosti raboty pretsedentnykh sistem. Programmnye produkty i sistemy, 2017, No. 4, pp. 625–631.
8. Doinikova E.V., Chechulin A.A., Kotenko I.V. Otsenka zashchishchennosti komp'iuternykh setei na osnove metrik CVSS. Informatsionno-upravliaiushchie sistemy, 2017, No. 6 (91), pp. 76–87. DOI: 10.15217/issn1684-8853.2017.6.76 .
9. Zhidko E.A., Razin'kov S.N. Model' podsistemy bezopasnosti i zashchity informatsii sistemy sviazi i upravleniia kriticheski vazhnogo ob"ekta. Sistemy upravleniia, sviazi i bezopasnosti, 2018, No. 1, pp. 122–135.
10. Krylov A.V. Problema izvlecheniia znanii s ispol'zovaniem rassuzhdenii na osnove pretsedentov. Izv. vuzov. Priborostroenie, 2018, t. 61, No. 11, pp. 956–962.
11. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.

12. Lovtsov D.A. Problemy pravovogo regulirovaniia elektronnogo dokumentooborota. Informatsionnoe pravo, 2005, No. 2, pp. 28–31.
13. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 273 pp. ISBN 978-5-93916-896-0.
14. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Pravovaia informatika, 2017, No. 2, pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .
15. Markov A.S. Pravoprimenenie otkrytykh dannykh s uchetom trebovanii po informatsionnoi bezopasnosti. Monitoring pravoprimeneniia, 2017, No. 3 (24), pp. 86–96. DOI: 10.21681/2412-8163-2017-3-86-96 .
16. Meshcheriakov R.V., Iskhakov S.Iu. Issledovanie indikatorov komprometatsii dlia sredstv zashchity informatsionnykh i kiberfizicheskikh sistem. Voprosy kiberbezopasnosti, 2022, No. 5 (51), pp. 82–99. DOI: 10.21681/2311-3456-2022-5-82-99 .
17. Ustselemov V.N. Sovershenstvovanie podsistemy informatsionnoi bezopasnosti na osnove intellektual'nykh tekhnologii. Prikladnaia informatika, 2016, t. 11, No. 3 (63), pp. 31–38.
18. Fomicheva S.G. Vliianie ranzhirovaniia indikatorov atak na kachestvo modelei mashinnogo obucheniia v agentnykh sistemakh nepreryvnoi autentifikatsii. T-Comm: Telekommunikatsii i transport, 2023, t. 17, No. 8, pp. 45–55. DOI: 10.36724/2072-8735-2023-17-8-45-55 .
19. Shelukhin O.I., Erokhin S.D., Polkovnikov M.V. Tekhnologii mashinnogo obucheniia i setevoi bezopasnosti. M. : Goriachaia liniia-Telekom, 2021. 360 pp. ISBN 978-5-9912-0913-7.
20. Iudin V.N., Karpov L.E. Model' povedeniia ob"ektov, podverzhennykh spontannomu izmeneniiu v pretsedentnom podkhode k upravleniiu. Trudy ISP RAN, 2016, t. 28, vyp. 4, pp. 183–192. DOI: 10.15514/ISPRAS-2016-28 (4)-11 .
21. Jung J. W., Lee S. W. Security requirement recommendation method using case-based reasoning to prevent advanced persistent threats. Applied Sciences. 2023. Vol. 13. No. 3. P. 1505.
22. Kim D., Jeong D., Seo Y. Intelligent Design for Simulation Models of Weapon Systems Using a Mathematical Structure and Case-Based Reasoning. Applied Sciences. 2020. No. 10 (21). P. 7642. DOI: 10.3390/app10217642 .
23. San Zaw K., Vasupongayya S. A case-based reasoning approach for automatic adaptation of classifiers in mobile phishing detection. Journal of Computer Networks and Communications. 2019. Vol. 2019. Art. ID 7198435. DOI: 10.1155/2019/7198435 .

ИЗМЕНЕНИЯ В СИСТЕМЕ ОФИЦИАЛЬНОГО ОПУБЛИКОВАНИЯ ПРАВОВЫХ АКТОВ В ЭЛЕКТРОННОМ ВИДЕ: МУНИЦИПАЛЬНЫЙ УРОВЕНЬ

Макаренко Т.Н.[1]

Ключевые слова: *информация, достоверность, полнота, систематизация, официальное опубликование, обнародование, электронное опубликование, нормативный правовой акт, муниципальный правовой акт, печатные издания, сетевые издания, официальный сайт.*

Аннотация

Цель работы: совершенствование научно-методической базы концепции юридической техники законодательства.

Методы исследования: системный и экспертный анализ, сравнительно-правовой и формально-юридический методы.

Результаты: обоснован вывод, что на федеральном уровне отсутствует единообразное правовое регулирование вопросов доступа к правовой информации, возникающих при официальном опубликовании и обнародовании муниципальных нормативных правовых актов органами местного самоуправления; проанализированы ключевые позиции Конституционного Суда РФ по данным вопросам; раскрыто соотношение понятий официального опубликования и обнародования; обоснованы предложения, направленные на реализацию конституционного требования об обязательности опубликования нормативных правовых актов в связи с выраженной позицией Конституционного Суда РФ.

EDN: YWNCVO

Введение

Местное самоуправление составляет одну из основ конституционного строя России, форму осуществления власти народом, через которую реализуется большинство прав и свобод граждан. По вопросам местного значения органами местного самоуправления (ОМС) принимаются муниципальные акты и доводятся до всеобщего сведения.

Открытость и *доступность* информации [5] о деятельности государственных органов и ОМС является одним из базовых конституционных принципов государства[2]. Обеспечение прав граждан на доступ к информации также является одним из основных принципов Стратегии[3] развития информационного общества в Российской Федерации на 2017—2030 гг.

Обеспечение открытости деятельности органов публичной власти предполагает распространение ими полной и *достоверной*[4] информации обо всех результатах и этапах реализации властных полномочий, гарантии получения в доступной форме информации о муниципальных нормативных правовых актах (МНПА) и их проектах всеми заинтересованными субъектами права.

Доступность информации о деятельности органов местного самоуправления обеспечивается размещением ОМС в сети Интернет информации о своей деятельности, распространением правовой информации, включая официальное опубликование изданных МНПА и их проектов в соответствии с положениями феде-

[2] Конституция РФ с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 07.03.2024).

[3] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

[4] Ст. 3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. № 165. Действующее законодательство, регулирующее правовые отношения, возникающие в сфере информации, информационных технологий и защиты информации, основывается на принципе достоверности информации и своевременности ее предоставления.

[1] ***Макаренко Татьяна Николаевна,*** *начальник отдела нормативных правовых актов Научного центра правовой информации при Министерстве юстиции Российской Федерации, соискатель ученой степени Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: tatyana.makarenko@scli.ru

ральных законов от 9 февраля 2009 г. № 8-ФЗ[5] и от 6 октября 2003 г. № 131-ФЗ[6].

Данными федеральными актами регулируется правовой режим открытости правовой информации и обязанность публичных органов власти размещать ее в сети Интернет, а также определение действия муниципальных правовых актов во времени, порядок и условия вступления их в силу, обязанность ОМС распространять не только нормативные, но и иные муниципальные акты. Представляется, например [3], что массив постановлений и распоряжений главы муниципального образования, главы местной администрации в части сведений о предоставленных земельных участках, проведенных контрольных мероприятиях и выданных предписаниях (но со скрытыми персональными данными) и тому подобной информации может быть оценен как *открытые данные* [2].

С официальным опубликованием неразрывно связано вступление в силу муниципальных правовых актов. Вопросы вступления в силу, опубликования и обнародования муниципальных правовых актов непосредственно регулирует ст. 47 Федерального закона № 131-ФЗ.

Необходимо заметить, что до внесения изменений Федеральным законом № 517-ФЗ[7] в ст. 47 Федерального закона № 131-ФЗ предусматривалось несколько способов доведения содержания муниципальных актов до всеобщего сведения, включая *официальное опубликование (обнародование)* в установленном порядке МНПА, затрагивающих права, свободы и обязанности человека и гражданина, как условие вступления указанных актов в силу.

Официальным опубликованием МНПА или соглашения, заключенного между ОМС, считалась первая публикация его полного текста *исключительно* в периодическом печатном издании, распространяемом в соответствующем муниципальном образовании, а опубликование (размещение) текста муниципального правового акта в официальном сетевом издании рассматривалось как дополнительное к печатному изданию; использовать сетевое издание в качестве альтернативы не предусматривалось. Способы доведения содержания муниципальных актов до всеобщего сведения определялись уставом муниципального образования [10].

Законодательного разграничения и уточнения понятий и терминов «*опубликование*» и «*обнародование*» применительно к муниципальным правовым актам Федеральный закон № 131-ФЗ не содержал, конституционная норма об *официальном опубликовании* всех актов, затрагивающих права и свободы граждан, толковалась расширительно, включая в нее и возможность *обнародования* муниципальных правовых актов.

Эти положения Федерального закона № 131-ФЗ не способствовали единообразному применению законодательства в части вопросов официального опубликования и обнародования муниципальных правовых актов, тем более что определение нормативности в отношении муниципальных актов также не урегулировано законодательно. На федеральном уровне также не приводится легальной дефиниции терминов «*нормативный правовой акт*», «*муниципальный нормативный правовой акт*», отсутствуют единые законодательные требования и методические подходы к выявлению критериев нормативности правового акта, что отражается в материалах судебной практики [1].

Основание внесения изменений. Позиция Конституционного Суда

Конституционный Суд РФ рассмотрел дело и принял Постановление № 23-П[8] о проверке конституционности законоположений п. 6 ч. 1 ст. 44, чч. 1 и 3 ст. 47 Федерального закона № 131-ФЗ в той мере, в какой они в системе действующего правового регулирования служат нормативным основанием для решения вопроса об официальном опубликовании (обнародовании) МНПА. Основанием для детального рассмотрения приведенных положений Федерального закона № 131-ФЗ Конституционным Судом явилось утверждение, что указанные законоположения позволяют ОМС не публиковать официально для всеобщего сведения МНПА, затрагивающие права, свободы и обязанности человека и гражданина, и поэтому не соответствуют ч. 3 ст. 15 Конституции РФ.

К основным выводам Конституционного Суда, представленным в Постановлении № 23-П, относятся следующие.

1. При рассмотрении дела Конституционный Суд РФ исходил из ранее им установленных положений, что предусмотренное конституционное требование официального опубликования нормативных правовых актов (НПА) компетентным органом публичной власти обусловлено общепризнанным *принципом правовой определенности*, лежащим в основе отношений государства и индивида, и означает всеобщее оповещение о том, что данный акт принят и подлежит действию в изложенном аутентичном содержании. Только тогда на лиц, подпадающих под его действие, распространяется общеправовая презумпция, в силу которой незнание

[5] Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Российская газета. 2009. № 25.

[6] Федеральный закон от 6 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» // Собрание законодательства РФ. 2003. № 40. Ст. 3822.

[7] Федеральный закон от 2 ноября 2023 г. № 517-ФЗ «О внесении изменений в Федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru, 02.11.2023.

[8] Постановление Конституционного Суда РФ от 27 мая 2021 г. № 23-П по делу о проверке конституционности п. 6 ч. 1 ст. 44, чч. 1 и 3 ст. 47 Федерального закона от 6 октября 2003 года № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» в связи с жалобой гражданина Ю.Г. Ефремова // Собрание законодательства РФ. 2021. № 23. Ст. 4175.

закона не освобождает от ответственности за его нарушение.

Возникающая же неопределенность относительно того, действует или не действует НПА, препятствует единообразию в его соблюдении, исполнении и применении и, как следствие, порождает противоречивую правоприменительную практику, ведет к нарушению принципов равенства и верховенства права, гарантий защиты конституционных прав и свобод, создает возможность злоупотреблений. При этом конституционное требование официального опубликования распространяется на все НПА, затрагивающие права, свободы и обязанности человека и гражданина, составляющие правовую систему России, представляет собой императивное и универсальное конституционное требование и адресовано всем органам, входящим в единую систему публичной власти, включая ОМС.

Конституция РФ не конкретизирует порядок и способы официального опубликования НПА, в частности, виды изданий (источников), в которых оно должно осуществляться, и тем самым возлагает обязанность урегулировать эти вопросы на органы публичной власти, и прежде всего — на законодателя.

2. Конституционный Суд РФ указал, что в связи с объективным изменением структуры *информационного пространства* [7, 8] и включению в перечень официальных изданий, в которых осуществляется официальная публикация НПА, сетевого издания «Официальный интернет-портал правовой информации»[9] (ОИППИ), позволяющего осуществлять функцию всеобщего оповещения о принятии НПА и ознакомления с ними с использованием новых информационных технологий — также возможно вступление в силу МНПА путем их опубликования (размещения) *исключительно* в официальном сетевом издании.

В качестве официального сетевого издания может использоваться официальный сайт муниципального образования, с учетом того, что действующее регулирование[10] связывает получение статуса сетевого издания с регистрацией сайта в качестве средства массовой информации (СМИ).

При этом возможность использовать для официального опубликования МНПА только официальное сетевое издание должна быть обусловлена исполнением в муниципальном образовании требований Федерального закона № 8-ФЗ о создании пунктов подключения к сети Интернет в целях обеспечения права неограниченного круга лиц на *доступ к информации* о деятельности государственных органов и ОМС в местах, доступных для пользователей информацией (в помещениях государственных органов, ОМС, государственных и муниципальных библиотек, в других доступных для посещения местах).

3. Постановление № 23-П имеет также важное значение, поскольку в нем перед законодателем и судебной властью ставится «на вид» различие категорий *официального опубликования* и *обнародования* МНПА[11].

Конституционный Суд разъяснил, что используемое понятие «*обнародование*» в Федеральном законе № 131-ФЗ приводится как дополнение или пояснение к понятию «*официальное опубликование*». По своему содержанию эти категории не тождественны, и Конституция РФ, разграничивая категории «*опубликование*» и «*обнародование*», не допускает того, чтобы закон или иной НПА, затрагивающий права, свободы и обязанности человека и гражданина, вступил бы в силу после обнародования отличным от официального опубликования способом.

Таким образом, данные законоположения, рассматриваемые в системе правового регулирования, не предполагают вступления МНПА в силу без их официального опубликования, а также наделяют муниципальные образования полномочием самостоятельно предусмотреть в интересах граждан, наряду с порядком официального опубликования МНПА, *дополнительные* способы их обнародования.

4. Конституционный Суд также принял к вниманию, что:

- тиражи официальных изданий, в которых публикуются МНПА, и их распространение должны обеспечивать реальную возможность ознакомления с такими актами, не создавая неоправданных усилий по их поиску;
- для муниципальных образований, с учетом в том числе их многообразия, в силу объективных, в частности, финансовых причин могут быть затруднительны: учреждение печатного СМИ, обеспечение достаточного тиража печатного издания, где публикуются МНПА, а также их распространение на территории муниципального образования.

Конституционный Суд также указал, что в силу *принципа единства публичной власти* нахождение вопросов защиты прав и свобод человека и гражданина, обеспечения законности и правопорядка в совместном ведении Российской Федерации и субъектов РФ предполагает необходимость для федеральных органов государственной власти и органов государственной власти субъектов РФ оказывать содействие муниципальным образованиям, ресурсы которых ограничены, в обеспечении официального опубликования МНПА.

5. Конституционный Суд РФ дал рекомендацию законодателю в кратчайший срок урегулировать вопросы официального опубликования МНПА в условиях цифровизации.

На урегулирование вопросов использования для официального опубликования МНПА, затрагивающих

[9] URL: http://www.pravo.gov.ru

[10] Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» // Российская газета. 1992. № 32.

[11] Обнародование и опубликование: возможно обнародование без опубликования, однако опубликование всегда приводит к обнародованию. Обнародование НПА (цель достигается его официальным опубликованием) — средство, способ.

права, свободы и обязанности человека и гражданина, возможностей современного информационного пространства был дан временно́й период — ОМС не позднее чем через два года с момента вступления в силу Постановления № 23-П обязаны внести изменения в уставы муниципальных образований и обеспечить официальное опубликование МНПА в соответствии с выраженной позицией Конституционного Суда.

На указанный переходный период МНПА, затрагивающие права, свободы и обязанности человека и гражданина, вступившие в силу на момент вступления в силу Постановления № 23-П и в течение двух лет после его вступления в силу (но не позднее внесения изменений в устав муниципального образования в соответствии с Постановлением № 23-П) и обнародованные без их официального опубликования в порядке, установленном уставом муниципального образования, признаются действующими с момента их первоначального обнародования.

При этом такие акты могут быть признаны судами недействующими по мотиву нарушения порядка их опубликования, если будет установлено, что лицам, чьи права и свободы затрагивают данные акты, не была обеспечена возможность ознакомиться с содержанием таких актов. Кроме того, могут быть признаны судами недействующими МНПА, которые вступят в силу в течение двух лет после вступления Постановления № 23-П в силу, если на момент вступления Постановления № 23-П в силу в муниципальном образовании определен источник официального опубликования муниципальных правовых актов, однако эти акты в нем не были опубликованы.

Ознакомившись с рассмотренными выводами Конституционного Суда РФ в Постановлении № 23-П, можно предположить, что *электронная форма* опубликования правовых актов будет признана основной в целом в системе официального опубликования, а бумажная — вспомогательной и для МНПА, поскольку опубликование в официальном сетевом издании может являться достаточным и эффективным средством обнародования нормативных актов при соблюдении условий доступности, а также упрощения признания статуса официального сетевого издания для целей официального опубликования МНПА за официальными сайтами органов публичной власти.

Переход на официальное опубликование МНПА в электронной форме будет способствовать процессам *систематизации* [7] массива законодательства, поскольку при организации работы по систематизации законодательства принципиально важными являются *полнота* информационного массива (учет и фиксация всего объема информации, отсутствие пробелов) и *достоверность* информации (использование официальных источников опубликования), а также будет способствовать решению институциональной *проблемы* отсутствия единого учетного официального верифицированного государственного ресурса всех правовых актов.

Создание Единого цифрового правового регистра (ЕЦПР) [11] правовых актов РФ как источника актуальной правовой информации в электронном виде, в котором должна храниться машиночитаемая достоверная правовая информация, пригодная для автоматизированной (цифровой) обработки при применении технологий искусственного интеллекта, позволит решить задачу глобальной работы, проводимой органами публичной власти по систематизации массива законодательства России.

Зарубежный опыт электронного опубликования правовых актов

Зарубежный опыт показывает динамику распространения практики официального электронного опубликования органами власти НПА в целях обеспечения доступа к правовой информации и доведения содержания правовых актов до своих граждан [10].

Основополагающими *принципами* при этом также являются бесплатность электронного издания, его доступность, обеспечение доступа к сети Интернет через публичные библиотеки, а также гарантированность идентичности печатной и электронной информации, т. е. ее достоверности.

Некоторые страны Европы (Бельгия, Франция, Эстония) отказались от издания бумажной версии официального журнала, оставив только его электронную форму. В других странах (Дания, Великобритания, Германия, Италия) издание электронной версии официальных печатных изданий используется как дополнительный способ опубликования.

Для многих стран (Канада, США, Великобритания, Португалия и др.) характерна множественность источников официального опубликования правовых актов, в зависимости от традиций и административно-территориального устройства страны.

Федеративные государства соблюдают двухзвенную систему нормативных актов, при которой каждая провинция, штат или земля имеет свой официальный орган печати. Кроме того, законы и подзаконные (административные) акты имеют раздельные издания.

Примеры стран, где публикация правовых актов осуществляется в электронной форме.

Бельгия[12]**.** Бельгийский официальный журнал[13] является официальным журналом в Королевстве Бель-

[12] По форме государственно-территориального устройства Бельгия — федеративное государство, состоящее из сообществ и регионов. Сообщества строятся по культурно-лингвистическому принципу, а регионы — по языково-территориальному. В сообществах и регионах созданы соответствующие представительные и исполнительные органы. Одновременно регионы Бельгии в административно-территориальном отношении делятся на 10 провинций. Территориальная организация местного самоуправления в Бельгии имеет 2-х уровневую структуру. Низовым уровнем местного самоуправления являются коммуны, входящие в провинции — второй уровень местного самоуправления.

[13] URL: https://justitie.belgium.be/nl/overheidsdienst_justitie/organisatie/belgisch_staatsblad

гия, в котором публикуются законы, королевские указы, официальные уведомления. Публикация находится в ведении Федеральной государственной службы юстиции.

Бумажная версия была заменена в 2003 г. электронной версией, доступной для общественности в Интернете. Электронная версия существует только для распространения через сеть Интернет. Публикации в электронном виде являются точными копиями аутентичных копий актов на бумажном носителе.

Франция. Принятые правовые акты Франции публиковались в Официальном печатном издании *Journal Officiel* с 1869 г. Начиная с 2016 г. официальный журнал не публикуется в печати и доступен только на официальном веб-сайте французского правительства *Légifrance*[14] по распространению законодательных и иных нормативных документов, а также решений верховных судов и апелляций по французскому законодательству. Сайт предоставляет публичный доступ к действующим текстам правовых актов и к прецедентному праву.

Португалия. С июля 2006 г. нормативные акты вступают в силу после их официального опубликования в электронном журнале *Diario da Republica Electrónico* на интернет-сайте[15]. Несколько заверенных печатных копий журнала передаются для сдачи на хранение в Национальный архив, Президенту, в Парламент, а также в высокие суды.

В автономных областях — на Азорских островах и Мадейре — есть свое печатное издание *Gazette*: *Jornal Oficial da Região Autónoma dos Açores* (*JORAA*) и Журнал Автономного региона Мадейра (*JORAM*). Они также доступны в Интернете, но в случае с JORAM[16] только печатная версия считается подлинной (официальной).

В рамках Евросоюза. Официальный журнал Европейского Союза (ЕС) OJEU[17] является официальной газетой для ЕС. С июля 2013 г. имеют юридическую силу только опубликованные в электронной форме выпуски Официального журнала. Бумажная версия больше не имеет юридической силы, за исключением случаев, когда журнал не может быть опубликован в Интернете из-за непредвиденного сбоя в работе ИТ-систем.

Кроме обеспечения официального опубликования, государства обеспечивают онлайн-доступ к принимаемым органами государственной власти правовым актам не только на собственных сайтах, но и на специальных общегосударственных сайтах.

Заметим, что официальный характер электронной публикации правовых актов признается странами повсеместно, а некоторые страны пошли по пути полного отказа от печатной версии официальных изданий и осуществляют опубликование только в электронной версии официальных изданий.

[14] URL: https://www.legifrance.gouv.fr

[15] URL: https://dre.pt/dre/home

[16] URL: https://joram.madeira.gov.pt/joram

[17] URL: https://op.europa.eu/en/law

Позиция законодателя

Через непродолжительное время после вступления в силу Постановления № 23-П на федеральном портале проектов НПА[18] был размещен законопроект, направленный на урегулирование порядка опубликования муниципальных правовых актов. В первоначальном варианте законодатель прямо последовал рекомендациям Конституционного Суда РФ и в размещенном законопроекте ограничился следующими изменениями в ст. 47 Федерального закона № 131-ФЗ:

- официальным опубликованием муниципального правового акта или соглашения, заключенного между ОМС, считается первая публикация его полного текста в периодическом печатном издании, распространяемом в соответствующем муниципальном образовании, либо первое опубликование (размещение) его полного текста в сетевом издании;
- опубликование (размещение) муниципальных правовых актов исключительно в сетевом издании должно осуществляться с учетом обеспечения права неограниченного круга лиц на доступ к информации о деятельности государственных органов и ОМС в местах, доступных для пользователей информацией;
- предусматривается возможность закрепления в уставе муниципального образования дополнительных способов обнародования муниципальных правовых актов (например, одним из способов обнародования может являться размещение муниципальных правовых актов на официальном сайте муниципального образования, на официальных сайтах иных органов публичной власти, если эти сайты не являются сетевыми изданиями).

По истечении двух с половиной лет нормативная конкретизация выводов Конституционного Суда РФ в контексте официального опубликования МНПА законодателем видоизменилась и приобрела некоторый выбор вариантов для правоприменителя.

Федеральным законом № 517-ФЗ ст. 47 Федерального закона № 131-ФЗ изложена в новой редакции. Законодатель оперирует следующими терминами для муниципальных правовых актов: *«официальное обнародование», «обнародование», «официальное опубликование», «опубликование», «публикация», «размещение»,* а также разделяет источники и виды изданий в зависимости от выбранного способа доведения муниципального акта до всеобщего сведения.

Новая редакция ст. 47 Федерального закона № 131-ФЗ определяет, что МНПА, затрагивающие права, свободы и обязанности человека и гражданина, устанавливающие правовой статус организаций, учредителем которых выступает муниципальное образование, а также соглашения, заключаемые между ОМС, вступают в силу после их *официального обнародования*.

[18] URL: https://regulation.gov.ru/

Под *обнародованием* муниципального правового акта, в том числе соглашения, заключенного между ОМС, понимается:

- официальное опубликование муниципального правового акта;
- размещение муниципального правового акта в местах, доступных для неограниченного круга лиц (в помещениях государственных органов, ОМС, государственных и муниципальных библиотек, других доступных для посещения местах);
- размещение на официальном сайте муниципального образования в информационно-телекоммуникационной сети Интернет;
- иной предусмотренный уставом муниципального образования способ обеспечения возможности ознакомления граждан с муниципальным правовым актом, в том числе соглашением, заключенным между ОМС.

Официальным опубликованием муниципального правового акта, в том числе соглашения, заключенного между ОМС, считается *первая публикация* его полного текста в периодическом печатном издании, распространяемом в соответствующем муниципальном образовании, или *первое размещение* его полного текста в сетевом издании.

Если официальное опубликование муниципального правового акта, в том числе соглашения, осуществляется в сетевом издании, в муниципальном образовании (МО) в соответствии с Федеральным законом № 8-ФЗ обеспечивается создание одного или нескольких пунктов подключения к сети Интернет в местах, доступных для их использования неограниченным кругом лиц без использования ими дополнительных технических средств.

Наименование периодического печатного и (или) сетевого издания (СМИ), в которых осуществляется официальное опубликование муниципальных правовых актов, в том числе соглашений, указываются в уставе МО.

Перечень периодических печатных изданий, сетевых изданий (СМИ), в которых осуществляется обнародование (за исключением официального опубликования) муниципальных правовых актов, в том числе соглашений, доводится до всеобщего сведения путем опубликования правового акта главы МО. Представляется, что для корректного применения ст. 47 Федерального закона № 131-ФЗ в данном виде потребуется разъяснение уполномоченных органов федеральной власти.

Вместе с тем следует рассматривать данные законоположения в системе правового регулирования с учетом позиции Конституционного Суда РФ, высказанной в Постановлении № 23-П, что МНПА не предполагают вступления в силу без их официального опубликования, а ОМС предусматривают, наряду с порядком официального опубликования МНПА, *дополнительные* способы их *обнародования* в интересах граждан.

Поэтому закрепление в уставе МО формулировки *«официальное опубликование (обнародование)»* для вступления в силу МНПА и соглашений будет противоречить ч. 2 ст. 47 Федерального закона № 131-ФЗ, а наличие в уставе положений о вступлении в силу муниципальных актов и соглашений указанными в п. 2—4 ст. 47 Федерального закона № 131-ФЗ дополнительными способами их обнародования или отсутствие в уставе МО норм об официальном опубликовании повлечет отказ в регистрации такого устава в соответствии с законодательством[19] о государственной регистрации уставов муниципальных образований.

Следовательно, в уставе МО могут быть указаны в качества источника официального опубликования:

- периодическое печатное издание, распространяемое в соответствующем МО, и сетевое издание (СМИ);
- только периодическое печатное издание, распространяемое в соответствующем МО;
- только сетевое издание (СМИ).

В уставе МО могут быть определены как одно, так и несколько периодических печатных изданий, распространяемых в соответствующем МО, и (или) сетевых изданий (СМИ), в которых осуществляется официальное опубликование муниципальных актов и соглашений.

Уточним: если в МО в соответствии с Федеральным законом № 8-ФЗ не обеспечивается создание одного или нескольких пунктов подключения к сети Интернет в местах, доступных для их использования неограниченным кругом лиц без использования ими дополнительных технических средств, официальное опубликование муниципального правового акта и соглашения не может осуществляться в сетевом издании (СМИ).

Следует заметить, что для приведения в соответствие терминологии по тексту Федерального закона № 131-ФЗ законодатель в нарушение юридической техники пояснений к применению или изменений не предусмотрел, и термины ст. 47 в новой редакции не пересмотрены в иных действующих положениях Федерального закона № 131-ФЗ, где продолжает использоваться рассмотренное Конституционным Судом РФ понятие *«официальное опубликование (обнародование)»*, в частности, в ст. 22 — «Местный референдум»; ст. 23 — «Муниципальные выборы»; ст. 24 — «Голосование по отзыву депутата, члена выборного органа местного самоуправления, выборного должностного лица местного самоуправления, голосование по вопросам изменения границ муниципального образования, преобразования муниципального образования»; ст. 25 — «Сход граждан, осуществляющий полномочия представительного органа муниципального образования»; ст. 26.1 — «Инициативные проекты»; ст. 28 — «Публичные слушания, общественные обсуждения»; ст. 29 — «Собрание граждан»; ст. 30 — «Конференция граждан

[19] Федеральный закон от 21 июля 2005 г. N 97-ФЗ «О государственной регистрации уставов муниципальных образований» // Собрание законодательства РФ. 2005. № 30 (часть I). Ст. 3108.

(собрание делегатов)»; ст. 44 — «Устав муниципального образования»; ст. 69.4 — «Соглашения об осуществлении международных и внешнеэкономических связей органов местного самоуправления»; ст. 74.1 — «Удаление главы муниципального образования в отставку».

Заключение

Введение новых понятий в нарушение юридической техники и не закрепленных официально легальных дефиниций терминов не способствует единому подходу и устранению пробелов в правовом регулировании и, соответственно, не способствует задачам систематизации законодательства РФ, развитию *института электронного опубликования* правовых актов и созданию условий для размещения машиночитаемых текстов правовых актов [4], а равно и укреплению конституционных гарантий реализации прав и законных интересов субъектов права в сфере представления правовой информации.

В условиях построения правового государства должны строго соблюдаться требования к технике подготовки как проектов федеральных законов, так и других НПА, к качеству их оформления. Точность и ясность формулировок правовых актов, их последовательность и логическая связь, использование единых приемов изложения юридических предписаний определяют *эффективность* их действий [7], не допускают *неопределенности* применения.

Информационное право как одна из наиболее динамично развивающихся отраслей российского права и его институты, включая институт электронного опубликования, сейчас переживают революционные изменения. Наиболее характерными для отрасли информационного права, учитывающими ее специфику, наряду с общеотраслевыми и межотраслевыми принципами права, являются такие принципы-постулаты, как: свободное обращение информации, открытость или публичность информации, баланс информационных интересов личности, общества и государства при приоритетности интересов личности [6].

При сохраняющихся темпах *цифровизации* [9] государство и общество находятся в состоянии вынужденной перестройки инфраструктур. Разумеется, старые методы и подходы уже не так эффективны, новые еще не полностью сформированы, однако это тот момент, когда регуляторы и нормотворцы должны активно «прислушиваться» к информационному праву. Совместными усилиями можно сформировать новые подходы, базирующиеся на основополагающих принципах для развития отрасли в целом и, в частности, института электронного опубликования правовых актов, предназначенного для реализации определенной информационной функции государства.

Рецензент: ***Ловцов Дмитрий Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*
E-mail: dal-1206@mail.ru

Литература

1. Атагимова Э.И., Борисова И.А., Макаренко Т.Н., Сарапкина Е.Н. Проблемы определения нормативности муниципальных правовых актов, подлежащих включению в федеральный регистр муниципальных нормативных правовых актов (с учетом судебной практики) // Мониторинг правоприменения. 2020. № 1. С. 8—15. DOI: 10.21681/2226-0692-2020-1-08-15 .
2. Борисов Р.С., Ефименко А.А. Анализ федерального законодательства об ограничении публикации открытых данных // Государственная власть и местное самоуправление. 2022. № 2. С. 42—47.
3. Дамм И А., Роньжина О.В., Акунченко Е.А., Волкова М.А., Корхов А.В. Открытость и доступность информации о правотворческой деятельности органов местного самоуправления в России // Российский юридический журнал. 2018. № 6. С. 85—97.
4. Лахтин С.Е., Цимбал В.А., Амелёнков А.А. Классификация форматов данных электронных документов для сериализации правовых актов в машиночитаемой форме // Правовая информатика. 2023. № 3. С. 75—88. EDN: RDXGWO.
5. Ловцов Д.А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере II. Качество информации // Информационное право. 2015. № 2. С. 52—60.
6. Ловцов Д.А. Эффективность правовых эргасистем в инфосфере // Правовая информатика. 2020. № 1. С. 4—14. DOI: 10.21681/1994-1404-2020-1-04-14 .
7. Ловцов Д.А. Информационная теория эргасистем. Тезаурус : монография. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
8. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.

9. Ловцов Д.А. Цифровая трансформация инфосферы правовых эргасистем и оценка защищенности привилегированной информации // Образовательное и правовое пространство цифрового мира: современность, перспективы и безопасность : монография. Краснодар : СКФ РГУП, 2023. С. 9—17. ISBN 978-5-907663-78-7.
10. Макаренко Т.Н., Сарапкина Е.Н., Благовещенский Н.Ю. Актуальные вопросы официального опубликования (обнародования) муниципальных нормативных правовых актов // Тр. Междунар. науч.-практ. конф. «Право и информация: вопросы теории и практики» (26 ноября 2021 г.) / Президентская библиотека им. Б.Н. Ельцина. СПб. : ПБ им. Б.Н. Ельцина, 2022. С. 109—120.
11. Макаренко Т.Н., Сарапкина Е.Н. Оптимизация официального опубликования нормативных правовых актов в электронном виде // Правовая информатика. 2023. № 3. С. 97—110. EDN: QUSYEZ.

CHANGES IN THE SYSTEM FOR OFFICIAL PUBLISHING OF LEGAL REGULATIONS IN ELECTRONIC FORM: THE MUNICIPAL LEVEL

Tat'iana Makarenko, *Head of the Legal Regulations Department of the Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation, external Ph.D. student at the Russian State University of Justice, Moscow, Russian Federation, Moscow, Russian Federation.*
E-mail: tatyana.makarenko@scli.ru

Keywords: *information, reliability, completeness, systematisation, official publication, promulgation, electronic publication, legal regulation, municipal regulation, printed publications, online publications, official website.*

Abstract

Purpose of the work: improving the scholarly and methodological basis for the concept of legal technique of the legislation.

Methods used in the study: system and expert analysis, the comparative legal and formal legal methods.

Study findings: a conclusion is justified that at the federal level there is a lack of single legal regulation of questions of access to legal information which arise in official publishing and promulgation of municipal regulations by local self-government bodies. The key positions of the Constitutional Court of the Russian Federation concerning the said questions are analysed. The relation between the concepts of official publishing and promulgation is expounded. A justification is given for proposals aimed at the implementation of the constitutional requirement on mandatory publishing of legal regulations due to the position expressed by the Constitutional Court of the Russian Federation.

References

1. Atagimova E.I., Borisova I.A., Makarenko T.N., Sarapkina E.N. Problemy opredeleniia normativnosti munitsipal'nykh pravovykh aktov, podlezhashchikh vkliucheniiu v federal'nyi registr munitsipal'nykh normativnykh pravovykh aktov (s uchetom sudebnoi praktiki). Monitoring pravoprimeneniia, 2020, No. 1, pp. 8–15. DOI: 10.21681/2226-0692-2020-1-08-15 .
2. Borisov R.S., Efimenko A.A. Analiz federal'nogo zakonodatel'stva ob ogranichenii publikatsii otkrytykh dannykh. Gosudarstvennaia vlast' i mestnoe samoupravlenie, 2022, No. 2, pp. 42–47.
3. Damm I A., Ron'zhina O.V., Akunchenko E.A., Volkova M.A., Korkhov A.V. Otkrytost' i dostupnost' informatsii o pravotvorcheskoi deiatel'nosti organov mestnogo samoupravleniia v Rossii. Rossiiskii iuridicheskii zhurnal, 2018, No. 6, pp. 85–97.
4. Lakhtin S.E., Tsimbal V.A., Amelenkov A.A. Klassifikatsiia formatov dannykh elektronnykh dokumentov dlia serializatsii pravovykh aktov v mashinochitaemoi forme. Pravovaia informatika, 2023, No. 3, pp. 75–88. EDN: RDXGWO.
5. Lovtsov D.A. Lingvisticheskoe obespechenie pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere II. Kachestvo informatsii. Informatsionnoe pravo, 2015, No. 2, pp. 52–60.
6. Lovtsov D.A. Effektivnost' pravovykh ergasistem v infosfere. Pravovaia informatika, 2020, No. 1, pp. 4–14. DOI: 10.21681/1994-1404-2020-1-04-14 .
7. Lovtsov D.A. Informatsionnaia teoriia ergasistem. Tezaurus : monografiia. M. : Nauka, 2005. 248 pp. ISBN 5-02-033779-Kh.

8. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
9. Lovtsov D.A. Tsifrovaia transformatsiia infosfery pravovykh ergasistem i otsenka zashchishchennosti privilegirovannoi informatsii. Obrazovatel'noe i pravovoe prostranstvo tsifrovogo mira: sovremennost', perspektivy i bezopasnost' : monografiia. Krasnodar : SKF RGUP, 2023, pp. 9–17. ISBN 978-5-907663-78-7.
10. Makarenko T.N., Sarapkina E.N., Blagoveshchenskii N.Iu. Aktual'nye voprosy ofitsial'nogo opublikovaniia (obnarodovaniia) munitsipal'nykh normativnykh pravovykh aktov. Tr. Mezhdunar. nauch.-prakt. konf. "Pravo i informatsiia: voprosy teorii i praktiki" (26 noiabria 2021 g.). Prezidentskaia biblioteka im. B.N. El'tsina. SPb. : PB im. B.N. El'tsina, 2022, pp. 109–120.
11. Makarenko T.N., Sarapkina E.N. Optimizatsiia ofitsial'nogo opublikovaniia normativnykh pravovykh aktov v elektronnom vide. Pravovaia informatika, 2023, No. 3, pp. 97–110. EDN: QUSYEZ.

ОНЛАЙН-МЕХАНИЗМ НАПРАВЛЕНИЯ ИНОСТРАННЫХ СУДЕБНЫХ ПОРУЧЕНИЙ

Карандашева Н.Н.[1]

Ключевые слова: *международный гражданский процесс, электронные судебные поручения, киберпространство, Интернет, онлайн-механизм, информационно-коммуникационные технологии, принцип процессуальной экономии, информационное (цифровое) пространство, эффективность.*

Аннотация

Цель работы: обосновать онлайн-механизм направления иностранных судебных поручений.

Методы исследования: системный анализ, специальные юридические методы: сравнительного правоведения (компаративистский), формально-юридического толкования и правового моделирования.

Результаты исследования: ввиду устаревания механизма, предусмотренного в Гаагских конвенциях (Гаагская конвенция по вопросам гражданского процесса 1954 г., Гаагская конвенция о вручении за границей судебных и внесудебных документов по гражданским и торговым делам 1965 г. и Гаагская конвенция о получении за границей доказательств по гражданским и торговым делам 1970 г.) обосновано предложение внедрить электронное судебное поручение (ЭСП, англ.: Electronic Letter Rogatory, e-LR) и трансграничную платформу ЭСП, что обеспечит высокую эффективность (оперативность, согласованность и экономичность) обмена информацией между судебными органами разных юрисдикций; обоснован вывод, что применение электронного судебного поручения и трансграничной платформы имеет перспективу развития в качестве одного из альтернативных порядков при направлении иностранных судебных поручений.

EDN: LVEPID

Введение

Сформулированные в конце XX в. порядки направления иностранных судебных поручений, определённые в Гаагских конвенциях 1954, 1965, 1970 гг.[2], потеряли свою актуальность в условиях цифровой эпохи. Современные темпы передачи информации существенно отличаются от методов и технологий, заложенных в основу процедур передачи судебных документов, закреплённых в действующих международных договорах. Развитие *информационно-коммуникационных технологий* (ИКТ) делает существующие процедуры устаревшими и неспособными удовлетворить потребности современного общества. Несоответствие временны́х параметров передачи информации при существующих порядках затрудняет эффективное функционирование систем передачи данных. В этой связи представляется необходимым пересмотреть и адаптировать международные соглашения, которые не учитывают современные способы передачи и обработки информации. Наиболее перспективным вариантом решения данной задачи видится в разработке нового механизма, который позволит расширить действие Гаагских конвенций и урегулирует вопросы применения современных цифровых технологий.

Упрощение и рационализация порядка направления иностранных судебных поручений с помощью ИКТ представляют собой одну из основных задач текущей повестки как в России[3], так и в зарубежных странах [15, 16].

Порядок направления иностранных судебных поручений

На сегодняшний день существует несколько порядков направления иностранных судебных поручений, которые различаются в зависимости от международ-

[2] Конвенция по вопросам гражданского процесса (Заключена в г. Гааге 01.03.1954) (с изм. от 25.10.1980) // СПС «КонсультантПлюс»; Конвенция о вручении за границей судебных и внесудебных документов по гражданским или торговым делам (заключена в г. Гааге 15.11.1965) // СПС «КонсультантПлюс»; Конвенция о получении за границей доказательств по гражданским или торговым делам (Заключена в г. Гааге 18.03.1970) // СПС «КонсультантПлюс».

[3] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» // СПС «КонсультантПлюс».

[1] ***Карандашева Наталия Николаевна,*** *аспирант кафедры международного частного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация.*

E-mail: nnkarandasheva@gmail.com

ных договоров, соглашений между государствами и национального законодательства. Основными из них являются:

1. *Дипломатический порядок* (для стран — участниц Гаагской конвенции по вопросам гражданского процесса 1954 г., не присоединившихся к Гаагской конвенции о вручении за границей судебных и внесудебных документов по гражданским и торговым делам 1965 г. и Гаагской конвенции о получении за границей доказательств по гражданским и торговым делам 1970 г., а также во многих двусторонних договорах (например, с Францией[4], США[5] и др.). Процедура предусматривает передачу поручений в рамках выполнения определённых действий на межгосударственном уровне путём целенаправленно созданных дипломатических каналов [14]. С исторической точки зрения дипломатический путь передачи поручений был первым, который предусматривал предоставление юридической помощи на межгосударственном уровне. Такой подход до 1960-х гг. был единственным в СССР, применяемым в сфере регулирования споров на международном уровне. К 20-м гг. XX в. СССР заключил более 40 соглашений с разными странами, применяя дипломатический порядок передачи поручений [2].

В отечественной и зарубежной литературе отмечается, что процедура получения и пересылки документации является затруднительной и бюрократизированной, а время передачи поручений по дипломатическим каналам составляет от 6 месяцев до года [4, 10, 17].

2. *Через центральные органы государств*. Государства имеют специальные центральные органы, ответственные за принятие и направление иностранных судебных поручений. Подобные поручения могут включать в себя уведомление сторон, перевод документов и организацию исполнения (Гаагская конвенция 1965 г., Гаагская конвенция 1970 г.).

3. *Непосредственный порядок передачи судебных поручений*. В некоторых случаях судебные поручения направляются непосредственно через компетентные органы другого государства, как это предусмотрено международными соглашениями или двусторонними договорами, включая: Соглашение СНГ о порядке разрешения споров, связанных с осуществлением хозяйственной деятельности от 20 марта 1992 г.; Регламент № 2020/1783 Европейского парламента и Совета Европейского союза (ЕС) «О сотрудничестве между судами государств-членов ЕС при получении доказательств по гражданским или коммерческим делам (сбор доказательств)»[6].

В отечественной доктрине неоднократно поднимался вопрос поиска наиболее актуального механизма осуществления передачи поручений судебного характера на межгосударственном уровне. Исследователи отмечают, что прямая передача поручений (направление поручений судом запрашивающего государства в суд запрашиваемого государства) адресату является наиболее эффективной [3, 9, 10]. В практической сфере деятельности такой подход принято называть «*прямым методом передачи поручений*», позволяющим значительно снизить число инстанций, которые обычно принимают участие в процессе передачи рассматриваемых поручений с момента их отправки и до получения ответа по ним.

К примеру, на региональном уровне в Европейском союзе внедрена система e-CODEX (e-Justice Communication via Online Data Exchange). Система e-CODEX представляет собой крупномасштабный пилотный проект в области электронного правосудия, позволяющий осуществлять трансграничные судебные процедуры между европейскими государствами-членами и обеспечивающий гражданам, предприятиям и специалистам в области права более лёгкий доступ к транснациональному правосудию. Его основная задача — ускорение и электронизация правосудия путём укрепления международного сотрудничества и создания инструментов для реализации электронных процедур. Одной из ключевых задач платформы e-CODEX является транспортировка данных и документов. В транснациональных условиях это означает перенос информации из одной страны в другую, включая также связь между порталом e-Justice и национальными системами [15].

Регламент № 2020/1783 касается сотрудничества между судами государств-членов Европейского Союза при получении доказательств в гражданских или коммерческих делах, регулирует процедуры сбора доказательств между судами в государствах — членах ЕС. В п. 7 Регламента № 2020/1783 указано, что для обеспечения ускоренной передачи запросов и сообщений между государствами — членами ЕС в целях получения доказательств необходимо использовать все соответствующие современные коммуникационные технологии. В этой связи, как правило, все сообщения и обмен документами должны осуществляться через безопасную и надёжную децентрализованную систему ИКТ, состоящую из национальных *информационных систем*, являющихся, например, взаимосвязанными и

[4] Соглашение между СССР и Францией о передаче судебных и нотариальных документов и выполнении судебных поручений по гражданским и торговым делам (Заключено в г. Париже 11 августа 1936 г.) // СПС «КонсультантПлюс».

[5] Обмен Нотами о порядке исполнения судебных поручений между СССР и Соединенными Штатами Америки (вместе с «Извлечениями из главы 28 кодекса Соединенных Штатов») (Состоялся в г. Москве 22 ноября 1935 г.) // СПС «КонсультантПлюс».

[6] Регламент № 2020/1783 Европейского парламента и Совета Европейского Союза «О сотрудничестве между судами государств-членов ЕС при получении доказательств по гражданским или коммерческим делам (сбор доказательств)» [рус., англ.] (Вместе с «Формами Запроса, Уведомления, Ответа, Информации», «Регламентом, признанным утратившим силу, со списком последующих изменений», «Корреляционной таблицей») (Принят в г. Брюсселе 25 ноября 2020 г.) // СПС «КонсультантПлюс».

технически совместимыми, и без ущерба для будущего технологического прогресса, основанного на развитии проекта e-CODEX. Информационная система должна позволять производить обмен данными исключительно между двумя государствами-членами ЕС без участия каких-либо учреждений в данном обмене.

Регламент № 2020/1783 был принят с общей целью уменьшения бремени расходов и неоправданных задержек для граждан и предприятий, участвующих в трансграничных процессах, за счет более быстрых механизмов передачи, менее зависимых от бумажных носителей информации.

Следует заметить, что государствам — членам ЕС предлагается перейти к использованию *видеоконференций*, если это разрешено законом, что существенно сокращает необходимость обременительных и дорогостоящих поездок и может облегчить разбирательство. Хотя на национальном уровне уже используется множество решений для проведения видеоконференций [11], в Плане действий «Электронное правосудие» на 2019—2023 гг. использование видеоконференций в трансграничных разбирательствах было названо приоритетным направлением [15]. Акцент на *цифровизацию* является частью широкой тенденции ЕС в области регулирования, направленной на модернизацию процедур судебного сотрудничества без изменения самих процедур, используя потенциал существующих средств ИКТ для передачи документов. Цифровизация всё больше становится важным активом для повышения эффективности и устойчивости каналов связи, присущих сотрудничеству между национальными органами в трансграничных делах ЕС, и, в конечном итоге, для обеспечения доступа к правосудию.

Прямое взаимодействие между должностными лицами судов, участников судебного процесса было предусмотрено ещё в Гаагской конвенции 1965 г. Помимо основных каналов передачи через центральные органы государства, в ст. 10 Гаагской конвенции 1965 г. предусматривается передача документов через ряд альтернативных каналов, включая:

а) почтовые каналы;

б) обращения судебных и должностных лиц к компетентным лицам государства вручения;

в) обращения участников судебного процесса к компетентным лицам государства вручения.

Вместе с тем при присоединении России к Гаагской конвенции 1965 г. была сделана оговорка, которая запрещает использование альтернативных каналов извещения на территории страны при принятии данной международной конвенции.

По срокам взаимодействия порядок передачи судебных поручений через центральные органы государств хотя и проще дипломатического порядка, однако остаётся излишне формализованным. Центральные органы предусматривают включение огромного количества инстанций, которые отвечают за разные этапы межгосударственного взаимодействия. В отечественной доктрине существует справедливое мнение о необходимости сокращения инстанций путём передачи поручения непосредственно из рассматривающих дело органов судебной власти в компетентные органы, при этом не привлекая Министерство юстиции РФ [1].

В п. 27 Постановления Пленума Верховного Суда РФ от 27.06.2017 № 23 «О рассмотрении арбитражными судами дел по экономическим спорам, возникающим из отношений, осложнённых иностранным элементом»[7], предусмотрено пять порядков направлений поручений, в зависимости от требований международных договоров и (или) арбитражного процессуального законодательства, а именно:

- путём непосредственного вручения участнику судебного разбирательства судебных документов, направленных по почте;
- непосредственно в компетентный суд государства исполнения поручения;
- непосредственно в центральные органы государства исполнения поручения;
- через территориальные органы Минюста РФ и МИД РФ — компетентному органу государства исполнения поручения;
- через центральные, территориальные и иные органы учреждений юстиции — компетентному суду (органу) государства исполнения поручения.

Однако перечисленные порядки в Постановлении Пленума № 23 не увеличивают число способов направления поручений в иностранные суды, а детализируют существующие три основных порядка.

Прослеживается тенденция рационализации существующих механизмов в правоприменительной практике РФ. Принцип *процессуальной экономии*, приведенный в п. 28 Постановления Пленума № 23, указывает на выбор того механизма взаимодействия компетентных органов государств, который обеспечивает наиболее быстрое и менее формализованное взаимодействие[8]. Представляется, что процессуальная экономия, отнесенная в судебной практике к числу принципов национального гражданского процесса, получит свое специальное содержание при рассмотрении трансграничных споров. Кроме того, выделяемый принцип нарушает традиционное правило соотношения договоров по юридической силе за счет установления более адаптивных процедур в сфере международного гражданского процесса. Дополнительным механизмом, обеспечивающим соблюдение принципа процессуальной экономии, является применение новых ИКТ и цифровых решений в целях более эффективного использования ресурсов и времени в рамках международного судебного сотрудничества.

Несмотря на то, что существующие механизмы учитывают принцип процессуальной экономии, они все же

---

[7] Постановление Пленума Верховного Суда РФ от 27.06.2017 № 23 «О рассмотрении арбитражными судами дел по экономическим спорам, возникающим из отношений, осложненных иностранным элементом» // Бюллетень Верховного Суда РФ. 2017. № 8.

[8] Там же.

ограничены в условиях современного информационного века. Представляется целесообразным разработать упрощённый механизм направления иностранных судебных поручений, соответствующий современным темпам передачи информации.

Перспективы развития онлайн-механизма направления иностранных судебных поручений

С целью оптимизации взаимодействия судебных органов предлагается несколько вариантов решения рассматриваемой задачи:

1) гармонизация законодательства в соответствии с рекомендациями относительно интеграции информационных технологий, предусмотренных в Практическом руководстве[9] по применению Гаагской конвенции 1965 г.;

2) внесение изменений или пересмотр уже вступивших в силу конвенций (более сложный унификационный процесс);

3) унификация в виде принятия нового международного юридического акта.

1. Процесс гармонизации. В отношении гармонизации первый шаг был предпринят ещё в 2003 г. Уполномоченная комиссия по практическому применению Гаагских конвенций (далее — Комиссия) обращала внимание на то, что применение современных технологий должно способствовать сотрудничеству между государствами, и нормы Гаагской конвенции 1965 г. не служат препятствием на пути их применения. Комиссия также рекомендовала использование более простых контактов между странами, ориентируясь на применение современных ИКТ, в частности, на использование *электронной почты* как оперативного, качественного и быстрого способа передачи документов[10].

В то же время в 2003 г. многие технологические средства, упоминаемые в данном акте и ставшие доступными в настоящее время, ещё не могли быть спрогнозированы. Статистические данные по всему миру, согласно данным Международного союза электросвязи (МСЭ), начинают отсчёт лишь с 2005 г., когда число пользователей составляло 16% от всего населения. За последние 10 лет количество интернет-пользователей выросло более чем в два раза. По прогнозам МСЭ, в 2023 г. Интернетом будут пользоваться около 5,4 млрд человек, или 67% населения Земли[11].

Использование цифровых технологий в процедуре направления и исполнения иностранных поручений может быть возможным даже в случае отсутствия прямого упоминания о них в Гаагских конвенциях. Такой вывод можно сделать, исходя из Практического руководства по применению Гаагской конвенции 1965 г. о вручении за границей судебных и внесудебных документов. Однако это зависит от ряда факторов, таких как национальное законодательство стран-участниц конвенций, практики и интерпретации судов, а также согласия сторон, участвующих в конкретном правовом процессе. Суды и учреждения могут решить, что использование цифровых технологий улучшает *эффективность* (*оперативность, согласованность, экономичность*) и *прозрачность* [7, 8] процедур направления и исполнения иностранных поручений.

Примером может служить использование *электронного апостиля* в рамках Гаагской конвенции 1961 г.[12], отменяющей требование легализации иностранных официальных документов. Программа электронного апостиля (*e-APP*) была инициирована в 2006 г. с целью стимулирования и поддержки интеграции технологических инноваций. Основной целью программы является улучшение доступности и удобства использования Гаагской конвенции 1961 г. путём применения общедоступных информационных средств. Международный форум по электронному апостилю закрепил понятие e-APP — Electronic Apostille Program, который включает в себя два ключевых элемента: электронные *апостили* и электронные *реестры*. Электронный апостиль может быть применён как к электронным документам, так и к бумажным документам, которые были сканированы и переведены в электронный формат. Трансграничный электронный реестр, в свою очередь, представляет собой публично доступный реестр, ведение которого осуществляется в электронной форме и даёт возможность каждому заинтересованному лицу осуществлять онлайн-проверку апостиля, подтверждая его подлинность и действительность.

2. Внесение изменений или пересмотр действующих конвенций. Это представляется наиболее трудоёмким, ввиду масштабности задачи. Кроме того, правовая процедура внесения поправок или пересмотра данных конвенций и многосторонних соглашений неодинакова. Поэтому принятие поправок и заключение соглашения об изменении многосторонних договоров между определёнными участниками приводит к неравнозначному содержанию текста конвенции в отношении всех государств-участников. Учитывая данные обстоятельства, считается наиболее целесообразным устранить разночтения толкования международных документов о возможности применения цифровых технологий при взаимодействии в вопросах оказании правовой помощи путём создания *единого международного документа*.

---

[9] Практическое руководство по применению Гаагской конвенции от 15 ноября 1965 г. о вручении за границей судебных и внесудебных документов по гражданским или торговым делам / Отв. ред. А.Н. Жильцов. М. : Волтерс Клувер, 2007. 320 с. ISBN 5-466-00240-2 — ISBN 978-5-466-00240-9.

[10] Заключения и рекомендации, принятые 4 ноября 2003 г. специальной комиссией по практическому применению Гаагских конвенций об апостиле, получении доказательств, вручении документов // СПС «КонсультантПлюс».

[11] См.: Committed to connecting the world. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[12] Конвенция, отменяющая требование легализации иностранных официальных документов (Заключена в г. Гааге 5 октября 1961 г.) // СПС «КонсультантПлюс».

3. Процесс унификации. Третьим вариантом совершенствования порядка направления иностранных судебных поручений с использованием ИКТ является разработка нового юридически обязательного международного документа. Цель этого акта заключается в установлении правового статуса использования современных цифровых технологий при направлении и исполнении судебных поручений между юрисдикциями и внедрении специализированной цифровой платформы, способной обеспечить надёжный обмен данными между судебными органами разных стран. Сфера действия данного юридического документа будет создана по принципу «зонтичного» регулирования, который предусматривает возможность расширения сферы применения существующих конвенций за счет принятия новой Конвенции, что позволит расширить её влияние и обеспечить применение в рамках существующих Гаагских конвенций. Это означает, что Конвенция будет предусматривать гибкость для расширения сферы действия, включая как Гаагские конвенции, так и двусторонние договоры.

Предложение нацелено на адаптацию правовых систем к реалиям цифровой эры и способствует развитию правовых норм и процедур. Разработка и принятие такого юридического акта могут быть осуществлены для реализации как на региональном, так и на универсальном уровне. Наиболее перспективным вариантом видится создание Конвенции в рамках БРИКС или ЕАЭС, что будет способствовать углублению международного судебного сотрудничества и унификации процедур по направлению и исполнению судебных поручений в указанном регионе.

Подобно тому, как программа электронного апостиля (e-APP) обеспечивает усовершенствованный механизм апостиля, можно представить аналогичную типовую модель электронного судебного поручения e-LR — Electronic Letters Rogatory. Программа e-LR может быть создана с целью облегчения и повышения эффективности процесса направления и исполнения судебных поручений между различными юрисдикциями. Путём применения цифровых технологий, аналогичных тем, что используются в e-APP, можно разработать электронные судебные поручения и соответствующие трансграничные электронные реестры. Программа e-LR представит поручение, выданное в электронной форме, подписанное *электронной цифровой подписью* [5, 7], обеспечивая его *аутентичность* и *целостность*. Это поручение может применяться как к передаче судебных документов, так и к указаниям на совершение определённых судебных действий, таких как сбор доказательств, вынесение решений и др.

Трансграничные электронные реестры, в свою очередь, предоставляли бы публично доступную базу данных, где можно проверить статус и подлинность электронных судебных поручений. Подобно электронному апостилю, электронные судебные поручения в e-LR могли бы быть подвергнуты онлайн-проверке (верификации), чтобы гарантировать их *легитимность* и соответствие юридическим требованиям. Такой механизм способствует оперативному, надёжному и прозрачному исполнению судебных поручений в международной практике, а также сокращению временных и ресурсных затрат на передачу и проверку документов между судами разных стран.

Модель e-LR — это цифровая форма судебного поручения, которое создаётся, направляется и хранится в электронной форме, форма, предназначенная для передачи между различными юрисдикциями через сети электронной связи и специализированные информационные платформы.

Алгоритм направления и исполнения иностранных судебных поручений

Представляется, что в настоящее время есть все предпосылки для внедрения *Трансграничной платформы электронных судебных поручений* (ТПЭСП) в качестве нового механизма передачи иностранных судебных поручений между судами, который представляет собой цифровую платформу, созданную для электронного обмена и хранения судебных поручений между судами разных государств. Платформа предоставляет эффективный механизм для передачи судебных поручений между странами с использованием современных цифровых технологий, что позволяет согласовать, упростить и ускорить процедуры судебного сотрудничества в международных гражданских делах.

ТПЭСП представляет собой инновационный подход в вопросе направления иностранных судебных поручений через использование Всемирной сети. Суть данного механизма заключается в том, чтобы разработать *единое цифровое пространство* [5, 6], специально адаптированное для направления и исполнения иностранных судебных поручений. Это позволит судам разных стран взаимодействовать эффективно и безопасно, обеспечивая соблюдение международных стандартов и гарантируя приватность. Идея нацелена на эффективное и безопасное направление и получение иностранных судебных извещений через виртуальную платформу, основанную на передовых технологиях и соблюдающую международные стандарты *конфиденциальности* и *безопасности* [5, 7].

Предлагается следующий рациональный алгоритм направления и исполнения иностранных судебных поручений.

Шаг 1. Регистрация в ТПЭСП: участники системы, такие как суды и стороны, проходят процесс регистрации в системе.

Шаг 2. Регистрация и направление поручений: суд одной страны, отправляющей поручение, регистрирует его в ТПЭСП. ТПЭСП автоматически уведомляет суд второй страны, с подтверждением получения, принимающей поручение, о его поступлении. Возможен **выбор способа извещения:** запросивший суд выбирает предпочтительный способ извещения из доступных ва-

риантов: электронная почта, SMS, системы мгновенных сообщений, платформа для видеоконференций.

Шаг 3. Уведомление и принятие иностранного суда. ТПЭСП генерирует уведомление и отправляет его соответствующему суду принимающей страны. Уведомление содержит информацию о поручении, его сроках и деталях. Суд принимающей страны принимает поручение и подтверждает это в ТПЭСП. В случае необходимости суд может запросить дополнительную информацию или уточнения.

Шаг 4. Исполнение поручения: суд принимающей страны обрабатывает поручение; результаты проведённых процессуальных действий вносятся в реестр. ТПЭСП автоматически уведомляет суд, направивший поручение. В случае невозможности исполнения иностранного судебного поручения в связи с отсутствием запрашиваемого правового механизма в стране, исполняющей судебное поручение, суд может обратиться за разъяснениями в запрашивающий суд. После получения разъяснений суд может применить процессуальные нормы той юрисдикции, в которой происходит основное судебное действие, что обеспечивает единообразие и согласованность процедур.

Шаг 5. Обновление статуса и завершение: суд принимающей страны обновляет статус поручения в ТПЭСП, отмечая его выполнение или любые другие изменения в ходе процесса исполнения. По завершении исполнения судебного поручения в ТПЭСП делается запись об окончании.

Этот алгоритм обеспечивает эффективное (оперативное, согласованное и экономичное) и практически безопасное взаимодействие между судами разных стран, обеспечивая их *информационную совместимость*, сокращая временные задержки и риски потери данных. ТПЭСП служит важным инструментом для современных международных судебных процедур и способствует улучшению глобального правоприменения. Такая виртуальная система иностранного судебного извещения значительно ускорит процесс передачи документов, обеспечивая быстрое и надёжное взаимодействие между судами и сторонами. Она также гарантирует *конфиденциальность* и *безопасность* [5] данных, делая процедуру направления и получения иностранных судебных извещений более эффективной и удобной.

Использование цифровых возможностей в процессе направления иностранных судебных поручений, с одной стороны, не вызывает затруднений, поскольку национальное законодательство как России, так и зарубежных стран позволяет активно использовать ИКТ в судебных процессах. С другой стороны, внедрение интернет-технологий в направление и исполнение иностранных судебных поручений осложняется консервативными взглядами и политическими интересами государств. Рассмотрим некоторые из возможных причин затруднения в вопросе использования Всемирной сети для направления и исполнения иностранных судебных поручений.

Во-первых, отсутствие регламентации. Внутреннее законодательство большинства зарубежных стран не имеет чётких нормативных рамок для использования цифровых технологий в контексте исполнения и направления иностранных судебных поручений (к примеру, возможность применения видеоконференцсвязи между иностранными судами).

Во-вторых, технические и организационные сложности. Эффективное использование сети Интернет требует стабильного и защищённого интернет-соединения, соответствующего оборудования, программного обеспечения и согласованности между разными судами, что может вызвать определённые затруднения в связи с различиями в технической оснащённости и организационных процессах.

В-третьих, безопасность и конфиденциальность данных. Трансграничная передача и хранение персональных данных может стать уязвимой с точки зрения обеспечения конфиденциальности и безопасности данных, особенно при передаче закрытой информации между судами разных стран.

В-четвёртых, необходимость согласия сторон: применение цифровых технологий требует согласия не только со стороны органов публичной власти, но и всех сторон, включая истца, ответчика и других участников судебного процесса.

В-пятых, культурные и юрисдикционные различия: разные страны имеют собственные культурные и юрисдикционные практики, которые могут затруднить применение видеоконференцсвязи в международных судебных процедурах. В некоторых национальных судебных системах отдаётся предпочтение традиционным методам направления и исполнения судебных поручений, что может препятствовать внедрению новых технологий.

Сложности, связанные с вопросами применения сети Интернет государствами в контексте возможности направления и исполнения поручений, возникают в том числе из-за децентрализованной природы управления сетью Интернет. В отечественной доктрине отмечается, что данное управление включает в себя не только государства и межправительственные организации, но и значительное количество негосударственных национальных организаций (Общество Интернета — Internet Society), некоммерческую организацию по управлению доменными именами и IP-адресами (ICANN) и др., а также структуры, не являющиеся юридическими лицами (Рабочая группа по проектированию Интернета — Internet Engineering Task Force, IETF) и др. Вместе с тем, несмотря на децентрализованную структуру сети Интернет, ключевую роль в её управлении продолжают играть США, под чьей юрисдикцией находятся компании, выполняющие функции по управлению Интернетом [13].

Решение *проблемы управления киберпространством* [12, 13] на основе модели многостороннего управления Интернетом способно создать условия для построения безопасного и открытого *информацион-*

ного пространства [7, 8], взаимодействие в котором между государствами строится на равных правах. Такой подход не только обеспечивает *стабильность* и *справедливость* в использовании киберпространства, но и создает основу для эффективного судебного взаимодействия, основанного на международных стандартах и обязательствах.

Заключение

Даже в условиях закрепления принципа процессуальной экономии в практике арбитражных судов РФ и применения наименее формализованного порядка направления и исполнения иностранных судебных поручений отсутствие правоприменительной практики в использовании интернет-технологий свидетельствует о нехватке документов универсального или регионального уровня, позволяющих преодолеть укоренившиеся консервативные взгляды государств в отношении использования интернет-ресурсов для международного взаимодействия судов. Единственным вариантом адаптации правовых систем к вызовам современной цифровой эры является внедрение ТПЭСП в качестве нового онлайн-механизма передачи иностранных судебных поручений между судами и e-LR, обеспечивая высокое быстродействие (оперативность), согласованность и экономичность международного судебного сотрудничества.

Принятие нового юридически обязательного международного документа, разработанного по принципу «зонтичного» регулирования, как на универсальном, так и на региональном уровнях способствует унификации и повышению *эффективности судебной системы* [7, 8], что улучшает деловой климат, придаёт устойчивость в развитии торговых отношений и поддерживает экономический рост.

Рецензент: ***Терентьева Людмила Вячеславовна,*** *доктор юридических наук, доцент, доцент кафедры международного частного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация.*
E-mail: terentevamila@mail.ru

Литература

1. Воронцова И.В. Нормативное регулирование направления и исполнения судебных поручений российскими и иностранными судами // Журнал российского права. 2007. № 6 (126). С. 47—55.
2. Григорьева О.Г. Развитие государственных и международных механизмов правовой помощи по гражданским делам в Советском Союзе // Право и управление. XXI век. 2012. № 1 (22). С. 37—40.
3. Григорьева О.Г. Разработка способов внешних сношений Советского Союза по вопросам оказания международной правовой помощи по гражданским делам // Социодинамика. 2013. № 1. С. 171—204. DOI: 10.7256/2306-0158.2013.1.342 .
4. Елисеев Н. Г. Извещение ответчика, находящегося за границей // Закон. 2016. № 6. С. 121—137.
5. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
6. Ловцов Д.А. Системология информационного права // Правосудие/Justice. 2022. Т. 4. № 1. С. 41—70. DOI: 10.37399/2686-9241.2022.1.41-70 .
7. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
8. Ловцов Д.А., Ниесов В.А. Формирование единого информационного пространства судебной системы России // Российское правосудие. 2008. № 11 (31). С. 78—88.
9. Лукашенкова Т.В. Оказание арбитражными судами международной правовой помощи // Арбитражный и гражданский процесс. 2006. № 12. С. 30—31.
10. Петрова М.М. Тенденции развития правового регулирования в сфере оказания международной правовой помощи по сбору и получению доказательств, находящихся на территории иностранных государств, по гражданским делам // Юриспруденция. 2011. № 3. С. 136—142.
11. Терентьева Л.В. Организационно-правовые особенности использования видеоконференцсвязи в арбитражных судах // Правовая информатика. 2017. № 3. С. 59—65. DOI: 10.21681/1994-1404-2017-3-59-65 .
12. Терентьева Л.В. Понятие киберпространства и очерчивание его территориальных контуров // Правовая информатика. 2018. № 4. С. 66—71. DOI: 10.21681/1994-1404-2018-4-66-71 .
13. Терентьева Л.В. Управление киберпространством по модели мультистейкхолдеризма // Право и экономика. 2019. № 3 (373). С. 11—20.
14. Унификация и гармонизация в международном частном праве. Вопросы теории и практики : монография / Отв. ред. Г.К. Дмитриева, М.В. Мажорина. М. : Норма, ИНФРА-М, 2022. 208 с. ISBN 978-5-91768-753-7.

15. Apostolos A. Digitalization of civil justice in the European Union. Alatoo Academic Studies. 2023. No. 1. Pp. 470–479. DOI: 10.17015/aas.2023. 231.44 . EDN: HWKEVC.
16. Francesconi E., Peruginelli G., Steigenga E., Tiscornia D. Conceptual Modeling of Judicial Procedures in the e-Codex Project. Casanovas P. et al. (Eds.) AI Approaches to the Complexity of Legal Systems: AICOL 2013. Part of the Lecture Notes in Computer Science, V. 8929. Springer Berlin Heidelberg. 2014. Pp. 202–216. DOI: 10.1007/978-3-662-45960-7_15 .
17. Harkness T. P. Discovery in international civil litigation. Washington, DC: Federal Judicial Center, 2015. Pp. 18–20.

AN ONLINE MECHANISM FOR SENDING FOREIGN LETTERS ROGATORY

Nataliia Karandasheva, *Ph.D. student at the Department of International Private Law of the Kutafin Moscow State Law University, Moscow, Russian Federation.*
E-mail: nnkarandasheva@gmail.com

Keywords: *international civil procedure, electronic letters rogatory, cyberspace, Internet, online mechanism, information and communication technologies, principle of procedural economy, information (digital) space, efficiency.*

Abstract

Purpose of work: justifying an online mechanism for sending foreign letters rogatory.

Methods used in the study: system analysis, special legal methods: the comparative legal method, the methods of formal legal interpretation and legal modelling.

Study findings: the mechanism provided for in the Hague Conventions (the 1954 Hague Convention on Civil Procedure, the 1965 Hague Convention on the Service Abroad of Judicial and Extra-Judicial documents in Civil and Commercial Matters and the 1970 Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters) has become outdated, therefore, a proposal is justified to introduce an Electronic Letter Rogatory (e-LR) and a Cross-Border e-LR Platform which would provide a highly efficient (prompt, co-ordinated and economic) exchange of information between judicial bodies in different jurisdictions. A conclusion is justified that using Electronic Letters Rogatory and the Cross-Border e-LR Platform has a prospect of development as an alternative procedure for sending foreign letters rogatory.

References

1. Vorontsova I.V. Normativnoe regulirovanie napravleniia i ispolneniia sudebnykh poruchenii rossiiskimi i inostrannymi sudami. Zhurnal rossiiskogo prava, 2007, No. 6 (126), pp. 47–55.
2. Grigor'eva O.G. Razvitie gosudarstvennykh i mezhdunarodnykh mekhanizmov pravovoi pomoshchi po grazhdanskim delam v Sovetskom Soiuze. Pravo i upravlenie. XXI vek, 2012, No. 1 (22), pp. 37–40.
3. Grigor'eva O.G. Razrabotka sposobov vneshnikh snoshenii Sovetskogo Soiuza po voprosam okazaniia mezhdunarodnoi pravovoi pomoshchi po grazhdanskim delam. Sotsiodinamika, 2013, No. 1, pp. 171–204. DOI: 10.7256/2306-0158.2013.1.342 .
4. Eliseev N. G. Izveshchenie otvetchika, nakhodiashchegosia za granitsei. Zakon, 2016, No. 6, pp. 121–137.
5. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
6. Lovtsov D.A. Sistemologiia informatsionnogo prava. Pravosudie/Justice, 2022, t. 4, No. 1, pp. 41–70. DOI: 10.37399/2686-9241.2022.1.41-70 .
7. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
8. Lovtsov D.A., Niesov V.A. Formirovanie edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii. Rossiiskoe pravosudie, 2008, No. 11 (31), pp. 78–88.
9. Lukashenkova T.V. Okazanie arbitrazhnymi sudami mezhdunarodnoi pravovoi pomoshchi. Arbitrazhnyi i grazhdanskii protsess, 2006, No. 12, pp. 30–31.

10. Petrova M.M. Tendentsii razvitiia pravovogo regulirovaniia v sfere okazaniia mezhdunarodnoi pravovoi pomoshchi po sboru i polucheniiu dokazatel'stv, nakhodiashchikhsia na territorii inostrannykh gosudarstv, po grazhdanskim delam. Iurisprudentsiia, 2011, No. 3, pp. 136–142.
11. Terent'eva L.V. Organizatsionno-pravovye osobennosti ispol'zovaniia videokonferentssviazi v arbitrazhnykh sudakh. Pravovaia informatika, 2017, No. 3, pp. 59–65. DOI: 10.21681/1994-1404-2017-3-59-65 .
12. Terent'eva L.V. Poniatie kiberprostranstva i ocherchivanie ego territorial'nykh konturov. Pravovaia informatika, 2018, No. 4, pp. 66–71. DOI: 10.21681/1994-1404-2018-4-66-71 .
13. Terent'eva L.V. Upravlenie kiberprostranstvom po modeli mul'tisteĭkkholderizma. Pravo i ekonomika, 2019, No. 3 (373), pp. 11–20.
14. Unifikatsiia i garmonizatsiia v mezhdunarodnom chastnom prave. Voprosy teorii i praktiki : monografiia. Otv. red. G.K. Dmitrieva, M.V. Mazhorina. M. : Norma, INFRA-M, 2022. 208 pp. ISBN 978-5-91768-753-7.
15. Apostolos A. Digitalization of civil justice in the European Union. Alatoo Academic Studies. 2023. No. 1. Pp. 470–479. DOI: 10.17015/aas.2023. 231.44 . EDN: HWKEVC.
16. Francesconi E., Peruginelli G., Steigenga E., Tiscornia D. Conceptual Modeling of Judicial Procedures in the e-Codex Project. Casanovas P. et al. (Eds.) AI Approaches to the Complexity of Legal Systems: AICOL 2013. Part of the Lecture Notes in Computer Science, V. 8929. Springer Berlin Heidelberg. 2014. Pp. 202–216. DOI: 10.1007/978-3-662-45960-7_15 .
17. Harkness T. P. Discovery in international civil litigation. Washington, DC: Federal Judicial Center, 2015. Pp. 18–20.

АНАЛИЗ МОНОГРАФИИ В.В. ОМЕЛЬЧЕНКО «ОБЩАЯ ТЕОРИЯ КЛАССИФИКАЦИИ»

Ловцов Д.А.[1]

Ключевые слова*: анализ, классификация, теория, всеобщность, качество, классы, методы, отношения, познание.*

Аннотация

Цель работы: научная оценка современного состояния использования универсальных методов классификации в системном познании исходного (неструктурированного, неупорядоченного, необусловленного) бесконечного множества (универсума) объектов, процессов и явлений реальности (мира, действительности, бытия).

Методы: системный и экспертный анализ монографии как научного труда, направленного на решение актуальных научных проблем классификации.

Результаты: исследованы содержание, структура, предназначение, актуальность, прагматические достоинства и апробация монографии; дана общая оценка монографии как общей теории классификации, базирующейся на использовании фундаментальных отношений тождества и различия, включая философские положения систематизации объектов, процессов или явлений реальности; в предложенной теории обоснован и представлен универсальный, всеобщий, эффективный инструмент познания исходного бесконечного множества объектов, процессов и явлений реальности.

Показаны роль и место общей теории классификации в познании и системе наук, общесистемные понятия и положения которой представляется целесообразным рассматривать как объекты междисциплинарных исследований.

EDN: JMSYDK

В любой современной книге о теории познания — логике, рассмотрению понятия «классификация» уделяется определенное внимание [3]. Умение правильно классифицировать предметы и объекты на классы часто называют *искусством классификации*[2]. Однако, несмотря на большое количество публикаций, посвященных рассмотрению этого вопроса уже в настоящее время[3] [14, 15], общесистемная (гносеологическая) сущность классификации не полностью раскрыта, не рассмотрен глубинный механизм классификации. Более того, само понятие «классификация» как действие (операция, метод) представляется весьма упрощенно в виде частного случая деления — логической операции над понятиями, при реализации которой выделяются: делимое понятие, основание деления, члены деления[4]. При этом классификация проводится по принципу двузначности или закону «исключенного третьего» [3]. Соответственно, любая другая классификация, проводимая не по указанному принципу, считается неправильной или ошибочной, что далеко не так.

Существующие на современном этапе подходы к классификации объектов, процессов и явлений реальности ориентированы, как правило, на прикладную, предметную сторону. В то же время концептуальной или общесистемной (гносеологической) стороне проблемы классификации в современной литературе уделяется мало внимания.

Рассмотренная в монографии тематика по систематизации объектов или процессов реальной действительности представляется достаточно актуальной. Развитие науки как сферы человеческой деятельности, направленной на систематизацию накопленных и получаемых новых объективных знаний о природе, обществе и самом человеке, базируется на «итерационной» разнообразной и многоаспектной систематизации и

[2] Ивлев Ю.В. Логика : учебник. М. : ТК «Велби», 2006. 288 с.

[3] Большой энциклопедический словарь. М. : Научное изд-во «БРЭ». СПб. : Норинг, 2000; Воронин Ю.А. Теория классифицирования и её приложения. Новосибирск : Наука, Сиб. отделение, 1985. 232 с.; Мейен С.В., Шрейдер Ю.А. Методологические аспекты теории классификации // Вопросы философии. 1976. № 12. С. 67—79; Философский словарь / Под ред. И.Т. Фролова. М. : Республика, 2001. 720 с.; Философская энциклопедия. В 5-ти тт. Т. 5. М. : Сов. энциклопедия, 1970.

[4] Новейший философский словарь. 3-е изд., исп. М. : Кн. дом. 2003. 1280 с.

[1] ***Ловцов Дмитрий Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заместитель по научной работе директора Института точной механики и вычислительной техники им. С.А. Лебедева Российской академии наук, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: dal-1206@mail.ru

классификации объектов исследования — упорядоченному их распределению по определённому признаку (свойству, характеристике), позволяющему установить их сходство (тождество) или различие. При этом на начальных этапах научных исследований используется, как правило, интуитивная дихотомическая классификация, а по их окончании — более продуктивная классификация на основе разработанной адекватной модели предметной области.

Вместе с тем продуктивность любой системы классификации в значительной степени определяется используемым категорийно-понятийным аппаратом, что обусловливает необходимость разработки общенаучного формально-логического аппарата — *теории систематизации*, обладающей достаточной общностью (широтой) и конструктивностью (глубиной). Требование конструктивности, т. е. формулирования (желательно в математической форме) не только общих, но и достаточно глубоких законов (*принципов* [4, 7, 8], основ) классификации, диктуется необходимостью унификации методологии систематизации в современных условиях интеграции научного знания.

Методология систематизации как учение о структурах (включая функциональную структуру — логическую организацию), системе принципиальных методов и комплексе средств систематизации, согласно трёхуровневой иерархии научного знания, имеет соответственно философский, системологический (общенаучный) и конкретно-научный (специальный) уровни [5]. Последний представлен наиболее полно, так как во всех конкретных науках разработаны и имеются достаточно продуктивные специфические методы систематизации своего материала. Унификация предполагает развитие методологии систематизации и классификации, прежде всего, философского и системологического уровней. Следовательно, первоочередными объектами рассмотрения при создании теории общей систематизации (классификации) являются её философские и системологические основы, исследованию которых и посвящена монография доктора технических наук, профессора, заслуженного деятеля науки и техники России Виктора Валентиновича Омельченко [9].

Рецензентами монографии выступили: д.т.н. Б.М. Абдрашитов, д.ф.-м.н., проф. В.Е. Кривоножко, д.филос.н., проф. Ю.В. Курносов и автор этой статьи.

Первое издание монографии «Общая теория классификации» вышло в свет в 2008—2010 гг. в двух книгах:

- книга 1 «Основы системологии познания действительности» — в издательстве ООО «ИПЦ Маска» [10];
- книга 2 «Теоретико-множественные основания» — в издательстве «Книжный дом «Либроком» [11].

Основной целью монографии первой редакции было обобщение [12] результатов докторской диссертации В.В. Омельченко и разработка общей теории классификации — основы *системного* познания исходного (неструктурированного, неупорядоченного, необусловленного) бесконечного множества (универсума) объектов, процессов и явлений реальности (мира, действительности, бытия), — такой теории, её понятий, положений, принципов и методов, которые являются универсальными, всеобщими и независимыми от предметной ориентированности.

После выхода в 2008—2010 гг. первого варианта монографии автор не спешил переиздавать её в новой улучшенной редакции, несмотря на обращения и пожелания от издательской группы URSS (издательство «Книжный дом «Либроком», «Издательство ЛКИ», «Издательство «Ленанд»). В новой второй редакции монографии 2024 г. её структура и основное содержание, по сути, не изменились, хотя качество формализованного представления общей теории классификации значительно улучшилось.

Структура и содержание второй редакции монографии «Общая теория классификации» представлены на рисунке. В монографии, состоящей из 2-х взаимосвязанных частей, последовательно рассматриваются «Методологические основы классификации объектов, процессов и явлений реальности» (кн. 1 в двух частях, включая философские положения классификации — принципы и законы познания реальности) и «Теоретико-множественные основания» (кн. 2, включая «Основы теории классификации и структурно-бинарного подхода к описанию и представлению объектов, процессов и явлений реальности»).

В ***первой*** главе рассматриваются общие подходы к пониманию и решению проблем классификации, в том числе следующие.

1. О сущности понятий *«классификация»* и *«систематизация»* (классификация объектов, процессов и явлений в древних писаниях; существующие подходы к пониманию сущности классификации, классификация и чувственное восприятие, классификация как интеллектуальная деятельность человека.

2. Предметные и общесистемные положения классификации.

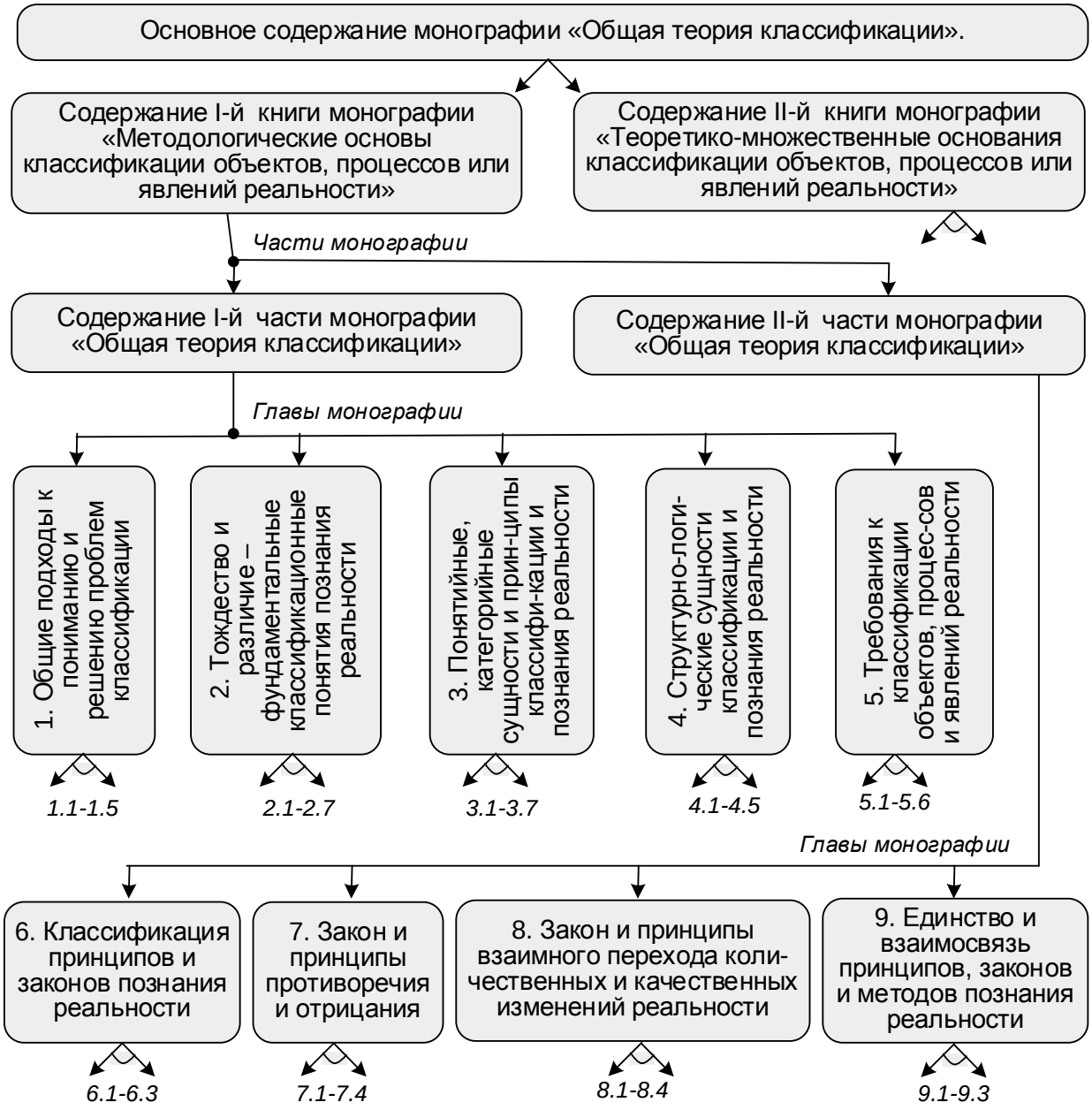
3. Классификация в познавательной деятельности человека (классификация — основа систематизации объектов, процессов и явлений реальности, как источник предметного знания, как метод и средство познания).

4. Осуществлен поиск механизма классификации (рассматриваются взаимосвязи понятий *«определение»* и *«классификация»,* взаимосвязи отождествления, различения и классификации, логико-интуитивное обоснование механизма классификации, базовые основы механизма классификации объектов, процессов и явлений реальности).

5. Обосновываются роль и место общей теории классификации в многоуровневой системе научных знаний.

Во ***второй*** главе осуществляется анализ тождества и различия — фундаментальных классификационных понятий познания реальности; в том числе рассматриваются:

1. Проблема научного определения фундаментальных отношений тождества и различия (традиционное



Структура и содержание монографии «Общая теория классификации»

представление понятий *тождество* и *различие,* о понятиях «тождество» и «различие» в живом великорусском языке и древних писаниях).

2. Базовые бинарные свойства — основа фундаментальных классификационных отношений тождества и различия (ведение общих классификационных понятий взаимоотношения между элементами множества *«самоотражение»* и *«несамоотражение»*, *«соразмерность»* и *«несоразмерность»*, *«переходность»* и *«непереходность»* — базовые свойства и отношения понятий тождества и различия).

3. *Порядок* и *непорядок* — свойства и отношения реальности (существующий подход к определению понятий *«порядок»* и *«непорядок»,* концептуальный уровень определения понятий *«порядок»* и *«непорядок»,* классификация свойств и отношений *порядка* в системе «порядок-непорядок», свойства и отношения *непорядка, предпорядка, порядка,* свойства и отношения *включения* — упорядоченности множеств, классификация свойств и отношений упорядоченности).

4. Структурно-логические свойства и отношения *связанности* объектов, процессов и явлений реальности (существующие подходы к описанию структурно-логических свойств и отношений реальности, определение структурно-логических свойств и отношений).

5. Свойства и отношения *тождества* — фундаментального понятия теорий познания и классификации (*самоотражение* — первое базовое свойство и отношение тождества, *подобие* — второе соединительное свойство и отношение тождества, *нестрогий предпо-*

рядок — третье соединительное свойство и отношение тождества, *нестрогий порядок* — четвёртое соединительное свойство и отношение тождества, *одинаковость* — пятое соединительное свойство и отношение тождества, *равенство* — шестое соединительное свойство и отношение тождества).

6. Свойства и отношения *различия* — фундаментального понятия теорий познания и классификации (*несамоотражение* — первое базовое свойство и отношение различия, *неподобие* — второе соединительное свойство и отношение различия, *строгий предпорядок* — третье соединительное свойство и отношение различия, *строгий порядок* — четвертое соединительное свойство и отношение различия, *неодинаковость* — пятое соединительное свойство и отношение различия, *неравенство* — шестое соединительное свойство и отношение различия, строгое определение понятия различия).

7. Система свойств и отношений *тождества* и *различия* — фундаментальных понятий теорий познания и классификации (гносеология свойств, отношений и понятий тождества и различия — основы классификации реальности, область определения понятий *тождества* и *различия* в пространстве объектов, процессов и явлений реальности, классификационная система свойств и отношений *тождества* и *различия,* логика формирования фундаментальных отношений *тождества* и *различия*).

В ***третьей*** главе представлены понятийные, категорийные сущности и принципы классификации и познания реальности, в том числе рассматриваются:

1. Анализ и систематизация классификационных понятий (классификация основных общесистемных сущностей познания реальности, анализ классификационных понятий, историческое осмысление классификационного понятия «символ», существующие определения понятий «символ», «символика» и «символизм», общесистемность и универсальность понятия «символ», новые определения понятий символики).

2. Анализ и классификация общесистемных категорий познания объектов, процессов и явлений реальности (существующие подходы к описанию категорий познания реальности, классификация общесистемных категорий познания реальности, рассмотрение с позиций классификации категорий: *единичного* и *общего, целого* и *части, качества* и *количества, конкретного* и *абстрактного*).

3. Анализ и классификация форм умозаключений познания реальности (троица системных сущностей умозаключения, общая классификация форм умозаключений, сущность второй формы умозаключения, сущность третьей формы умозаключения).

4. Принципы классификации реальности.

5. Принцип целеполагания классификации реальности и проблема его реализации (анализ существующих подходов к определению и обоснованию принципа целеполагания, классификация принципа целеполагания).

6. Принцип познаваемости реальности и проблема его реализации (принцип познаваемости с философских позиций и с позиций общей теории классификации, принцип системности, принцип упорядоченности, принцип цикличности).

7. Принцип объективности классификации реальности и проблема его реализации (частные принципы *достоверности* и *соответствия* классификации).

В ***четвертой*** главе рассмотрены структурно-логические сущности классификации реальности, в том числе:

1. Структурные положения классификации объектов, процессов или явлений реальности.

2. Классификация на базе применения последовательных структур классификационных элементов (классификация последовательно упорядоченных систематизаций, статическая и динамическая формы представления классификаций).

3. Классификация на базе применения радиальных, полносвязанных и комбинированных структур.

4. Классификация объектов, процессов и явлений реальности на базе применения многоуровневых структур (многоуровневые классификации, классификация на базе применения графов, словесная или дескрипторная классификация, библиографическая классификация, двоичная, троичная и «многоичная» классификации, геометрическая или фрактальная классификация, достоинства и недостатки многоуровневой классификации);

5. Классификация объектов, процессов или явлений с использованием логики разных описаний (классификация с использованием логики: видо-родовых, причинно-следственных и пространственно-временных свойств и отношений [3]).

В ***пятой*** главе рассмотрены требования к классификации объектов, процессов и явлений реальности, в том числе:

1. Анализ существующих подходов к заданию требований к классификации.

2. Требования к целеполаганию классификации объектов, процессов и явлений реальности.

3. Требования к эффективности классификации (проблема эффективности решения научно-практических задач, целеориентированность оценки эффективности классификации, классификация показателей и критериев эффективности решения научно-практических задач, методические рекомендации по обоснованию и выбору критериев эффективности решения научно-практических задач, результативность, реализуемость, ресурсоемкость и ресурсообеспеченность классификации).

4. Требования к целостности классификации объектов, процессов и явлений (полнота и последовательность декомпозиции на классы).

5. Требования к достоверности классификации объектов, процессов и явлений реальности (тождественность принятой модели классификации истинному состоянию реальности, обоснование и выбор оснований классификации, требования к глубине и четкости классификации, общие требования к классификации

объектов, процессов и явлений реальности, требования к компактности, простоте, наглядности, гибкости классификации).

В ***шестой*** главе проведена классификация принципов и законов познания реальности, в том числе:

1. Описание и представление принципов и законов познания (традиционный и системный подходы к описанию и представлению принципов и законов познания).

2. Закон тождества и различия — базовый закон познания реальности (традиционное представление закона тождества и различия, принципы тождества и различия — основные принципы познания реальности).

3. Закон классификации объектов, процессов и явлений — базовый закон познания реальности.

В ***седьмой*** главе рассмотрены с позиций классификации закон и принципы противоречия и отрицания, в том числе:

1. Существующие подходы к определению принципа или закона противоречия и отрицания.

2. Структурно-логические аспекты закона противоречия и отрицания.

3. Логико-диалектические аспекты закона противоречия и отрицания.

4. Особенности закона противоречия и отрицания при классификации объектов или процессов реальности.

В ***восьмой*** главе с позиций классификации рассмотрен закон и принципы взаимного перехода количественных и качественных изменений реальности, в том числе:

1. Закон взаимного перехода количественных и качественных изменений реальности (классификация качественно-количественных изменений реальности, объяснение закона взаимного перехода количественных и качественных изменений реальности, в том числе с позиций познания реальности).

2. Закон исключения третьего и отрицания.

3. Закон переходности и отрицания.

4. Закон достаточного основания и отрицания.

В ***девятой*** главе с позиций классификации рассмотрены единство и взаимосвязь принципов, законов и методов познания реальности, в том числе:

1. Систематизация взаимосвязей принципов и законов познания.

2. Особенности соотношения законов познания в единстве их взаимосвязей (особенности проявления законов: противоречия и отрицания, исключения третьего и отрицания, переходности и отрицания);

3. Познание как наука о всеобщих законах, принципах и методах отражения реальности (основные функциональные элементы познания реальности, содержание и формы познания реальности, классификация как основа познания реальности).

Таким образом, в данной работе автор достаточно подробно и наглядно показал, что общая теория классификации, её основные понятия, положения, принципы, логика и методы универсальны и применимы как для общих, так и для прикладных наук, а также для любых объектов, процессов и явлений реальности (мира, действительности, бытия) во всех предметно-ориентированных сферах деятельности человека.

Монография предназначена для разработки общей теории систематизации, базирующейся на методологических принципах аксиоматического подхода к определению фундаментальных понятий тождества и различия. В основу монографии положены труды автора, опубликованные в 1994—2000 гг. в изданиях РАН, а также использована обширная философская, математическая, научно-техническая и др. литература за период с начала зарождения научного знания в древних писаниях и по сегодняшний день. Общие принципы и методы построения монографии, многочисленные содержательные примеры получили широкое обсуждение в 1999—2006 гг. на Межвузовском постоянно действующем научном семинаре Военной академии имени Петра Великого «Информатизация управления», руководимом рецензентом — автором данной статьи, а также в открытой печати.

В книге подробно и диалектически рассмотрены *основы систематизации*: понятия, отношения, аксиомы, принципы, законы, правила, а также концепция и основы комплексного системно-информационного подхода к описанию и представлению принципов и законов познания [5, 13]. Причём материал изложен с учётом решения практических задач распознавания, диагностики, идентификации и контроля состояния сложных динамических объектов [5].

В целом, изложенные в монографии концептуально-философские принципы и обоснованный формально-логический аппарат систематизации объектов произвольной природы предназначены для повышения эффективности применения *информационно-математического обеспечения* профессиональной управленческой деятельности, в связи с чем автором были привлечены известные работы по информатизации и оптимизации управления сложноорганизованными объектами технических, технологических, экономических, экологических, организационно-правовых и др. комплексов [1, 2, 5—8].

Монография успешно апробирована в научной деятельности Института системного анализа Российской академии наук, Государственного НИИ системного анализа Счетной палаты Российской Федерации, а также в учебном процессе Военной академии имени Петра Великого, Российского государственного университета правосудия, Южно-Российского института финансового контроля и аудита и получила высокую оценку преподавателей, аспирантов, слушателей, курсантов и студентов.

Предложенный в монографии подход к классификации и систематизации включен в «Государственные требования к минимуму содержания и уровню требований к специалистам для получения дополнительной квалификации «Аудитор государственного и муниципального управления», которые введены в действие приказом Министерства образования и науки Российской Федерации от 15 февраля 2008 г. № 58. Эти требо-

вания легли в основу эксперимента по обучению специалистов контрольно-счетных органов Российской Федерации по новому направлению подготовки «Аудит государственного и муниципального управления», проводимого в Южном Федеральном округе на базе Южно-Российского института финансового контроля и аудита.

Автору целесообразно продолжить развитие своего научного проекта и получение новых интересных обобщений и результатов, а его ученикам — направить усилия на практическое внедрение методов общей теории классификации в различные предметно-ориентированные направления деятельности.

Данную монографию можно рекомендовать для изучения эргатических (человеко-машинных) систем (эргасистем) различного государственного уровня и назначения во всех научных институтах и вузах страны.

Литература

1. Борисов Р.С., Ефименко А.А. Классификатор правовых актов для установления правового режима публикуемой информации // Правовая информатика. 2021. № 4. С. 31—45. DOI: 10.21681/1994-1404-2021-4-31-45 .
2. Бурый А.С. Лингвистические аспекты формирования терминологической базы информационных систем // Правовая информатика. 2021. № 4. С. 46—56. DOI: 10.21681/1994-1404-2021-4-46-56 .
3. Королев В.Т., Ловцов Д.А., Радионов В.В. Системный анализ. Часть. 2. Логические методы / Под ред. Д.А. Ловцова. М. : РГУП, 2017. 160 с.
4. Ловцов Д.А. Классификатор правовых режимов информации ограниченного доступа: принципы создания // Актуальные проблемы информационно-правового пространства : сб. науч. тр. XI Всеросс. науч.-прак. конф. «Общество и право в информационном пространстве» (26 декабря 2016 г.) / СКФ РГУП. Краснодар : СКФ, 2017. С. 104—111.
5. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
6. Ловцов Д.А. Информационные правоотношения: особенности состава и продуктивная классификация // Информационное право. 2009. № 1. С. 3—6.
7. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54 .
8. Ниесов В.А. Систематизация законодательства в сфере защиты информации судопроизводства // Проблема информационной безопасности. Компьютерные системы. 2014. № 4. С. 126—132.
9. Омельченко В.В. Общая теория классификации. В двух кн. Кн. I. Методологические основы классификации объектов, процессов или явлений / Предисл. Д.А. Ловцова. М. : КнигИздат, 2024. 770 с. ISBN 978-5-4492-0542-1.
10. Омельченко В.В. Общая теория классификации. В двух частях. Часть I. Основы системологии познания действительности / Предисл. Д.А. Ловцова. М. : ИПЦ «Маска», 2008. 466 с. ISBN 978-5-91146-297-0.
11. Омельченко В.В. Общая теория классификации. В двух частях. Часть II. Теоретико-множественные основания // Предисл. Д.А. Ловцова. М. : Кн. дом «Либроком», 2010. 296 с. ISBN 978-5-397-01327-7.
12. Омельченко В.В. Теоретические основы классификации нечетких ситуаций при испытаниях сложных технических комплексов. М. : Военная академия им. Петра Великого, 1999. 628 с.
13. Омельченко В.В. Основы систематизации. В двух частях. М. : Кн. дом «Либроком», 2012. 480 с.
14. Покровский М.П. Введение в классиологию. Екатеринбург : ИГГ УрО РАН, 2014. 484 с.
15. Субботин А.Л. Классификация. М. : ИФ РАН, 2001. 94 с.

BOOK REVIEW

ANALYSIS OF THE MONOGRAPH BY V. OMEL'CHENKO "GENERAL THEORY OF CLASSIFICATION"

Dmitrii Lovtsov, *Dr.Sc. (Technology), Professor, Honoured Scientist of the Russian Federation, Deputy Director for Research of the Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Head of the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: dal-1206@mail.ru

Keywords: *analysis, classification, theory, universality, quality, classes, methods, relations, cognition.*

Abstract

Purpose of the work: academic assessment of the modern state of using universal classification methods in system cognition of the initial (unstructured, unordered, unconditioned) infinite set (universe) of objects, processes and phenomena of reality (the world and being).

Methods used: system and expert analysis of the monograph as a scholarly work aimed at solving topical academic problems of classification.

Study findings: the content, structure, purpose, topicality, practical advantages and assessment of the monograph are studied. A general evaluation of the monograph is given as of a general theory of classification based on using fundamental relations of identity and difference including philosophical provisions for systematisation of objects, processes or phenomena of reality. The proposed theory presents and justifies a universal, general, efficient tool for cognition of the initial infinite set of objects, processes and phenomena of reality.

The role and place of the general theory of classification in cognition and system of academic disciplines are shown, and it is deemed appropriate to consider the general system concepts and provisions of the theory as objects of interdisciplinary research.

References

1. Borisov R.S., Efimenko A.A. Klassifikator pravovykh aktov dlia ustanovleniia pravovogo rezhima publikuemoi informatsii. Pravovaia informatika, 2021, No. 4, pp. 31–45. DOI: 10.21681/1994-1404-2021-4-31-45 .
2. Buryi A.S. Lingvisticheskie aspekty formirovaniia terminologicheskoi bazy informatsionnykh sistem. Pravovaia informatika, 2021, No. 4, pp. 46–56. DOI: 10.21681/1994-1404-2021-4-46-56 .
3. Korolev V.T., Lovtsov D.A., Radionov V.V. Sistemnyi analiz. Chast'. 2. Logicheskie metody. Pod red. D.A. Lovtsova. M. : RGUP, 2017. 160 pp.
4. Lovtsov D.A. Klassifikator pravovykh rezhimov informatsii ogranichennogo dostupa: printsipy sozdaniia. Aktual'nye problemy informatsionno-pravovogo prostranstva : sb. nauch. tr. XI Vseross. nauch.-prak. konf. "Obshchestvo i pravo v informatsionnom prostranstve" (26 dekabria 2016 g.). SKF RGUP. Krasnodar : SKF, 2017, pp. 104–111.
5. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
6. Lovtsov D.A. Informatsionnye pravootnosheniia: osobennosti sostava i produktivnaia klassifikatsiia. Informatsionnoe pravo, 2009, No. 1, pp. 3–6.
7. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Pravovaia informatika, 2017, No. 2, pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .
8. Niesov V.A. Sistematizatsiia zakonodatel'stva v sfere zashchity informatsii sudoproizvodstva. Problema informatsionnoi bezopasnosti. Komp'iuternye sistemy, 2014, No. 4, pp. 126–132.
9. Omel'chenko V.V. Obshchaia teoriia klassifikatsii. V dvukh kn. Kn. I. Metodologicheskie osnovy klassifikatsii ob"ektov, protsessov ili iavlenii. Predisl. D.A. Lovtsova. M. : KnigIzdat, 2024. 770 pp. ISBN 978-5-4492-0542-1.
10. Omel'chenko V.V. Obshchaia teoriia klassifikatsii. V dvukh chastiakh. Chast' I. Osnovy sistemologii poznaniia deistvitel'nosti. Predisl. D.A. Lovtsova. M. : IPTs "Maska", 2008. 466 pp. ISBN 978-5-91146-297-0.
11. Omel'chenko V.V. Obshchaia teoriia klassifikatsii. V dvukh chastiakh. Chast' II. Teoretiko-mnozhestvennye osnovaniia. Predisl. D.A. Lovtsova. M. : Kn. dom "Librokom", 2010. 296 pp. ISBN 978-5-397-01327-7.
12. Omel'chenko V.V. Teoreticheskie osnovy klassifikatsii nechetkikh situatsii pri ispytaniiakh slozhnykh tekhnicheskikh kompleksov. M. : Voennaia akademiia im. Petra Velikogo, 1999. 628 pp.
13. Omel'chenko V.V. Osnovy sistematizatsii. V dvukh chastiakh. M. : Kn. dom "Librokom", 2012. 480 pp.
14. Pokrovskii M.P. Vvedenie v klassiologiiu. Ekaterinburg : IGG UrO RAN, 2014. 484 pp.
15. Subbotin A.L. Klassifikatsiia. M. : IF RAN, 2001. 94 pp.

Основные направления работы конференции

Современные технологии в информационном обществе

Посвящена применению информационных и коммуникационных технологий в образовании и социально-экономической сфере. Рассматриваются вопросы: управления образовательным процессом в высшем, среднем и начальном образовании; дистанционного обучения; применения ИКТ для повышения качества преподавания; применения ИКТ для управления, регулирования и повышения качества социальных и бизнес-процессов; и другие.

Фундаментальные, поисковые и прикладные исследования в науке, технике и технологиях

Рассматриваются вопросы использования современных ИКТ при проведении научных исследований и разработке новых видов техники и технологий в промышленности.

Энергетика и энергосберегающие технологии

Посвящена вопросам разработки новых видов источников энергии и их практического применения, использования альтернативных источников энергии в жизни и деятельности человека, повышения их эффективности.

Антенны, СВЧ техника, технологии и производство радиоэлектронных систем

Рассматриваются вопросы электромагнитной совместимости, излучения, приема и распространения электромагнитных волн, управления полями с помощью различных физических явлений, численного электродинамического моделирования, исследования, разработки и создания антенн, СВЧ-устройств, материалов и компонентов проектирования спецоборудования для радионавигации, радиолокации, телевидения, радиоастрономии, радиоуправления, радиоэлектронной борьбы и телекоммуникаций.

Передовые медицинские технологии

Рассматриваются вопросы применения современных технологий в различных областях здравоохранения

Основные сроки и условия участия в конференции.

30 июля 2024 г. — окончание льготного периода регистрации, приема материалов докладов и организационных взносов;

1 сентября 2024 г. — окончание регистрации, приема материалов докладов;

1 сентября 2024 г. — окончание приема организационных взносов;

1—10 октября 2024 г. — сроки проведения конференции

Регистрация в качестве участника конференции осуществляется на сайте конференции www.diag.ru путем заполнения соответствующей формы.

Место проведения

Краснодарский край, город-курорт Сочи, Адлерский курортный городок

LEGAL INFORMATICS

ISSN 1994-1404

1

2024

Scientific Centre for Legal Information
under the Ministry of Justice
of the Russian Federation

http://uzulo.su/prav-inf
E-mail: inform360@yandex.com
Telephone: (495) 197-89-06