ПРАВОВАЯ ИНФОРМАТИКА

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ
№ 1, 2023 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 31.03.2023 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
2023, 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 31th of March, 2022.
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

НОВЫЕ АКТУАЛЬНЫЕ ОСНОВАНИЯ МОДЕРНИЗАЦИИ В СФЕРЕ ИНФОРМАЦИОННОГО ПРАВА

Запольский С. В.[1], Исаков В. Б.[2]

Ключевые слова: *модернизация, цифровизация, информационное право, информационные правоотношения, финансовый контроль, информационно-правовое регулирование, достоверность информации, юридическая техника, систематизация, нормативный правовой акт, текущая редакция.*

Аннотация

Цель работы: исследовать изменения в правовой политике, вызываемые совершенствованием цифровых технологий в сфере правотворчества и правоприменения, в осуществлении государственной власти и управления, повышения эффективности финансового контроля.

Методы исследования: системный анализ, информационно-правовое моделирование и историческая экстраполяция.

Результаты: обоснованы требования к модернизации и цифровизации в сфере информационного права и правового регулирования информационных отношений в предметной области финансового контроля, налогообложения, ценообразования и бюджетного финансирования; определен рациональный двухэтапный порядок принятия поправок в нормативные правовые акты; обоснованы рекомендации законотворческим и правоприменительным органам по практической реализации тенденций научно-технической революции в сфере информационных технологий и цифровизации управленческой, контрольной и юрисдикционной деятельности, а также в области юридического образования и правовой науки.

DOI: 10.21681/1994-1404-2023-1-4-14

В настоящее время человечество находится в активной фазе очередной научно-технической революции, движущими факторами которой являются биотехнологии, информационные технологии и искусственный интеллект. Естественно, что соответствующие процессы не обходят и сферу права. В литературе высказан широкий спектр мнений о тенденциях и необходимых изменениях права и правового регулирования в новых условиях [5, 8]. Попытаемся выделить из них те, которые можно отнести к ближайшим и неотложным перспективам модернизации в сфере *информационного права* [7, 11].

Изменение объектов и предметов правового регулирования

Широкое распространение цифровых технологий в различных сферах деятельности, регулируемых правом, ведет к появлению новых общественных отношений и новых *предметов* регулирования. В определенном смысле предмет правового регулирования можно сравнить с сетью дорог: одни участки этой «сети» уже заасфальтированы и превращены в современные высокоскоростные цифровые магистрали; другие готовятся к «электронному асфальтированию»; третьи — представляют собой дороги и проселки, которые будут покрыты «электронным асфальтом» не скоро.

Какие участки считаются «хорошо заасфальтированными»? Можно указать на следующие виды *информационных правоотношений*: банковские (электронный банкинг); биржевые (электронные биржи, электронные биржевые маклеры); некоторые элементы транспортных отношений (продажа билетов, допуск на объекты транспортной инфраструктуры); конкурсы и тендеры (электронные торги и аукционы); электронная торговля (торговля через автоматы, интернет-торговля) и др.

К числу участков, которые только «готовятся к асфальтированию», можно отнести: управленческое делопроизводство (безбумажный документооборот); некоторые виды государственных услуг (далее — госуслуг) (получение документов, справок, свидетельств

[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] ***Исаков Владимир Борисович,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, профессор-исследователь НИУ «Высшая школа экономики», г. Москва, Российская Федерация.*
E-mail: visakov@hse.ru

и др.); некоторые виды страхования (например, страхование мелких автоаварий); некоторые процедуры разрешения споров (например, международный арбитраж по спорам о доменных именах: рассмотрение споров в международном арбитраже в Женеве производится дистанционно, в электронной форме, на основании представленных сторонами электронных документов); некоторые виды административной ответственности, где факт правонарушения можно надежно зафиксировать с помощью технических средств (ответственность за нарушение правил дорожного движения).

Наконец, существует группа отношений, компьютеризация которых проблематична. В группу последних можно отнести: конституционные отношения (структура и порядок формирования государственных органов, права и свободы граждан — за исключением отдельных процедур, например, электронного голосования); правонарушения и преступления, в правовую модель которых входят оценочные понятия: особая жестокость, исключительный цинизм и др.; семейные отношения и имущественные отношения граждан в семье: развод, оставление ребенка с родителями, раздел имущества, права на наследование, совместное проживание, отношения в области контроля и надзора и др.

Очевидно, что сфера информационных правоотношений, осуществляющихся в электронной форме, будет расширяться. Процесс расширения сферы компьютеризированных отношений определяют несколько факторов.

Технический фактор. Создаются все новые и новые компьютерные программы, средства коммуникации и технические устройства, меняющие облик производства и бытовую среду человека. Например, торговля в значительном объеме переходит в Интернет, медицина становится объектом теледоступа, образовательные системы приобретают планетарный характер, доступ к культурным ценностям (музеям, выставкам, картинным галереям) — бесплатным и круглосуточным и др. Причем процесс технических инноваций не остановить. Торможение инноваций в одной стране приводит лишь к тому, что открытия и инновации происходят в другой стране.

Политический фактор. Наиболее значимые общественные отношения, основные «несущие конструкции» общества и государства, такие как основы общественного и государственного устройства, система органов государственной власти и способы их формирования, гражданство, основные права и свободы человека и гражданина, на наш взгляд, останутся сферой «ручного» правового регулирования на достаточно долгий срок. Компьютеризировать их сложно, да и нецелесообразно. Компьютеризированы могут быть лишь отдельные формы и технологии их осуществления, например, избирательные процедуры, плебисциты и референдумы, а также способы осуществления ряда других конституционных прав (права на участие в государственном управлении, на труд, на информацию и др.).

Социальный фактор. Нельзя не учитывать, что значительная часть населения, особенно люди старшего поколения, психологически не готовы к использованию современных цифровых технологий. Они с недоверием относятся к использованию пластиковых карт, перечислению на них зарплат и пенсий, не имеют персональных аккаунтов в службе занятости, государственной налоговой службе, пенсионном фонде, на портале госуслуг и др. У многих нет адресов электронной почты, с которых можно было бы подать заявку и на которые получить официальную информацию, они испытывают затруднения при пользовании современными многофункциональными телефонами и др. Даже православная церковь, выражая опасения верующих, выступила против цифровых идентификационных номеров граждан, без которых невозможно массовое внедрение информационных технологий в сфере управления и бизнеса[3].

При этом широкие слои населения не доверяют не столько технике, сколько целям и намерениям органов управления, продвигающих внедрение цифровых технологий в сферах производства, управления и обслуживания, но решительно не желающих что-либо менять в отношениях, которые обеспечивают их положение в обществе. В результате технический прогресс и прогресс в социальных отношениях идут несинхронно, разными темпами [20]. Разрыв новой технической реальности и консервативных социальных отношений становится все более заметным и драматичным. Очевидно, что в этих условиях преждевременный демонтаж нормативно-правовых гарантий и правовых процедур, массовая замена их компьютерными (цифровыми) информационными технологиями могут привести не к социальному прогрессу, а к еще большему социальному эгоизму и безответственности правящих элит, подавлению социальной и экономической активности, снижению правовой и социальной защищенности личности.

Среди ученых-юристов идет дискуссия об изменениях в средствах и методах воздействия на общественные отношения. Высказывается, в частности, мысль о необходимости алгоритмизации права, «переводе в цифру» действующих юридических норм [10]. Вот как видят этот процесс руководители проекта автоматизации права А. Вашкевич и А. Дуюнов: «*Законодательные инициативы по-прежнему готовятся на привычном, естественном языке. По сути, инициативы — это техническое задание. Затем эти инициативы с помощью языка программирования… перерабатываются в код, готовится законопроект в машиночитаемом виде. На следующем этапе законопроект автоматически проверяется на соответствие уже принятым законам. Система сравнивает новый акт с предыду-*

[3] См.: Официальная позиция Русской Православной Церкви по проблемам электронной идентификации личности. URL: https://ruskline.ru/analitika/2016/10/04/oficialnaya_poziciya_russkoj_pravoslavnoj_cerkvi_po_problemam_elektronnoj_identifikacii_lichnosti

щими — формирует отчёт о выявленных несоответствиях или противоречиях… Рассмотрение проекта проходит в привычном режиме — законодатель, с помощью специального браузера, видит текст на естественном языке. Голосует в этом же браузере, но закон принимается именно в виде кода»[4].

На наш взгляд, более перспективным направлением модернизации средств и методов правового регулирования является *социально-правовой реинжиниринг* общественных отношений, т. е. такая их перестройка, когда резко сокращается необходимость в принятии, толковании и применении правовых норм, исчезают старые предметы правового регулирования и появляются новые [4]. В качестве примера успешного социально-правового реинжиниринга можно привести *смарт-контракты* [19], которые представляют собой компьютерные программы, предназначенные для заключения, проверки и контроля исполнения контрактов в цифровом виде. Смарт-контракты сегодня реально используются в высококомпьютеризированных областях бизнеса, таких как банковское дело, страхование, некоторые отрасли промышленности. Нельзя не заметить, что в этом случае происходит полный реинжиниринг регулируемых правом отношений: пакет смарт-контрактов может заменить целый штат юристов и управленцев[5]. Соответственно, исчезают административные и трудовые правоотношения, появляются правоотношения технического сервиса, обеспечения безопасности, страхования новых видов рисков и др. Очевидно, что в данном случае происходит не просто «алгоритмизация права» — осуществляется полный демонтаж прежнего правового регулирования с его заменой новыми техническими инструментами.

Социальный инжиниринг, появление новых отношений и новых предметов правового регулирования неизбежно отражаются на системе и структуре права. На наш взгляд, не проблема *системы права* носит застойный характер, а в ее научной разработке существует многолетний застой и пока не просматриваются новые подходы. Проблематика системы права — не недостаток, а напротив, одна из позитивных сторон, отличающих советскую, а теперь и российскую юридическую науку от зарубежной. В.Н. Синюков, как представляется, совершенно обоснованно связывает проблему системы права с духом социального оптимизма и «социального конструктивизма», которым было пронизано раннее советское общество [18].

Модернизация процесса законотворчества

Можно привести немало примеров, когда технический прогресс в сфере права затронул и область законотворчества. Тем не менее *нормативные правовые акты* (НПА), принимаемые в бумажной форме, до сих пор обрабатываются децентрализованно ведомственными справочно-кодификационными службами. Для этих целей используются картотеки, картоматы, ведение служебных «контрольных экземпляров» НПА. Одной из популярных техник кодификационной работы до недавнего времени были «вклейки и вычеркивания», когда дополнения подклеивались в бумажную версию НПА, а места, утратившие силу — вычеркивались. Разумеется, в современных условиях для ведения «контрольных экземпляров» широко используется электронная техника [15].

Нередко сам законодатель дает указания столь общего характера («*изменить наименование по всему тексту закона*», «*включить термин по всему тексту закона в соответствующем роде, числе и падеже*»), что они воспринимаются и реализуются кодификаторами по-разному. При сохранении децентрализованной кодификационной обработки НПА исключить подобные ситуации практически невозможно [17]. Приведенные примеры говорят о том, что существующая практика технико-юридической обработки «бумажных» НПА не лишена недостатков, которые в современных условиях становятся все более и более очевидными.

Проблема создания и поддержания в актуальном состоянии «текущих редакций» НПА — одна из самых сложных в *юридической технике* законотворчества. В ходе традиционного «бумажного» законотворчества законодатель принимает *базовый* НПА, затем в разное время и по разным обстоятельствам вносит в него изменения и дополнения, оформляя их самостоятельными НПА. Каждая новая поправка образует новую *текущую* (актуальную на данный момент) *редакцию* базового НПА. Кто и как должен оформлять эту новую «текущую редакцию»?

В сложном положении оказались официальные правовые базы данных. Законодатель уполномочил их публиковать в электронном виде принятые НПА и признал опубликованные версии официальными. Однако он не уполномочил их создавать официальные текущие редакции НПА, т. е. не предоставил им права вести *официальную текущую кодификацию*, которая поддерживала бы НПА в актуальном контрольном состоянии. Конечно, это упростило ведение официальных баз данных, но одновременно сделало их неполнофункциональными и неконкурентоспособными на рынке правовой информации. На официальном интернет-портале правовой информации в тестовом режиме запущена база данных «Тексты федеральных законов с внесенными изменениями»[6]. Коммерческие правовые базы данных предоставляют аналогичную информацию уже несколько десятилетий.

Проблема создания и поддержания в актуальном состоянии текстов НПА должна быть решена, на наш взгляд, следующим способом: создание и ведение «текущих редакций» НПА должно быть вменено в обязан-

[4] Автоматизация права. Новые резервы эффективности. Сценарии и технологии. Версия 2.0 // Симплоер. [Б. г.]. С. 8—9.

[5] Кругликов К. Что такое смарт-контракты? URL: http://yandex.ru/q/law/7001555201

[6] См. URL: http://pravo.gov.ru/ips/

ность органам, принимающим данные акты. В этом случае отпадет первооснова для появления устаревших, неактуальных или конфликтующих межу собой «текущих редакций» [10].

Из данного предложения вытекает, что при принятии любой поправки в НПА должно происходить не одно, а *два голосования: первым* голосованием принимается поправка, *вторым* голосованием – утверждается НПА в новой редакции с включенной в него поправкой. Именно эта редакция и будет считаться официальной «текущей редакцией» НПА на данный момент. Только подобным способом, на наш взгляд, можно ликвидировать разобщенную децентрализованную кодификацию, обеспечить пользователей безупречными текущими редакциями НПА, исключить появление «детей лейтенанта Шмидта» — устаревших, неактуальных, противоречащих друг другу «текущих редакций».

Мы привели один конкретный пример неадекватности устоявшегося, но явно устаревшего кодификационного подхода, препятствующего модернизации законотворчества. Обозначим, хотя бы кратко, некоторые другие проблемы:

- постоянный необоснованный рост количества НПА, являющийся в значительной мере результатом отсутствия последовательной правовой политики в данном вопросе и невнимания руководителей госструктур к данному аспекту законотворчества;
- низкий уровень стабильности НПА, частое изменение (иногда по нескольку раз в год) базовых НПА, что мешает предпринимателям, предприятиям и организациям в формировании рабочих программ и бизнес-планов;
- отсутствие разумного баланса между *инструктивностью* (описательностью) и *нормативностью* НПА;
- принятие разнопредметных по содержанию НПА (депутаты называют их «братскими могилами»);
- присвоение НПА одинаковых наименований (так, почти 400 федеральных законов, принятых Государственной Думой действующего VII созыва, имеют в своем наименовании слова: «О внесении изменений в отдельные законодательные акты Российской Федерации»);
- внесение новых изменений не в первичные документы, а в их «изменения» и даже изменений в изменения изменений, что принципиально противоречит правилам юридической техники и существенно затрудняет кодификацию законодательства.

Более двадцати пяти лет развития российского законодательства в русле новой Конституции РФ породили огромный и сложный нормативно-правовой массив. За это время в России не проводилось масштабных кодификационных работ. В результате практически во всех отраслях законодательства накопился материал, требующий *систематизации* и кодификации. Со всей определенностью перед российской юридической наукой встает вопрос о подготовке к проведению очередной плановой систематизации и кодификации действующего законодательства.

Трудно согласиться с политиками, депутатами и некоторыми учеными, что в современных условиях в силу высокого уровня развития информационных технологий *проблема систематизации* законодательства утратила значение. Дело вовсе не в том, что с помощью современных компьютерных поисковых инструментов можно в считанные секунды найти любой закон, правоприменительный акт, вообще любой документ. Необходимость систематизации законодательства диктуется не только удобством поиска и обнаружения НПА, хотя и это, конечно, не последний вопрос, а необходимостью поддержания *системности* самого права, правового регулирования, государственного управления и, как следствие, — системности возникающих на их основе общественных отношений [6, 11, 14, 16]. Реально упорядочить жизнь общества и общественные отношения может лишь то, что само систематизировано, организовано, упорядочено. Законодательство, которое разрозненно, запутано, противоречиво, — не в состоянии справиться с этой задачей.

Государство должно серьезно озаботиться развитием и укреплением информационно-правовой культуры общества и граждан. Умышленное искажение информации, ложь и клевета, неисполнение обязанностей по внесению и обновлению данных, необоснованное ограничение доступа к информации — могут иметь в современном информационном обществе катастрофические последствия. Подобные действия должны наказываться максимально строго, невзирая на должностной статус лица, отравившего общество дезинформацией.

О правовой природе контроля и надзора как института государственного управления

Переориентирование российской хозяйственной системы на решение публичных задач, в том числе интересов государства по обеспечению суверенитета страны в ходе СВО и других потребностей общенационального характера предполагает глубокое познание правовой природы каждого из применяемых инструментов регулирования. В этом смысле *контроль и надзор*, выступая как важнейший канал обратных связей центров управления с управляемыми субъектами, действующими преимущественно в автономном режиме, приобретают ведущее значение во всем механизме хозяйствования [9].

Стране предстоит глубокая реформа сложившихся форм управления экономическим развитием, включая перестройку финансового механизма. Налогообложение и другие формы мобилизации средств в доходы государства, бюджетные отношения, практика финансирования народного хозяйства в целом, кредитно-расчетные отношения, валютная политика, т. е. все то, что охватывается понятием «финансового механизма»,

одновременно с предстоящими реформами нуждается в существенном повышении качества *информации финансового контроля*.

Предотвращение противоправных посягательств на финансовые ресурсы государства, повышение эффективности использования мобилизуемых средств для финансирования тех или иных экономических мероприятий, оценка применяемых форм и методов управления невозможны без осуществления на современной информационно-цифровой основе финансового контроля.

Контролю и надзору посвящено большое количество научных исследований. Заметим, однако, что этот институт изучается как вид управленческой деятельности, который, как и любая деятельность вообще, не является предметом науки права. Мы полагаем, что только те или иные отношения являются объектом юридического анализа, но не контрольная деятельность как таковая. В силу этой причины информационные правоотношения, возникающие в ходе контроля и надзора, остаются малоизученными, что негативно сказывается как в целом на правовом регулировании, так и на эффективности *цифровых методов контроля*. Поэтому успех цифровизации контроля и надзора во многом зависит от точности учета особенностей складывающихся здесь правоотношений и отражения этих особенностей в применяемых юридических конструкциях.

Главный дефект господствующей конструкции контроля, а под ним мы понимаем прежде всего *финансовый контроль* — ориентация на *проверку* как на контрольную операцию деятельности (действия или бездействия) подконтрольного субъекта. Этим мы ограничиваем осуществление контроля, вытекающее из всех функций контроля, только возможностью совершения неких технических действий — проверочных мероприятий. К ним на практике относят простую проверку, выездную проверку, документальную проверку, рейды, контрольные закупки, инспекционные визиты и др. Между тем потенциальный инструментарий финансового контроля значительно шире, он и может и должен строиться на принципиально иной методологической базе. Далеко не случайно в последнее время в практику входит ограничительное планирование проверок (по принципу — не более такого-то количества за период времени) и даже моратория на проверки. Практически количество контрольных мероприятий за последний год снижено более чем на 40%.

На первый взгляд, это противоестественно, ведь ограничениями лимитируется деятельность органов финансового контроля, специально для этого государством созданных. Мы же считаем, что речь идет о перераспределении функций контроля между различными органами, а также о необходимости диверсификации методов его осуществления.

Исторически финансовый контроль формировался в нашей стране как безусловное право некоего органа или должностного лица потребовать объяснений, представив документы; затребовать те или иные доказательства от контролируемого субъекта, обязанности последнего выполнить требования контролера, а также право контролера интерпретировать имеющиеся сведения, давать им экономическую, правовую или политическую оценку и право реализации результатов путем докладов, представлений, обобщений, актов, направляемых в соответствующие органы управления или другие контрольные или следственные органы или непосредственно в суды. При этом публичный интерес всегда превалировал над интересом частным, а взаимоотношения органа контроля и подконтрольного субъекта в той или иной мере строились на *презумпции виновности* подконтрольного.

Сменяющие друг друга исторические эпохи если и изменили эти отношения, то только юридическим «приспособлением» условий работы подконтрольного субъекта под возможные запросы контролера (обязанность вести бухгалтерский учет, хранить денежные средства в кредитных учреждениях, осуществлять учет движения ценностей и др.). Будь то контроль за полнотой платежей в бюджеты различных уровней, слежение за распределением бюджетных ассигнований, совершение государственных расходов, предоставление и возврат кредитов, любые инвестиционные программы, валютные расчеты и даже проверка осуществления финансового контроля — все основывается на *проверке* как ведущей форме финансового контроля, являющейся в конечном счете формой взаимоотношений двух людей или двух групп работников, сторон проверки.

Зададимся теперь вопросом — в чем существо и цель возникновения контрольных правоотношений? Ответ может быть простым и однозначным — в получении *достоверной информации* [12] о деятельности подконтрольного субъекта, а сами контрольные отношения есть не что иное, как *информационные правоотношения*. Посредством этой констатации мы вправе приравнять контроль в целом и финансовый контроль в частности к объектам информационно-правового регулирования, цифровизация которых существенно повышает *достоверность*, *объективность* и *оперативность* получения необходимой информации в целях управления [14], освободить ее сбор и обработку от субъективизма и возможного противодействия ее получения со стороны подконтрольного субъекта, в значительной мере упростить и удешевить как сам процесс контроля, так и порядок реализации данных, полученных путем контроля. Нет сомнения в том, что финансовый контроль, осуществляемый путем получения объективных цифр и алгоритмов, непременно упразднит контроль людей над людьми и их действиями, каким бы объективным и достоверным он (контроль) ни старался быть.

О цифровизации финансового контроля

Цифровизация финансового контроля потребует внедрения новых и обновления применяемых контрольных механизмов. Прежде всего, следовало бы

обратить внимание на *бухгалтерский учет*, «подрастерявший» в условиях рыночной экономики свою публичную направленность и ставший более частноправовым институтом, в том числе в связи с исчезновением отраслевой (министерской) организации бухгалтерского учета.

В условиях цифровизации должен обрести бóльшую мощность *аудит*, понимаемый как инструмент обеспечения интересов собственников (инвесторов) хозяйствующих субъектов, основанных на складочном капитале, прежде всего в акционерных обществах. Каждый инвестор-миноритарий должен быть наделен возможностью беспрепятственного получения актуальной информации по всем интересующим вопросам.

Значительные возможности заложены и в такой форме контроля, как *мониторинг*. Скорее всего, речь должна идти о гармоничном взаимодействии банковского, финансового мониторинга с бухгалтерским учетом в хозяйствующих субъектах и органах с распределительными функциями. Особенно актуален мониторинг в регулировании денежного обращения, валютных операций и искоренения обналичивания и «отмывания» денежных средств.

Статистический учет и отчетность — инструмент управления, возможный только в условиях цифровой реализации, и сейчас он выполняет важные функции. Думается, что статистика может в значительно бóльшей степени, нежели сейчас, использоваться в финансовом контроле, если решить ряд организационных вопросов *доступа к статистической информации* [1].

Нетрудно заметить, что вышеназванные формы финансового контроля носят преимущественно «бесконтактный» характер и осуществляются без использования организационной формы проверки. Конечно же, это не значит, что проверки и, в частности, выездные проверки следует упразднить вообще; проверки будут осуществляться, но преимущественно в виде *комплексных расследований* по наиболее одиозным делам, требующим организационных выводов принципиального характера.

Законодательство о контроле не так давно обогатилось фундаментальным актом — Федеральным Законом № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[7], которым, прежде всего, создана *идеологическая база* контрольной деятельности как особой формы правового регулирования управленческих отношений, в том числе определены исходные начала для перевода финансового контроля на информационно-цифровой метод осуществления.

Нередко под финансовым контролем понимается не только информационная, но и правоохранительная деятельность по реализации данных, полученных в ходе сбора соответствующей информации. Представляется, что эти два вида правовой деятельности следует разграничить как несовпадающие по предмету, но связанные между собой процессуально. Выявленные в ходе контроля факты ждут реагирования в кадровом, организационном или юридическом отношении, в том числе и применения юридической ответственности. Но именно здесь наблюдается явный правовой пробел — либо соответствующие данные не получают должного юридического оформления, либо акт, справка, постановление, сведения в иной форме не вызывают интереса у органов управления, прокуратуры, следствия, т. е. у тех, кто уполномочен на реализацию данных контроля.

В самом широком смысле *проблемы цифровизации* финансового контроля состоят в нахождении адекватных технических средств для формирования гармонизированного юридического механизма, обеспечивающего, с *одной* стороны, допускаемую законом глубину анализа финансовой и хозяйственной информации, характеризующей деятельность подконтрольных субъектов, с *другой* — исключающего дублирование и мелкотемье контроля, вмешательство в ход экономических процессов без необходимости.

Цифровизация финансового контроля — настоятельная необходимость в деле повышения эффективности действия бюджетного механизма, полноты налогообложения, регулирования денежного обращения, деофшоризации национальной экономики и в конечном счете искоренения бесхозяйственности и непроизводительных затрат. Цифровизация также позволит упорядочить и сократить государственные расходы на осуществление самóго финансового контроля, потребляющего ныне значительные публичные денежные ресурсы.

Проблемы осуществления финансового контроля в условиях цифровизации экономических процессов являются предметом острых политических дискуссий и научных исследований. С *одной* стороны, внедрение цифровых технологий позволяет упростить процесс сбора, обработки и хранения информации о финансово-хозяйственной деятельности субъектов финансовых правоотношений, а также обеспечить эффективное взаимодействие контролирующих и подконтрольных субъектов. С *другой* стороны, цифровая трансформация финансовых правоотношений, вызванная структурной перестройкой мировой экономики, приводит к появлению новых проблем в сфере осуществления финансового контроля, которые обусловлены прежде всего отсутствием правового обоснования технологических процессов, что в конечном счете приводит к неправовому разрешению конфликтных ситуаций и, как следствие, к ослаблению роли финансового контроля в регулировании экономики.

Недостаток в правовом регулировании цифровой модели финансового контроля восполняется созданием «*времянок*» *вместо фундаментальных правовых*

[7] Федеральный Закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31. 3 авг. Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

условий» [3, с. 52] , что не позволяет сформировать единообразный подход к регулированию цифровых инструментов и обеспечить полноценный контроль государства за функционированием информационных систем.

Полагаем, что в целях обеспечения резистентности финансовой системы к экономическим кризисам цифровизация финансового контроля, направленная на упрощение взаимодействия контролирующих и подконтрольных субъектов, должна происходить параллельно с разрешением обострившихся в новых экономических реалиях ключевых проблем в сфере государственного управления, а также в области регулирования налогообложения, ценообразования и бюджетного финансирования.

Цифровизация открывает новые возможности для формирования эффективной модели взаимодействия контролирующих и подконтрольных субъектов. Однако отступление от ключевых принципов организации государственного управления способно привести к тому, что инструменты реализации контрольно-надзорной функции превращаются в механизм давления на подконтрольные субъекты. Совпадение государственных функций федеральных органов исполнительной власти, применение контролирующими органами не предусмотренных законом административных процедур приводит к ослаблению гарантий защиты прав участников гражданского оборота. Так, активное использование налоговыми органами не предусмотренных Налоговым Кодексом РФ форм *предпроверочного анализа* привело к развитию негативной практики проведения финансового контроля, проявляющейся в неограниченном усмотрении фискальных органов при осуществлении контрольно-надзорной функции.

Информационные системы, обеспечивающие осуществление финансового контроля, призваны гарантировать финансовую дисциплину и исключить незапланированные правовым актом о бюджете расходы. Однако с помощью внедряемых цифровых технологий невозможно разрешить вопросы оптимизации бюджетных расходов, вызванные отсутствием эффективных правовых инструментов воздействия на экономику и неспособностью соответствующих государственных органов вовремя предотвратить нарушения, препятствующие стабильному экономическому развитию.

В современных экономических условиях складывается ситуация, когда недостатки государственного регулирования экономики компенсируются бюджетным финансированием мероприятий, направленных на предотвращение негативных экономических последствий, вызванных неэффективной денежно-кредитной, фискальной или бюджетной политикой. Об этом свидетельствуют возрастающие объемы бюджетных средств, выделяемых из резервных фондов органов исполнительной власти. По состоянию на 1 января 2021 г. принято 153 решения Правительства РФ о выделении средств резервного фонда Правительства РФ на решение вопросов, связанных с финансовым обеспечением мероприятий, направленных на предотвращение влияния ухудшения экономической ситуации на развитие отраслей экономики, а также с профилактикой и устранением последствий распространения коронавирусной инфекции на территории России. По экспертной оценке Счетной палаты РФ, в соответствии со сводной росписью бюджетные ассигнования на указанные цели выделены в размере 2 855 592,5 млн руб.[8] Очевидно, что применяемый подход в регулировании экономики не нацелен на обеспечение оптимизации бюджетных расходов.

Увеличение разрыва между виртуальной и реальной экономикой обостряет проблемы, связанные с осуществлением финансового контроля за денежным обращением, эмиссией денег, а также за доходами транснациональных компаний. В процессе цифровой трансформации фискальная сфера и область денежной эмиссии оказались наиболее уязвимыми. В условиях активного роста *криптовалютного рынка* [13] во всем мире государства утрачивают контроль над осуществлением денежной эмиссии, опосредованной банковской системой, и принимают комплекс мер, направленных на укрепление денежного суверенитета. Российской Федерацией в рамках обозначенного направления принят Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», в соответствии с которым цифровая валюта не может использоваться в гражданском обороте в качестве законного средства платежа. Кроме того, в государстве происходит процесс создания правовых условий эмиссии *цифрового рубля*, рассматриваемого в качестве непосредственного инструмента контроля за денежным обращением.

Модернизация юридической науки и юридического образования

Оценивая нынешнее состояние юридической науки, можно говорить о многолетнем, продолжающемся застое. И дело не только в ставшем хроническим недофинансировании науки. Какие задачи ставит общество и государство перед наукой? На какие проблемы ориентирует ученых? Можно констатировать, что горизонт задач, которые ставят перед наукой, сводится, по существу, к преодолению мелких трудностей. Серьезная, ориентированная на перспективу наука для этого в принципе не нужна: не зря ведь говорят, что из пушки по воробьям не стреляют.

Между властью и наукой назрел не только интеллектуальный, но и ценностный разрыв. Конституционные положения о том, что власть принадлежит народу, а основной обязанностью власти является обеспече-

[8] Оперативный доклад Счетной палаты РФ об исполнении федерального бюджета и бюджетов государственных внебюджетных фондов, январь — декабрь 2020 года. URL: https://ach.gov.ru/ upload/iblock/e37/e371835371389756c2d319de62f0bd12.pdf

ние его прав и свобод, не просто отошли в тень — они вызывают иронию и насмешки ввиду явного отрыва от действительности [2, с. 84]. Конкретный пример — российская пенсионная реформа. В 90-е годы действовавшая в тот период пенсионная система, построенная на принципе солидарности поколений, была подвергнута уничтожающей критике. Правительство потратило массу сил и средств, чтобы убедить граждан в необходимости перехода к накопительной пенсионной системе, построенной на принципе: «Каждый — сам кузнец своего счастья». Но в последние годы и эта система подвергается масштабной ревизии. Правительство целенаправленно ее разрушает: ликвидированы практически все независимые пенсионные фонды, в том числе вполне успешные. У них под разными предлогами отозваны лицензии, а пенсионные накопления переданы в Пенсионный фонд России. Повышен возраст выхода на пенсию. Заморожена индексация пенсий работающим пенсионерам.

Сегодня мир переживает бурный всплеск научно-технической революции. Едва ли не еженедельно сообщается о новых изобретениях, информационных технологиях, средствах коммуникации. Складывается впечатление, что российская юридическая наука выпала из этого процесса. Разрушена система целеполагания в науке: в плане фундаментальных исследований она практически перешла на самозаказ. Архаичный уровень внутринаучного диалога не позволяет понять, где и что происходит. Нет никакой информации о состоянии самой юридической науки и ее результативности. В сфере «официальной» науки практически не используются новые современные формы научной коммуникации и коллективной мыследеятельности. Управление наукой завязло в ведомственном бюрократизме. Отсутствие видимых признаков прогресса в науке создает предпосылки для застоя в юридической практике, в том числе — в практике юридического образования.

Все позитивные и негативные процессы, происходящие в стране и в мире, так или иначе, затрагивают сферу образования. Многие социальные инновации зарождаются именно в сфере образования и уже оттуда на плечах выпускников и молодых специалистов переносятся в практику. Можно сказать, что сфера образования — это область жизни, в которой создается будущее страны. С высокой степенью вероятности в сфере юридического образования можно прогнозировать следующие изменения:

1. Сократится потребность в «юридических бухгалтерах», т. е. юристах, специализирующихся на простейших юридических операциях — выдаче справок, удостоверений, оформлении типовых договоров и др. Реинжиниринг правовых отношений и переход на безбумажные технологии приведет к массовому сокращению прежде всего этой категории специалистов.

2. Вырастет потребность в «стратегических юристах», «юристах-аналитиках», способных формировать правовую политику, прогнозировать развитие научно-технического прогресса, помогать внедрению инноваций, защищать интеллектуальные права, приспосабливать правовые формы к меняющимся общественным отношениям, находить решения новых и нестандартных социально-правовых ситуаций.

3. Сохранят ценность специалисты, имеющие два образования: юридическое и техническое (или медицинское, фармацевтическое, спортивное и др.). Наличие второго образования позволяет юристу владеть отраслевой терминологией, понимать корни возникающих проблем и объясняться с отраслевыми специалистами на их языке. Разумеется, юрист с подобным набором квалификаций всегда будет востребован в своей сфере деятельности.

Вместе с тем существует немало препятствий и трудностей, которые мешают развитию образования в России. Так, множество проблем в этой сфере создал поспешный, плохо продуманный и неподготовленный переход на Болонскую систему образования. Он состоялся в рамках господствующей парадигмы: *«На Западе — все хорошо и замечательно, у нас — одни ошибки и недостатки»*. Данная парадигма, на наш взгляд, представляет собой уродливую деформацию сознания, открытое признание собственной интеллектуальной несостоятельности. Каковы, с нашей точки зрения, конкретные проблемы юридического образования, препятствующие модернизации юридического образования?

Качественное образование основывается, как правило, на жесткой диктатуре компетентности. Слово «компетентность» здесь ключевое. Это должна быть настоящая, завоеванная многолетним трудом и признанная научным сообществом компетентность, а не пестрая экспозиция дипломов на стене служебного кабинета.

4. Независимо от сферы деятельности и специализации, необходимо готовить юристов к работе в постоянно меняющейся информационной среде. Компьютерная и информационная грамотность в необходимом объеме должны стать обязательным и неизменным требованием к выпускнику юридического вуза. Это относится и к преподавателям, которые должны объяснять студентам свои предметы не на пальцах и даже не на грифельных досках, а изначально при помощи используемых на практике компьютерных программ и технологий. Сегодня же часто можно наблюдать, как не преподаватель студенту, а студент объясняет преподавателю, как преодолеть компьютерный сбой или запустить ту или иную программу.

5. Новая модель образования не должна приводить к искусственному навязыванию преподавателям «модных» форм и методов обучения, например, «перевернутых классов», онлайн-курсов и др. Ведь речь идет об очень тонкой сфере личного творчества. Надо осторожно стимулировать преподавателя к поиску оптимальной модели преподавания, органичной именно для него и его научной дисциплины. Вместо этого на преподавателей часто «давят», заставляют их использовать незрелые, методически слабо прорабо-

танные, но «модные» методы и технологии, которые во многих случаях не дают ожидаемого эффекта.

6. Следует в целом поддержать использование в сфере образования «проектных» форм обучения, когда студенты не только получают предметные знания, но и тут же, в условиях вуза, пытаются практически использовать их, разрабатывая общественно значимые, а иногда и востребованные на рынке, экономически успешные проекты. Только не надо стричь всех под одну гребенку. В юриспруденции, в отличие, скажем, от инженерного или художественного творчества, *проектный подход* менее развит и требует разработки своих, особых форм. В противном случае работа над проектами, ныне активно насаждаемая на юридических факультетах, может легко превратиться в их профанацию.

Преодоление устаревших, консервативных, бюрократических форм управления образованием и его реальный разворот к актуальным проблемам национального развития должны остановить его деградацию, продолжающуюся в нашей стране уже несколько десятилетий.

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. Андрюшечкина И. Н. Правовое регулирование доступа к статистической информации о деятельности судов общей юрисдикции // Российское правосудие. 2008. № 11(31). С. 89—98.
2. Бабурин С. Н. Нравственное государство. Русский взгляд на ценности конституционализма. М. : Норма, 2023. 536 с.
3. Бачило И. Л. Государство и право в XXI в. Реальное и виртуальное. М. : Юркомпани, 2012. 280 с.
4. Варламова Н. В. Цифровые права — новое поколение человека // Труды государства и права РАН. 2019. № 14(4). С. 141—145.
5. Габов А. В., Хаванова И. А. Эволюция роботов и право XXI в. // Вестник Томского гос. ун-та. 2018. № 435. С. 215–233.
6. Ершов В. В. Правовое и индивидуальное регулирование общественных отношений : монография. М. : РГУП, 2018. 628 с.
7. Ершов В. В., Ловцов Д. А. Информационное право — базовая дисциплина специальности «Прикладная информатика в юриспруденции» // Информационное право. 2006. № 3. С. 34—38.
8. Залоило М. В., Пашенцев Д. А. Национальный правопорядок России в условиях цифровизации // Вестник СПбГУ. Сер. 14. Право. 2019. Т. 10. № 2. С. 196—209.
9. Зубарев С. М. Система контроля в сфере государственного управления. М. : Норма, 2019. 152 с.
10. Исаков В. Б. Цифровое будущее права: упования и угрозы // Вестник Моск. ун-та им С. Ю. Витте. Сер. 2. Юридические науки. 2019. № 4(22). С. 28—34.
11. Ловцов Д. А. Системология информационного права // Правосудие/Justice. 2022. Т. 4. № 1. С. 41—70. DOI: 10.37399/2686-9241.2022.1.41-70 .
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. Имплементация «цифровых» прав в экономике: информационно-правовые аспекты // Российское правосудие. 2020. № 10. С. 42—53.
14. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
15. Минбалеев А. В. Проблемы регулирования искусственного интеллекта // Вестник Южно-Уральского гос. ун-та. Сер. Право. 2018. Т. 18. № 4. С. 82—87.
16. Наумов В. Б. Право в эпоху цифровой трансформации: в поисках решений // Российское право: Образование. Практика. Наука. 2018. № 6 (108). С. 4—11.
17. Полякова Т. А., Чеботарева А. А. О новом «регуляторном ландшафте» в условиях цифровой трансформации системы права и экономики // Информационное право. 2020. № 2(64). С. 4—8.
18. Синюков В. Н. Системная методология и закономерности правового регулирования // Проблемы системы и систематизации законодательства : сб. ст. / Под ред. В.Б. Исакова и Е.Н. Салыгина. М. : Юриспруденция, 2018. С. 140—155.
19. Федосеев С. В. Информационные и программные аспекты разработки и применения смарт-контрактов // Правовая информатика. 2021. № 3. С. 27–35. DOI: 10.21681/1994-1404-2021-3-27-35 .
20. Ястребов О. А. Искусственный интеллект в правовом пространстве // Вестник РУДН. Сер. Юридические науки. 2018. Т. 22. № 3. С. 315—328.

NEW TOPICAL GROUNDS FOR MODERNISATION IN THE SPHERE OF INFORMATION TECHNOLOGY LAW

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

Vladimir Isakov, *Dr.Sc. (Law), Professor, Honoured Lawyer of the Russian Federation, Researching Professor at the National Research University Higher School of Economics, Moscow, Russian Federation.*
E-mail: visakov@hse.ru

Keywords: *modernisation, digitalisation, information technology law, information legal relations, financial control, information technology law regulation, information reliability, legal technique, systematisation, regulatory instrument, current version.*

Abstract

Purpose of the paper: studying changes in the legal policy brought about by improvements in digital technologies used in the sphere of law-making and law enforcement, public administration and management, and raising the efficiency of financial control.

Methods of study: system analysis, information technology law modelling and historical extrapolation.

Study findings: a justification is given for the requirements to modernisation and digitalisation in the sphere of information technology law and legal regulation of information legal relations in the subject area of financial control, taxation, price setting and budget financing. A rational two-stage procedure for adopting amendments to regulatory instruments is determined. A justification is given for the recommendations addressed to law-making and law enforcement bodies concerning the practical implementation of tendencies of the revolution in the sphere of information technology and digitalisation of managerial, controlling and jurisdictional activities as well as in the field of legal education and legal theory.

References

1. Andriushechkina I. N. Pravovoe regulirovanie dostupa k statisticheskoi informatsii o deiatel'nosti sudov obshchei iurisdiktsii. Rossiiskoe pravosudie, 2008, No. 11(31), pp. 89–98.
2. Baburin S. N. Nravstvennoe gosudarstvo. Russkii vzgliad na tsennosti konstitutsionalizma. M. : Norma, 2023. 536 pp.
3. Bachilo I. L. Gosudarstvo i pravo v XXI v. Real'noe i virtual'noe. M. : Iurkompani, 2012. 280 pp.
4. Varlamova N. V. Tsifrovye prava – novoe pokolenie cheloveka. Trudy gosudarstva i prava RAN, 2019, No. 14(4), pp. 141–145.
5. Gabov A. V., Khavanova I. A. Evoliutsiia robotov i pravo XXI v. Vestnik Tomskogo gos. un-ta, 2018, No. 435, pp. 215–233.
6. Ershov V. V. Pravovoe i individual'noe regulirovanie obshchestvennykh otnoshenii : monografiia. M. : RGUP, 2018. 628 pp.
7. Ershov V. V., Lovtsov D. A. Informatsionnoe pravo – bazovaia distsiplina spetsial'nosti "Prikladnaia informatika v iurisprudentsii". Informatsionnoe pravo, 2006, No. 3, pp. 34–38.
8. Zaloilo M. V., Pashentsev D. A. Natsional'nyi pravoporiadok Rossii v usloviiakh tsifrovizatsii. Vestnik SPbGU, ser. 14. Pravo, 2019, t. 10, No. 2, pp. 196–209.
9. Zubarev S. M. Sistema kontrolia v sfere gosudarstvennogo upravleniia. M. : Norma, 2019. 152 pp.
10. Isakov V. B. Tsifrovoe budushchee prava: upovaniia i ugrozy. Vestnik Mosk. un-ta im S.Iu. Vitte, ser. 2. Iuridicheskie nauki, 2019, No. 4(22), pp. 28–34.
11. 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 .
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. Implementatsiia "tsifrovykh" prav v ekonomike: informatsionno-pravovye aspekty. Rossiiskoe pravosudie, 2020, No. 10, pp. 42–53.
14. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
15. Minbaleev A. V. Problemy regulirovaniia iskusstvennogo intellekta. Vestnik Iuzhno-Ural'skogo gos. un-ta, ser. Pravo, 2018, t. 18, No. 4, pp. 82–87.

16. Naumov V. B. Pravo v epokhu tsifrovoi transformatsii: v poiskakh reshenii. Rossiiskoe pravo: Obrazovanie. Praktika. Nauka, 2018, No. 6 (108), pp. 4–11.
17. Poliakova T. A., Chebotareva A. A. O novom "reguliatornom landshafte" v usloviiakh tsifrovoi transformatsii sistemy prava i ekonomiki. Informatsionnoe pravo, 2020, No. 2(64), pp. 4–8.
18. Siniukov V. N. Sistemnaia metodologiia i zakonomernosti pravovogo regulirovaniia. Problemy sistemy i sistematizatsii zakonodatel'stva : sb. st. Pod red. V.B. Isakova i E. N. Salygina. M. : Iurisprudentsiia, 2018, pp. 140–155.
19. Fedoseev S. V. Informatsionnye i programmnye aspekty razrabotki i primeneniia smart-kontraktov. Pravovaia informatika, 2021, No. 3, pp. 27–35. DOI: 10.21681/1994-1404-2021-3-27-35 .
20. Iastrebov O. A. Iskusstvennyi intellekt v pravovom prostranstve. Vestnik RUDN, ser. Iuridicheskie nauki, 2018, t. 22, No. 3, pp. 315–328.

НОРМАТИВНО-СПРАВОЧНАЯ ИНФОРМАЦИЯ В СУДЕБНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

***Андрюшечкина И.Н.*[1], *Зивенко О.Д.*[2]**

Ключевые слова: *нормативно-справочная информация, автоматизированная информационная система, автоматизированное судебное делопроизводство, информационное обеспечение, судебная информация, аналитическая информация, централизованные справочники, программные изделия, информационная совместимость, требования, ГАС РФ «Правосудие».*

Аннотация

Цель работы: исследование структуры и содержания нормативно-справочной информации в судебных автоматизированных информационных системах с целью поддержания эффективности информационного обеспечения.

Методы: системный анализ, прагматическая классификация и продуктивная кластеризация; экспертное оценивание.

Результаты: исследованы вопросы нормативно-правого регулирования ведения нормативно-справочной информации, используемой в специальном программном обеспечении (программных изделиях), входящих в состав ГАС РФ «Правосудие» и иных автоматизированных информационных систем, используемых в судах Российской Федерации; определено условное распределение общесистемных справочников по программным изделиям ГАС РФ «Правосудие»; определены практические задачи и перспективы ведения централизованных справочников в подсистеме «Организационное обеспечение» ГАС РФ «Правосудие»; оценена роль нормативно-справочной информации в межведомственном взаимодействии автоматизированных информационных систем государственных органов.

DOI: 10.21681/1994-1404-2023-1-15-33

Введение

Современная нормативная база, лежащая в основе деятельности судебной системы Российской Федерации, за последние несколько лет претерпела существенные изменения: увеличились как объем анализируемых *учетных* и *статистических* показателей, так и их значимость для *системного анализа* [10] судебной практики и принятия управленческий решений в сфере законопроектной деятельности. Возросли *требования* к открытости правосудия и доступности для граждан сервисов судебной системы, межведомственному взаимодействию судов с федеральными и региональными органами государственной власти и управления. Современные и перспективные информационные технологии требуют постоянной адаптации программных изделий ГАС РФ «Правосудие»[3] к уровню мировой IT-индустрии.

[3] Государственная автоматизированная система Российской Федерации (ГАС РФ) «Правосудие» — это территориально распределенная автоматизированная информационная система, предназначенная для формирования единого информационного пространства судов общей юрисдикции и системы Судебного департамента при Верховном Суде РФ (СД), обеспечивающая информационную и технологическую поддержку судопроизводства на принципах поддержания требуемого баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации. URL: http://techportal.sudrf.ru/?id=234 . Разработка ГАС РФ «Правосудие» началась в 2004 г., в 2014 г. после упразднения Высшего Арбитражного Суда РФ полномочия организации деятельности федеральных арбитражных судов возлагаются на СД, а вопросы технической поддержки и модификации информационных систем — на Информационно-аналитический центр СД.

[1] ***Андрюшечкина Ирина Николаевна,*** *кандидат юридических наук, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, начальник отдела организационно-методического обеспечения ведения судебной статистики Главного управления организационного обеспечения деятельности судов Судебного департамента при Верховном Суде Российской Федерации, Российская Федерация, г. Москва.*

E-mail: andr-home2008@yandex.ru

[2] ***Зивенко Олег Дмитриевич,*** *кандидат технических наук, старший научный сотрудник, директор проектов ООО «Итерион» — головной исполнитель работ по модификации и техническому сопровождения программных изделий ГАС РФ «Правосудие», Российская Федерация, г. Москва.*

E-mail: zivenko@mail.ru

Согласно ГОСТ Р 59853-2021[4], *нормативно-справочная информация* (НСИ) представляет собой информацию, заимствованную из нормативных документов и *справочников* и используемую при функционировании *автоматизированных информационных систем* (АИС). НСИ является основой для интеграции *информационного обеспечения* ГАС РФ «Правосудие».

Справочники используются программными изделиями (ПИ) ГАС РФ «Правосудие», обеспечивающими, в частности, процессы судебного делопроизводства, сбора и обработки судебной и ведомственной статистики, ведения кадровой информации и финансово-хозяйственной деятельности в судебной системе Российской Федерации.

Справочники используются в АИС в качестве реквизитов учетных показателей и, как следствие, служат основным средством формализации основных характеристик, контроля ключевых показателей в процессе ввода данных в учетные системы судебного делопроизводства и последующего их анализа, поддержки задач судопроизводства [1, 14]. НСИ обеспечивает возможность работы с консолидированной судебной информацией на федеральном уровне, формируемой как из специального программного обеспечения (СПО), выполняющего целевые и функциональные задачи в системе ГАС РФ «Правосудие», так и СПО различных разработчиков, выполняющих те же задачи, эксплуатируемые в судах разного уровня или различающиеся в судах по субъектам Российской Федерации, а также является основой взаимодействия АИС правоохранительных и других государственных органов[5]. НСИ является основой для формализации *нормативной* и *терминологической* базы. По своей сути и сложившейся практике эксплуатации ГАС РФ «Правосудие» она является основной областью применения *системы классификации и кодирования информации*[6] (СККИ) [3, 4] в данном проекте. СККИ строится с учетом требований общероссийских нормативных документов и нормативных документов, регламентирующих разработку компонентов АИС в системе судебных органов РФ. НСИ состоит из совокупности взаимоувязанных классификаторов информации, справочников, нормативных и методических документов по их разработке, внедрению, ведению, совершенствованию и контролю за использованием.

Роль и место нормативно-справочной информации в составе информационного обеспечения

Информационное обеспечение (ИО)[7] ГАС РФ «Правосудие» представляет собой совокупность форм документов, классификаторов и справочников на основе СККИ, нормативной базы, содержащей конструкторские и эксплуатационные документы в части формирования ИО, нормативные документы предметной области, подлежащей автоматизации, а также реализованных решений по объемам, размещению и формам существования структурированной информации, ведение которой осуществляется с помощью выбранных систем управления базами данных (СУБД) и других программных средств [6—8]. В проектной и конструкторской документации[8] определено, что ИО ГАС РФ «Правосудие» предназначено для удовлетворения информационных потребностей должностных лиц судов общей юрисдикции и органов Судебного департамента при Верховном Суде РФ (СД) при выполнении возложенных на них функциональных задач, а также для обеспечения информационной совместимости функциональных подсистем[9] (ФПС) и *комплексов средств автоматизации* (КСА) между собой и с внешними взаимодействующими и вышестоящими АИС[10].

Под *информационными потребностями* должностных лиц судов общей юрисдикции и органов СД понимается совокупность информационных ресурсов и данных (информация в различных формах существования, проявления и представления [6—8]), которые используются должностными лицами при выполнении своих функциональных обязанностей, в том числе с использованием КСА. При этом информация должна быть доступна конкретному должностному лицу *непосредственно* (например, в виде распечатки или экранной формы документа, отчета, аналитической справки, схемы, карты и др.) или *опосредованно* (например, в виде значения классификационного кода характеристики

[4] ГОСТ Р 59853-2021. Автоматизированные системы. Термины и определения. М., 2022.

[5] В судебной системе эксплуатируется несколько программных средств и АИС судебного делопроизводства: программное изделие (ПИ) «Судебное делопроизводство» («СДП») для федеральных судов и ПИ «АМИРС» для мировых судей, включенные в состав подсистемы «Судебное делопроизводство и статистика» ГАС РФ «Правосудие», программный комплекс (ПК) «Мировые судьи» и АИС «Правосудие» в г. Москве, государственная информационная система Санкт-Петербурга «Автоматизация деятельности судебных участков мировых судей Санкт-Петербурга», ПК «Мировые судьи» Оренбургской области, ПК «Судебно-арбитражное делопроизводство» («САД»), АИС «Судопроизводство» в арбитражных судах.

[6] Разработка НСИ осуществляется в соответствии с требованиями основных положений единой системы классификации и кодирования информации (ЕСКК) технико-экономической и социальной информации и унифицированных систем документации (Постановление Правительства Российской Федерации № 1212 от 01.11.1999). Система классификации и кодирования информации ГАС «Правосудие» соответствует требованиям ГОСТ 6.10.1-88, ГОСТ 6.10.4-84, ГОСТ 6.10.5-87, ПР 50.1.019-2000, ПР 50.1.020-2000, ПР 50.1.021-2000.

[7] ГОСТ Р 59853-2021. Автоматизированные системы. Термины и определения. М., 2022.

[8] ИРЦВ.42 5500 9.077.П5. Описание информационного обеспечения ГАС РФ «Правосудие».

[9] В ГАС РФ «Правосудие» содержатся подсистемы функционального и технологического характера, в состав которых включаются программные изделия.

[10] Например, информационный обмен между подсистемами «Организационное обеспечение» и «Судебное делопроизводство и статистика», «Банк судебных решений» «Кадры», информационный обмен сведениями о рассматриваемых делах между судами различных судебных инстанций. К внешним по отношению к ГАС РФ «Правосудие» можно отнести АИС Верховного Суда РФ, федеральных арбитражных судов, Генеральной прокуратуры, МВД России, ФНС России и др., с которыми осуществляется информационный обмен, связанный с реализацией правосудия судами.

объекта, значения справочника учетного показателя и др.), в зависимости от функциональных обязанностей и уровня доступа пользователя.

Под *информационной совместимостью* ФПС и КСА понимается возможность использовать при переработке информации данные, получаемые от взаимодействующих элементов системы и внешних источников данных. *Проблему* обеспечения информационной совместимости ФПС и КСА следует рассматривать в контексте обеспечения их *эффективного* информационного взаимодействия на основе интеграции информационных ресурсов судов общей юрисдикции и органов СД, НСИ, формируемой с использованием единой СККИ, *унифицированной системы документов*, единых методов формализации текстов (данных), единой системы словарей и языковых средств взаимодействия пользователей с КСА.

В составе ГАС РФ «Правосудие» информационное обеспечение реализуется в виде информационных баз (баз данных, массивов информации [6]), содержащих данные оперативного характера, и НСИ в интересах пользователей и обеспечения взаимодействия с другими АИС; унифицированных форм документов и классификаторов. Возможность работы с ИО в системе реализуется средствами технического и программного обеспечения (ПО) на основе решений по лингвистическому и правовому обеспечению [6].

При разработке ИО учтены следующие организационно-методические *принципы*: методическое единство ИО; системность и информационная совместимость подсистем и компонентов ИО; унификация и структуризация форм обмена информацией; интеграция обработки информации [6].

Разработка и использование НСИ в ГАС РФ «Правосудие» реализуются в создании классификаторов информации, справочников информации и унифицированных форм документов (отчетных форм по справочникам).

Общими *принципами* функционирования НСИ и ведения работ, связанных с развитием ГАС РФ «Правосудие», являются:

- учет изменений в законодательстве, регулирующем организацию судебной деятельности и осуществление правосудия;
- открытость и общедоступность НСИ для должностных лиц судов общей юрисдикции и органов СД с учетом степени *конфиденциальности* [9] информации;
- автоматизация процесса переработки информации;
- обеспечение методического и организационного единства НСИ;
- комплексность НСИ, предусматривающая наиболее полный охват информации, используемой при взаимодействии между ФПС и КСА;
- постоянная актуализация информации;
- обязательность применения НСИ при разработке новых задач, ФПС и информационных ресурсов системы;
- совместимость НСИ, АИС и ресурсов ГАС РФ «Правосудие» с АИС государственных органов, с которыми осуществляется информационный обмен.

Основными *задачами* НСИ являются:

- упорядочение, унификация, классификация и кодирование информации, циркулирующей и перерабатываемой в ГАС РФ «Правосудие»;
- обеспечение информационной совместимости функциональных подсистем \ГАС РФ «Правосудие», а также взаимодействующих АИС государственного управления;
- обеспечение методического и организационного единства в области разработки, внедрения, применения, ведения и совершенствования классификаторов информации ГАС РФ «Правосудие»;
- обеспечение возможности компактного хранения, автоматизированного поиска и обобщения информации;
- обеспечение однозначности и сопоставимости циркулирующей в ГАС РФ «Правосудие» информации;
- создание условий для формирования *единого информационного пространства* в системе судебных органов [11, 12].

В классификаторах и справочниках НСИ представляется упорядоченная совокупность унифицированных наименований единичных и агрегированных позиций (группировок), характеризующих различные аспекты судебной деятельности и обеспечения деятельности судов в системе СД. Унификация наименований в классификаторах обеспечивается за счет устранения синонимии и омонимии в процессе их разработки и устанавливается правилами по стандартизации[11], а также ведомственными нормативами в соответствии с категорией классификатора или справочника.

В состав НСИ ГАС РФ «Правосудие» включены следующие категории классификаторов информации: общероссийские классификаторы, общесистемные классификаторы и справочники, локальные справочники программных изделий.

Подсистема «Организационное обеспечение», включающая программное изделие «Организационное обеспечение» (ПИ «ОО»), предназначена для создания, ведения и распространения НСИ в целях поддержания информационной совместимости и технологического единства информационных потоков судов и системы СД.

В рамках мероприятий по разработке ПИ «ОО» были сформированы документы, регламентирующие порядок создания, совершенствования, ведения и применения классификаторов, форм документов, а также определяющие средства их ведения. К ним относятся:

[11] ПР 50.1.019-2000. Основные положения Единой системы классификации и кодирования технико-экономической и социальной информации и унифицированной системы документации в Российской Федерации. М., 2000; ПР 50.1.020-2000. Порядок разработки общероссийских классификаторов. М., 2000.; ПР 50.1.021-2000. Положение о ведении общероссийских классификаторов на базе информационно-вычислительной сети Госкомстата России. М., 2000.

описание СККИ, применяемой для построения НСИ; описание применения ПИ «ОО» и руководство пользователя ПИ «ОО».

Автоматизированная система ведения НСИ в ПИ «ОО» обеспечивает поддержание в актуальном состоянии используемых в системе общесистемных классификаторов и справочников[12] и выполняет следующие *функции*:

- создание и поддержка в актуальном состоянии *эталонных* (контрольных) и *рабочих* экземпляров и архивов классификаторов;
- формирование классификаторов (их фрагментов, разделов) для баз данных ФПС;
- ведение учета пользователей системы ведения НСИ;
- автоматизированная и ручная загрузка используемых в системе классификаторов (*автоматизированная* загрузка предполагает формирование классификаторов с информационных носителей и по каналам связи, а *ручная* — ввод информации с клавиатуры), а также конвертирование информации из существующих информационных ресурсов государственных, в том числе правоохранительных органов, от судов общей юрисдикции и органов СД (в части оперативной актуализации информационно-адресной информации)[13];
- автоматизированная и ручная актуализация классификаторов в базах данных системы;
- поиск объектов классификации по различным задаваемым условиям (по кодам, наименованиям, контекстным включениям и др.);
- формирование и выдача информации по классификаторам и справочникам (в целом, фрагменты, описательные части) в виде отчетов в текстовом и табличных форматах на внешних информационных носителях, отчетов на устройства отображения и печати — отчеты, аналитические справки, средства цветового контроля;
- формирование и выдача классификаторов и справочников в машиночитаемом формате (*.xml*) для использования в АИС, применяющих справочники в учетных показателях.

Организация ведения справочников и классификаторов

Создание и поддержание в актуальном состоянии эталонов общесистемных классификаторов и справочников, сопровождающих их нормативных и методических документов осуществляются в рамках подсистемы «Организационное обеспечение» (с применением ПИ «ОО») должностными лицами профильного подразделения информационно-аналитического центра (ИАЦ) поддержки ГАС РФ «Правосудие» в соответствии с предусмотренными Уставом центра видами деятельности[14] и с учетом «закрепления» справочников за структурными подразделениями[15].

В данной подсистеме обеспечивается *централизованное ведение и распространение* на все КСА следующих категорий классификаторов и справочников: фрагментов общероссийских классификаторов, используемых в ГАС РФ «Правосудие», и общесистемных справочников (используемых более чем в одной подсистеме). При этом на все КСА поставляются единые информационные и программные средства по работе с НСИ, включая функции, реализующие обмен данными.

Следует заметить, что локальные справочники (ЛС), используемые только в одной подсистеме, сопровождаются информационными и программными средствами использующих их подсистем[16]. При необходимости, в случае невозможности напрямую использовать термины общесистемных справочников (ОСС) осуществляется сопряжение (*гармонизация*) терминов ОСС и ЛС. Например, общесистемный справочник 9200 «Категории гражданских и административных дел» по содержанию связан с локальным справочником категорий дел ПИ «СДП». Для реализации связей между соответствующими терминами формируются перекодировочные таблицы (*рис. 1*).

В общем случае процесс гармонизации реализуется как функционал F изоморфного преобразования множества M терминов общесистемного справочника (классификатора) в множество L терминов локального представления:

$$F\{M(m_1,\dots,m_i,\dots.,m_n)\} \Rightarrow \\ \Rightarrow L(l_1,\dots,l_i,\dots.,l_n),\ \ i=1,\dots,n, \qquad (1)$$

где n — количество терминов общесистемного и локального представления (например, категория «О восстановлении в родительских правах», код 13001003, соответствует локальному представлению с кодом 016Г).

[12] В ПИ «ОО» предусмотрено ведение НСИ, используемой в более чем одном программном изделии ГАС РФ «Правосудие».

[13] От управлений СД в субъектах Российской Федерации поступают сведения о создании судебных участков мировых судей, их адресах.

[14] Приказ Судебного департамента при Верховном Суде РФ от 12 июля 2018 г. № 113 (ред. от 13.08.2021) «Об утверждении Устава федерального государственного бюджетного учреждения «Информационно-аналитический центр поддержки ГАС РФ «Правосудие».

[15] В соответствии с Приказом Судебного департамента от 14 мая 2015 г. № 125 «Об организации эксплуатации, сопровождения и развития Государственной автоматизированной системы Российской Федерации «Правосудие» и автоматизированных систем федеральных арбитражных судов», Приложение № 3. Перечень общесистемных классификаторов подсистемы «Организационное обеспечение «ГАС РФ «Правосудие», закрепленных за структурными подразделениями Судебного департамента при Верховном Суде РФ.

[16] Например, локальными являются справочники пользователей ПИ СДП в конкретном суде. Справочники, содержащие характеристики объектов недвижимости, ведутся непосредственно в ПИ «Недвижимость». Бóльшая часть справочников учетных показателей судебного делопроизводства в настоящее время ведется непосредственно в автоматизированных системах разработчиками соответствующего СПО.

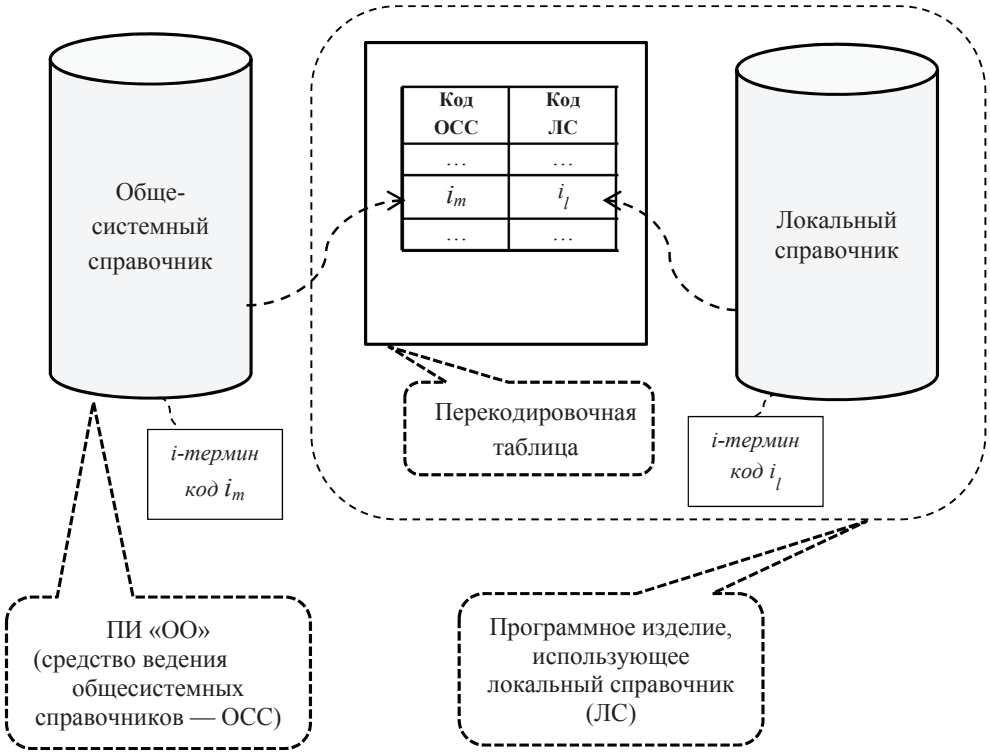

Рис. 1. Использование перекодировочных таблиц для гармонизации терминов общесистемного и локального справочников

Для реализации более сложных (неизоморфных) связей, если количество терминов n общесистемного представления не равно количеству терминов k локального представления, необходима разработка специального алгоритма $A\{M_s\} \Rightarrow L_s$ на стороне локального приложения — преобразования подмножества $M_s \in M$ множества M в подмножество $L_s \in L$ множества L для получения количества k терминов локального представления:

$$F\{M(m_1, \dots, m_i, \dots., m_n)\} \Rightarrow \quad (2)$$
$$\Rightarrow L(l_1, \dots, l_j, \dots., l_k), j = 1, \dots, k, i = 1, \dots, n;$$

$$F\{M(m_1, \dots, A\{M_s\}, \dots., m_n)\} \Rightarrow \quad (3)$$
$$\Rightarrow L(l_1, \dots, \{L_s\}, \dots., l_k),$$

где n — количество терминов общесистемного представления, k — количество терминов локального представления, $k \neq n$.

Подсистема «ОО» представляет собой совокупность информационных и программных средств, функционирующих на всех КСА, где предполагается информационное взаимодействие между задачами и подсистемами. Информационные средства ПИ «ОО» содержат условно-постоянную информацию (УПИ)[17] и включают в свой состав общероссийские классификаторы, общесистемные справочники ГАС, а также необходимую для функционирования системы иную нормативно-справочную информацию. Программные средства ПИ «ОО» обеспечивают создание, ведение и распространение УПИ на КСА и устанавливаются в полном объеме на рабочих местах всех КСА, где представлен фонд УПИ.

Для обеспечения *достоверности* [6] и *сопоставимости* классификаторов, входящих в состав НСИ, общероссийские и общесистемные классификаторы распространяются централизованно из ИАЦ СД, а техническая поддержка на КСА осуществляется работниками филиалов ИАЦ. Общероссийские классификаторы централизованно поставляются в ПИ «ОО» в порядке, установленном Правительством РФ[18], для дальнейшего распространения в ФПС и задачах системы.

Эталоны системных классификаторов, которые используются более чем в одной подсистеме (задаче), учитываются в эталонной базе на основе поступающих из подсистем и КСА заявок на *модификацию* соответствующего классификатора в части адресной информации судебных органов, справочников федеральных судов и судебных участков мировых судей. Актуализация общесистемных справочников, содержащих составы преступлений и правонарушений в статьях кодексов (УК РФ, КоАП РФ) и связанных с ними, влияющих на показатели

[17] Под условно-постоянной информацией понимается информация, которая вводится единожды, сравнительно редко изменяется и многократно используется. Примером такой информации могут служить различные классификаторы, настройки, перечни, реестры, нормативно-справочная информация и др.

[18] См.: Постановление Правительства РФ от 10 ноября 2003 г. № 677 «Об общероссийских классификаторах технико-экономической и социальной информации в социально-экономической области» // СПС «КонсультантПлюс».

судебной статистики[19] [1, 2], осуществляется путем внесения новых записей или редакций на основе норм законов после вступления в силу принятого изменения.

Для достижения однозначности в классификаторах, входящих в состав СККИ, осуществляется взаимоувязка наименований понятий и кодов классификаторов, а также всей совокупности показателей и условно-постоянной информации. При этом классификаторы, используемые в ГАС РФ «Правосудие», имеют различную структуру, формат, алфавит кода, правила написания наименований объектов[20].

Разработка новых классификаторов (справочников) проводится с учетом основных *требований* к системам классификации и кодирования информации, а также к классификаторам [5, 13]. Обоснованные методы классификации обеспечивают: учет особенностей решения и корректное решение конкретных задач функционирования ГАС РФ «Правосудие»; минимальные затраты и трудоемкость ведения классификаторов; информационную совместимость с классификаторами других АИС и др.; однозначную идентификацию объекта (понятия); оптимальную длину кода; защиту от ошибок; возможность автоматизированной переработки информации и др. После разработки проектов новых общесистемных классификаторов выполняется проведение их экспертизы на отсутствие дублирования понятий и терминов в других классификаторах.

При этом предусматривается кодирование наиболее важных свойств (характеристик) объектов, включаемых в общесистемный классификатор. В настоящее время в ГАС РФ «Правосудие» используется 72 общесистемных справочника, включая 5 общероссийских классификаторов[21]. Количественный состав справочников постоянно изменяется в связи с изменениями предметной области. Так, после упразднения межрегиональных центров технической поддержки и передачи в ИАЦ СД и его филиалы полномочий сопровождения ГАС РФ «Правосудие» соответствующий справочник этих организаций выведен из эксплуатации. В связи с межведомственным информационным взаимодействием добавлены справочники организаций ФСИН, правоохранительных органов, предметов исполнения (в исполнительном производстве) и ряд других.

Описание применения программного изделия в ГАС РФ «Правосудие» предоставляет пользователю возможность ознакомится с функционалом ПИ (в данном случае ПИ «ОО»), но не определяет порядок работы с ним. Так и Описание применения ПИ «ОО» не регулирует вопросов организации работы по ведению и распространению НСИ, однако эта работа требует взаимодействия разных организаций и их должностных лиц: ИАЦ СД и его филиалов, СД и управлений СД в субъектах Российской Федерации.

В текущей версии ПИ «ОО», содержащей более 70 справочников, работа ведется работниками ИАЦ во взаимодействии с работниками соответствующих подразделений СД, ответственными лицами Росстата, Генеральной прокуратуры, Федеральной службы судебных приставов и др. Поэтому с учетом задач, решаемых в ГАС РФ «Правосудие» и в целом в судебной системе, необходимо *нормативное* регулирование порядка взаимодействия систем во времени (подсистем и программных изделий, использующих НСИ). Представляется, что таким документом должен быть «Регламент централизованного ведения нормативно-справочной информации Государственной автоматизированной системы Российской Федерации «Правосудие»[22] (далее — Регламент).

Регламент должен определять перечень мероприятий по поддержанию справочников в актуальном состоянии: основания и порядок внесения в них изменений, информирование и распространение потребителям — программным изделиям ГАС РФ «Правосудие» и внешним заинтересованным потребителям[23], формирование «преднастроенных» отчетов по справочникам[24] и предоставление *справочной* и *аналитической* информации на основе содержания справочников[25].

В Регламенте должна быть отражена система классификаторов и справочников, входящих в состав единой системы НСИ, по *источникам* получения сведений (импортируемые и создаваемые) и основаниям внесения изменений в справочник. К *импортируемым* справочникам относятся все общероссийские классификаторы, источником которых является Росстат (поставляются

[19] Андрюшечкина И.Н. Судебная статистика : учеб. пособие. М. : РГУП. 2022. 292 с. ISBN: 978-5-93916-979-0.

[20] В ГАС РФ «Правосудие» используются три типа справочников: линейные (имеющие последовательный классификационный код), иерархические (характеризующие связи типа «часть — целое» и «элемент — класс»; их код состоит из фасетов верхних уровней и текущего уровня), табличные (имеющие уникальные структурные особенности, например, судебные органы имеют признаки как типов, так и территорий).

[21] ПИ «Организационное обеспечение», версия 24.

[22] Проект такого документа в течение последних лет поэтапно разрабатывался ИАЦ СД совместно с подразделениями СД — кураторами справочников, но как нормативный документ не утверждался приказом СД. В Государственном задании ИАЦ на 2023 г. в разделе 2: Информационное обеспечение ведения судопроизводства и делопроизводства предусмотрено в п. 2.9: Организация и осуществление мероприятий по формированию единого информационного пространства федеральных судов и мировых судей, поддержке функционирования и развития «ГАС РФ «Правосудие» описание работ включает актуализацию и разработку регламентирующих документов (проектов документов), в том числе «ведения НСИ ГАС РФ «Правосудие».

[23] Основными востребованными справочниками внешними АИС являются справочники федеральных судов и судебных участков мировых судей, которые используются в качестве учетных реквизитов в сведениях по исполнительному производству в ФССП России и в Генеральной прокуратуре для отражения в учете уголовных дел, направленных на судебное рассмотрение.

[24] Выгрузка данных справочников в шаблоны отчетов текстового или табличного форматов.

[25] Формирование «преднастроенных» аналитических форм для задач судебной статистики: таблицы размеров штрафов по строкам форм отчетности, цветовой раскраски разделов программных шаблонов по подсудности, допустимости видов наказаний и результатов рассмотрения дел на основе справочников УК РФ и КоАП РФ с привязками по категориям и видам наказаний.

на договорных отношениях), а также справочники, ведение и поддержание актуальности которых осуществляются другими органами, но сведения из которых используются в учетных реквизитах судебного делопроизводства (например, справочник 20000 «Правоохранительные органы Генеральной прокуратуры РФ», а также справочники ФССП России: 30000 «Справочник предметов исполнения», 31000 «Виды судебных актов в рамках исполнительного производства», 31110 «Виды исполнительных документов»).

Представляется, что поскольку *требования* Регламента должны быть изложены в систематизированном виде, так как группы справочников имеют взаимосвязанное содержание, то в Регламенте целесообразно использовать таблицы и схемы (в приложениях). Например, значения справочника 7312 «Виды судопроизводства» используются в справочнике 9200 «Категории гражданских и административных дел», который связан со значениями справочника 7314 «Производства по материалам». Категории гражданских и административных дел справочника 9200 привязываются к записям справочника 9223 «Строки статистической отчетности», которые соответственно привязаны к записям справочника 9224 «Формы статистической отчетности». Аналогичная связь есть и у категорий производств по материалам (7314 — 9223 — 9224). Категории гражданских и административных дел привязываются к соответствующим наименованиям строк в разделах как «один к одному» или несколько категорий к одной строке в формах № 2 «Отчет о работе судов общей юрисдикции по рассмотрению гражданских, административных дел по первой инстанции», № 7 «Отчет о работе судов общей юрисдикции по рассмотрению гражданских, административных дел в апелляционном порядке», № S07 «Сведения о рассмотрении судами общей юрисдикции некоторых категорий гражданский дел, административных дел по первой инстанции и дел об административных правонарушениях (приложение к формам № 1-АП, 2)». Категории производств по материалам распределяются в статистических показателях соответствующих форм статистической отчетности по видам судопроизводства: *уголовное* судопроизводство — форма № 1 «Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции»; производство по делам об *административных* правонарушениях — форма № 1-АП «Отчет о работе судов общей юрисдикции по рассмотрению дел об административных правонарушениях» (*табл. 1*).

Кроме того, в табличном представлении справочников целесообразно дать краткое описание справочника и основание его введения. Поля для аналогичных

Таблица 1

Пример использования справочников в формах статистической отчетности

Справочник	Раздел формы	Форма статистической отчетности
9200	2, 3	2
9200	2, 3, 4, 5	S07
7314	4	1
7314	9	2
7314	2	1-АП

сведений необходимо предусмотреть и в ПИ «ОО», поскольку определенные актуальные пометки в программу могут быть внесены до утверждения изменений в Регламенте.

С точки зрения *происхождения* общесистемные справочники (ОСС) можно условно разделить на следующие категории:

- *импортируемые* (общероссийские классификаторы, заимствованные или получаемые из АИС других государственных органов);
- *экспортируемые* (основная группа справочников, предназначенных для классификации и кодирования информации программных изделий ГАС РФ «Правосудие»; данные из справочников могут передаваться во внешние АИС):
- *технологические* (предназначенные для обеспечения функционирования ПИ «ОО»: настройки автоматизированных рабочих мест, список пользователей, функциональные комплексы задач).

Наибольшую долю составляют *экспортируемые* справочники, создаваемые в ПИ «ОО» для выполнения функциональных задач другими подсистемами в программных изделиях ГАС РФ «Правосудие». Так, в табл. 2 фрагментарно представлен пример условного распределения справочников по программным изделиям ГАС РФ «Правосудие». Следует заметить, что при изменении законодательной и нормативной базы, появлении новых функциональных требований к ПИ, вводом в эксплуатацию новых задач указанные справочники могут использоваться также для нового функционала. Таким образом, соотнесение справочников и конкретных программных изделий имеет вариативный характер. Кроме того, ПИ «ОО» как системообразующий компонент ГАС РФ «Правосудие» является средством актуализации основных общесистемных справочников, что представлено в табл. 3.

Таблица 2

Условное распределение общесистемных справочников по программным изделиям ГАС РФ «Правосудие»[26]

Программные изделия и подсистемы, использующие ОСС[27]	**Используемые справочники**
Программные изделия и подсистемы обеспечения судебного процесса	
ПИ «АМИРС» (комплекс программ для обеспечения деятельности судебных участков мировых судей) Подсистема «Судебное делопроизводство и статистика»	1. Перечень привязок категорий составов уголовных преступлений к составам УК РФ 2. Перечень привязок видов уголовных наказаний к составам УК РФ 3. Перечень привязок категорий составов административных правонарушений к составам КоАП РФ 4. Федеральные суды, судейские сообщества, органы системы Судебного департамента 5. Судебные участки мировых судей 6. Кодекс Российской Федерации об административных правонарушениях 7. Производства по материалам 8. Виды административных наказаний 9. Категории составов уголовных преступлений 10. Тип файла приложения 11. Признак преступления 12. Тип периодического взыскания 13. Тип нормативного правового акта 14. Типы документов, удостоверяющих личность физического лица 15. Виды исполнительного документа 16. Тип должника или взыскателя 17. Справочник правоохранительных органов 18. Виды наказаний УК РФ 19. Справочник видов постановлений и иных документов должностных лиц ФССП России 20. Категории дел (гражданское и административное судопроизводство) 21. Категории составов административных правонарушений 22. Уголовный кодекс Российской Федерации 23. Перечень привязок видов административных наказаний к составам КоАП РФ
ПИ «БСР» Подсистема «Банк судебных решений (судебной практики)»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 3. Виды наказаний УК РФ 4. Категории составов уголовных преступлений 5. Виды судебных постановлений (гражданское производство) 6. Виды административных наказаний 7. Виды постановлений и определений по делу об административном правонарушении 8. Категории составов административных правонарушений 9. Этапы судопроизводства (судебные инстанции) 10. Виды судебных постановлений (уголовное производство) 11. Подразделения суда 12. Типы документов 13. Вид судопроизводства 14. Уголовный кодекс Российской Федерации 15. Кодекс Российской Федерации об административных правонарушениях 16. Типы судов и органов Судебного департамента

[26] Наименования подсистем и включаемых в них программных изделий представлены в Схеме деления ГАС «Правосудие». URL: https://techportal.sudrf.ru/?id=373

[27] В состав подсистемы входит одно или несколько программных изделий, выполняющих различные взаимосвязанные или аналогичные функции, но используемые на объектах автоматизации разного уровня.

Программные изделия и подсистемы, использующие ОСС	**Используемые справочники**
ПИ «БИД» (база исполнительных документов) Подсистема «Судебное делопроизводство и статистика»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Виды исполнительного документа 3. Тип нормативного правового акта 4. Признак преступления 5. Справочник видов постановлений и иных документов должностных лиц ФССП России 6. Тип файла приложения 7. Тип периодического взыскания 8. Типы документов, удостоверяющих личность физического лица 9. Справочник предметов исполнения 10. Судебные участки мировых судей 11. Субъекты РФ
ПИ «Присяжные» Подсистема «Судебное делопроизводство и статистика»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «Стакс-центр» Подсистема «Судебная статистика Судебного департамента»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 3. Судебные участки мировых судей
ПИ «СЭ» Подсистема «Судебная экспертиза»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «СДП» (судебное делопроизводство, используемое в федеральных судах общей юрисдикции и ПИ «Судимость») Подсистема «Судебное делопроизводство и статистика»	1. Перечень привязок категорий составов уголовных преступлений к составам УК РФ 2. Перечень привязок видов уголовных наказаний к составам УК РФ 3. Федеральные суды, судейские сообщества, органы системы судебного департамента 4. Виды наказаний УК РФ 5. Категории составов уголовных преступлений 6. Этапы судопроизводства (судебные инстанции) 7. Виды судебных постановлений (уголовное производство) 8. Лица, участвующие в деле 9. Производства по материалам 10. Вид судопроизводства 11. Уголовный кодекс Российской Федерации 12. Кодекс Российской Федерации об административных правонарушениях 13. Типы судов и органов Судебного департамента 14. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 15. Формы статистической отчетности 16. Строки статистической отчетности 17. Категории дел (гражданское и административное судопроизводство) 18. Виды административных наказаний 19. Категории составов административных правонарушений 20. Судебные участки мировых судей 21. Судьи 22. Территориальная юрисдикция судов 23. Перечень привязок видов административных наказаний к составам КоАП РФ 24. Перечень привязок категорий составов административных правонарушений к составам КоАП РФ
Обеспечивающие программные изделия и подсистемы	
ПИ «АУ» Подсистема «Административное управление»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)

Программные изделия и подсистемы, использующие ОСС	**Используемые справочники**
ПИ «АКСА-центр» Подсистема «Ведомственная статистика Судебного департамента»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Судебные участки мировых судей 3. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «Документооборот» Подсистема «Документооборот и обращение граждан»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Типы судов и органов Судебного департамента 3. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 4. Общероссийский классификатор — управленческая документация (ОКУД)
ПИ «ИП», «МС», «СХСА» (обеспечивают работу Интернет-портала — ПИ «ИП», модуля сопряжения с автоматизированными системами судебного делопроизводства — ПИ «МС», системы хранения судебных актов консолидированной базы данных сведений по делам и судебных актов с сайтов судов — ПИ «СХСА») Подсистема «Интернет-портал ГАС РФ «Правосудие»	1. Перечень привязок категорий составов уголовных преступлений к составам УК РФ 2. Перечень привязок категорий составов административных правонарушений к составам КоАП РФ 3. Перечень привязок видов уголовных наказаний к составам УК РФ 4. Территориальная юрисдикция судов 5. Категории составов уголовных преступлений 6. Категории дел (гражданское и административное судопроизводство) 7. Виды административных наказаний 8. Категории составов административных правонарушений 9. Производства по материалам 10. Уголовный кодекс Российской Федерации 11. Кодекс Российской Федерации об административных правонарушениях 12. Типы судов и органов Судебного департамента 13. Субъекты РФ 14. Виды наказаний УК РФ 15. Судебные участки мировых судей 16. Федеральные суды, судейские сообщества, органы системы судебного департамента 17. Территориальная юрисдикция участков мировых судей 18. Перечень привязок видов административных наказаний к составам КоАП РФ
ПИ «ИСС-П» Информационно-справочная подсистема	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Типы судов и органов Судебного департамента 3. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «МТР» Подсистема «Материально-технические ресурсы»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Типы судов и органов Судебного департамента 3. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 4. Товары 5. Единицы измерения 6. Коды бюджетной классификации
ПИ «Недвижимость» Подсистема «Недвижимость»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 3. Коды бюджетной классификации
ПИ «СО», ПИ «СТП» Подсистема «Обеспечение эксплуатации, сервисного обслуживания и технической поддержки»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «ДО» Подсистема «Обучение кадров — дистанционное обучение»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)

Программные изделия и подсистемы, использующие ОСС	**Используемые справочники**
ПИ «ОСв» Подсистема «Общественные связи»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «ИК», ПИ «ИТ». Подсистема «Отображение информации коллективного пользования» (в информационном киоске суда — ПИ «ИК», на информационных табло — ПИ «ИТ»)	1. Перечень привязок категорий составов уголовных преступлений к составам УК РФ 2. Перечень привязок категорий составов административных правонарушений к составам КоАП РФ 3. Перечень привязок видов уголовных наказаний к составам УК РФ 4. Виды наказаний УК РФ 5. Категории составов уголовных преступлений 6. Категории дел (гражданское и административное судопроизводство) 7. Виды административных наказаний 8. Категории составов административных правонарушений 9. Производства по материалам 10. Вид судопроизводства 11. Уголовный кодекс Российской Федерации 12. Кодекс Российской Федерации об административных правонарушениях 13. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 14. Федеральные суды, судейские сообщества, органы системы судебного департамента 15. Территориальная юрисдикция судов 16. Перечень привязок видов административных наказаний к составам КоАП РФ
ПИ «Кадры-П» Подсистема «Кадры»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Субъекты РФ 3. Типы судов и органов Судебного департамента 4. Общероссийский классификатор стран мира (ОКСМ) 5. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 6. Общероссийский классификатор — управленческая документация (ОКУД) 7. Общероссийский классификатор начального профессионального образования (ОКНПО) 8. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов (ОКПДТР) 9. Общероссийский классификатор специальностей по образованию (ОКСО) 10. Судебные участки мировых судей
ПИ «Право-П» Подсистема «Право» (база данных ведомственных нормативных актов Судебного департамента)	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПТК «ВИВ» (программно-технический комплекс для обеспечения внешнего информационного взаимодействия) Подсистема «Организационное обеспечение»	1. Федеральные округа Российской Федерации 2. Федеральные суды, судейские сообщества, органы системы судебного департамента 3. Судебные участки мировых судей 4. Субъекты РФ 5. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов (ОКПДТР) 6. Справочник видов постановлений и иных документов должностных лиц ФССП России 7. Тип файла приложения 8. Признак преступления 9. Тип периодического взыскания 10. Тип нормативного правового акта 11. Типы документов, удостоверяющих личность физического лица 12. Справочник предметов исполнения 13. Подразделения ФССП России 14. Типы судов и органов Судебного департамента 15. Общероссийский классификатор видов экономической деятельности (ОКВЭД) 16. Общероссийский классификатор валют (МКВ)

Программные изделия и подсистемы, использующие ОСС	Используемые справочники
ПИ «СС» Подсистема «Судейское сообщество»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «СКИФ» Подсистема «Управление и контроль Функционирования»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Типы судов и органов Судебного департамента 3. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «КФХД» (контроль финансово-хозяйственной деятельности) Подсистема «Финансовый контроль»	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Типы судов и органов Судебного департамента 3. Общероссийский классификатор объектов административно-территориального деления (ОКАТО)
ПИ «УБС», ПИ «БПФ» Подсистема «Финансы» (учет бюджетных средств — ПИ «УБС», бюджетное планирование и финансирование — ПИ БПФ)	1. Федеральные суды, судейские сообщества, органы системы судебного департамента 2. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 3. Коды бюджетной классификации 4. Общероссийский классификатор видов экономической деятельности (ОКВЭД) 5. Общероссийский классификатор валют (МКВ) 6. Коды бюджетной классификации

Таблица 3

Перечень основных общесистемных справочников, актуализируемых в программном изделии «Организационное обеспечение»

Программные изделия и подсистемы, использующие ОСС[28]	Используемые справочники
ПИ «ОО» Подсистема «Организационное обеспечение»	1. Территориальные Единицы Российской Федерации 2. Федеральные округа Российской Федерации 3. Военно-судебные округа 4. Рода, виды войск и воинских формирований 5. Настройки АРМ 6. Перечень привязок категорий составов уголовных преступлений к составам УК РФ 7. Общероссийский классификатор объектов административно-территориального деления (ОКАТО) 8. Общероссийский классификатор — управленческая документация (ОКУД) 9. Общероссийский классификатор — единицы измерения (ОКЕИ) 10. Общероссийский классификатор начального профессионального образования (ОКНПО) 11. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов (ОКПДТР) 12. Коды бюджетной классификации 13. Товары 14. Номенклатура дел и документов 15. МЦП 16. Судебные участки мировых судей 17. Судьи 18. Федеральные суды, судейские сообщества, органы системы судебного департамента

[28] В состав подсистемы входит одно или несколько программных изделий, выполняющих различные взаимосвязанные или аналогичные функции, но используемые на объектах автоматизации разного уровня.

Программные изделия и подсистемы, использующие ОСС[28]	**Используемые справочники**
ПИ «ОО» Подсистема «Организационное обеспечение»	19. Территориальная юрисдикция участков мировых судей 20. Территориальная юрисдикция судов 21. Подразделения суда 22. Лица, участвующие в деле 23. Производства по материалам 24. Типы документов 25. Вид судопроизводства 26. Уголовный кодекс Российской Федерации 27. Общероссийский классификатор стран мира (ОКСМ) 28. Общероссийский классификатор видов экономической деятельности (ОКВЭД) 29. Общероссийский классификатор валют (МКВ) 30. Общероссийский классификатор специальностей по образованию (ОКСО) 31. Общероссийский классификатор форм собственности (ОКФС) 32. Единицы измерения 33. Функциональные комплексы задач ГАС Правосудие 34. Субъекты РФ 35. Виды собственности 36. Справочник видов постановлений и иных документов должностных лиц ФССП России 37. Тип файла приложения 38. Признак преступления 39. Тип периодического взыскания 40. Тип нормативного правового акта 41. Типы документов, удостоверяющих личность физического лица 42. Виды исполнительного документа 43. Тип должника или взыскателя 44. Виды судебных актов в рамках исполнительного производства 45. Справочник предметов исполнения 46. Справочник правоохранительных органов 47. Виды наказаний УК РФ 48. Категории составов уголовных преступлений 49. Подразделения ФССП России 50. Подразделения ФСИН России 51. Подразделения ГИБДД 52. Подразделения ГП 53. Формы статистической отчетности 54. Строки статистической отчетности 55. Виды судебных постановлений (гражданское производство) 56. Категории дел (гражданское и административное судопроизводство) 57. Виды административных наказаний 58. Виды постановлений и определений по делу об административном правонарушении 59. Категории составов административных правонарушений 60. Перечни категорий судопроизводства 61. Пользователи 62. Этапы судопроизводства (судебные инстанции) 63. Виды судебных постановлений (уголовное производство) 64. Кодекс Российской Федерации об административных правонарушениях 65. Типы судов и органов Судебного департамента 66. Общероссийский классификатор органов государственной власти и управления (ОКОГУ) 67. Перечень привязок видов административных наказаний к составам КоАП РФ 68. Перечень привязок категорий составов административных правонарушений к составам КоАП РФ 69. Перечень привязок видов уголовных наказаний к составам УК РФ 70. Вид (род) войск и воинских формирований 71. Воинские звания

Актуальные справочники автоматизированно обрабатываются АИС-потребителями, для чего выгружаемые сведения в машиночитаемом формате должны иметь дату актуальности справочника. Справочники выгружаются в формат *.xml* в полном объеме.

Примеры решаемых задач автоматизации

Как один из ***примеров*** решаемых задач автоматизации можно рассмотреть реализацию требований в техническом задании (ТЗ) для АИС судебного делопроизводства[29] информационного взаимодействия по передаче сведений в Социальный фонд России (объединил с 01.01.23 Пенсионный фонд и Фонд социального страхования) — сведений по ряду категорий дел, решения по которым являются юридическими основаниями для осуществления различных выплат лицу: о признании лица дееспособным или ограниченно дееспособным и отмене судом таких ограничений, о признании лица умершим или безвестно отсутствующим, отмена решений об этих фактах, лишение или ограничение в родительских правах, восстановление или снятие таких ограничений.

Реализация требования ТЗ на 2022 г. для АИС судебного делопроизводства в федеральных судах (ПИ «СДП») предусматривала отбор дел по требуемым категориям, однако часть категорий, а именно об отмене предыдущий судебных решений, отсутствовала в качестве строк-показателей в статистической отчетности и не выделялась в первичном учете при выборе категорий гражданских дел из справочника 9200 «Категории гражданских и административных дел». Соответственно, выполнение задачи потребовало добавления в справочник 9200 новых категорий по видам сведений, которые надо передать другому органу.

Классификатор гражданских и административных дел представляет собой *иерархический* справочник. Выделяемые категории относились к делам из семейных правоотношений, связанных с воспитанием детей (об отмене ограничения родительских прав), и к делам особого производства (об отмене решения признании умершим, безвестно отсутствующим, недееспособным, о снятии ограничений в дееспособности).

Выделяемые категории необходимо включить в новый узел иерархии «Споры, связанные с воспитанием детей», а имеющуюся одноименную категорию, куда и входили дела, относящиеся к выделяемым категориям, перевести в ретро-запись с датой окончания действия 31.12.23, создав запись «Иные семейные споры, связанные с воспитанием детей» и новые вышеуказанные категории с 01.01.24. В этот узел также перейдут уже имеющиеся категории семейных дел, имеющиеся в справочнике, а также вновь выделенные, относимые в Постановлении Пленума Верховного Суда РФ[30] к группе «семейные споры, связанные с воспитанием детей».

В связи со включением категорий в классификатор и необходимости контроля в дальнейшем для информационного обмена указанные категории выделены в проектах форм статистической отчетности о рассмотрении гражданских и административных дел по первой и апелляционной инстанциям (форма № 2 и 7) на 2024 г. (*рис. 2*).

В настройке статистических показателей строк статистической отчетности (форма № 2 и 7) часть ранее введенных категорий из узла «Споры, связанные с воспитанием детей» будет привязана к одноименным значениям в строках статистической отчетности (например, о лишении родительских прав), и в строку-группировку «Иные споры, связанные с воспитанием детей» войдут все остальные выделенные споры и категория «Иные семейные споры, связанные с воспитанием детей».

Аналогичные изменения — в справочнике 9200 для гражданских дел особого производства, в которых из категории «иные дела особого производства» нужно выделить дела особого производства по отмене ранее вынесенных судебных решений: об отмене решения о признании безвестно отсутствующим или об объявлении умершим[31] (ст. 280 ГПК РФ), отмене ограничения гражданина в дееспособности и признание гражданина дееспособным (ст. 286 ГПК РФ) и добавить категорию «Прочие дела особого производства», если по харак-

[29] Требования применительно к подсудности гражданских дел относились к ПИ «СДП».

[30] В узел (группу) включаются все категории, перечисленные в Постановлении Пленума Верховного Суда РФ от 27 мая 1998 г. № 10 (ред. от 26.12.2017) «О применении судами законодательства при разрешении споров, связанных с воспитанием детей». К спорам, связанным с воспитанием детей, относятся: споры о месте жительства ребенка при раздельном проживании родителей (п. 3 ст. 65 СК РФ); об осуществлении родительских прав родителем, проживающим отдельно от ребенка (п. 2 ст. 66 СК РФ); об устранении препятствий к общению с ребенком его близких родственников (п. 3 ст. 67 СК РФ); о возврате родителям ребенка, удерживаемого не на основании закона или судебного решения (п. 1 ст. 68 СК РФ); о возврате опекунам (попечителям) подопечного от любых лиц, удерживающих у себя ребенка без законных оснований (п. 2 ст. 150 СК РФ); о возврате приемному родителю ребенка, удерживаемого другими лицами не на основании закона или судебного решения (п. 3 ст. 153 СК РФ); о лишении родительских прав (п. 1 ст. 70 СК РФ); о восстановлении в родительских правах (п. 2 ст. 72 СК РФ); об ограничении родительских прав (п. 1 ст. 73 СК РФ); об отмене ограничения родительских прав (ст. 76 СК РФ) и др. Поскольку в п. 1 указанного Постановления Пленума ст. 77 Семейного Кодекса (СК) РФ непосредственно не перечислена, но есть оговорка «и другие», считаем, что ее можно отнести в группу «Споры, связанные с воспитанием детей».

[31] В случае явки или обнаружения места пребывания гражданина, признанного безвестно отсутствующим или объявленного умершим, суд новым решением отменяет свое ранее принятое решение. Соответственно, новое решение суда является основанием для отмены управления имуществом гражданина и для аннулирования записи о смерти в книге государственной регистрации актов гражданского состояния. Новое решение порождает правовые последствия, реализация которых осуществляется органами, заинтересованными в получении таких решений от судов: отменяется управление имуществом безвестно отсутствующего гражданина, т. е. расторгается договор доверительного управления имуществом, и имущество возвращается явившемуся гражданину, гражданину, объявленному умершим, возвращается сохранившееся имущество, прекращается право иждивенцев на получение пенсии по случаю потери кормильца.

Фрагмент Раздела 3. Движение и результаты рассмотрения гражданских дел формы № 2 и Раздел 3. Результаты рассмотрения гражданских апелляционных дел по удовлетворенным жалобам и представлениям (строки в таблицах разделов совпадают)					
Категории гражданских дел				**№ стр. текущего отчета**	**№ стр. проекта**
Дела искового производства	**споры, возникающие из семейных правоотношений**	**иные споры, связанные с воспитанием детей**		25	25
		из строки 25: «иные споры, связанные с воспитанием детей»	споры о месте жительства ребенка при раздельном проживании родителей (п. 3 ст. 65 СК РФ)		26
			об осуществлении родительских прав родителем, проживающим отдельно от ребенка (п. 2 ст. 66 СК РФ)		27
			об устранении препятствий к общению с ребенком его близких родственников (п. 3 ст. 67 СК РФ)		28
			о возврате родителям ребенка, удерживаемого не на основании закона или судебного решения (п. 1 ст. 68 СК РФ)		29
			о возврате опекунам (попечителям) подопечного от любых лиц, удерживающих у себя ребенка без законных оснований (п. 2 ст. 150 СК РФ)		30
			о возврате приемному родителю ребенка, удерживаемого другими лицами не на основании закона или судебного решения (п. 3 ст. 153 СК РФ)		31
			об отмене ограничения родительских прав (ст. 76 СК РФ)		32
			об отобрании ребенка при непосредственной угрозе жизни ребенка или его здоровью (ст.77 СК РФ)		33

Рис. 2. Настройка статистических показателей (Форма № 2)

теру заявления требования не относятся ни к одной из выделенных категорий.

Рассмотрим еще один ***пример*** реализации требований ТЗ по доработке автоматизированного судебного делопроизводства на 2022 г., предусматривающей использование централизованных справочников в процедуре автоматического расчета срока хранения гражданских и административных дел в электронных картотеках судебного делопроизводства.

Сроки хранения устанавливаются нормативными документами СД[32], содержащими также перечень пунктов (статей перечня) по категориям дел, определенным характеристикам дел или результатам рассмотрения дел, влияющими на сроки хранения. Для реализации задачи *автоматизированного формирования срока хранения* по категории дела необходимо учтенную категорию гражданского или административного дела (по справочнику 9200) связать с категориями перечня архивного хранения, которые могут как полностью совпадать с выделенными категориями справочника, так и различаться по наименованию, но быть, по сути, одинаковыми по содержанию или содержаться в статье по перечню сроков хранения в обобщенном виде. В ПИ «ОО» выделенные значения перечней сроков хранения предусмотрены в справочнике 112 «Номенклатура дел и документов». Проблемой для задачи *автоматизированного расчета сроков хранения* категории гражданских и административных дел по статьям и пунктам Перечня является выделение в статьях категорий гражданских дел, являющихся более детализированными по содержанию, нежели значения категорий дел в справочнике 9200, использующиеся в первичном учете требований в картотеках автоматизированного судебного делопроизводства, и по которым установлены сроки хранения, отличающиеся от обобщенных категорий. Поэтому единственным решением для автоматизации расчета является добавление и выделение их

[32] Приказ Судебного департамента при Верховном Суде РФ от 9 июня 2011 г. № 112 (ред. от 20.12.2019) «Об утверждении Перечня документов федеральных судов общей юрисдикции с указанием сроков хранения» утратил силу в связи с изданием Приказа Судебного департамента при Верховном Суде РФ от 21 декабря 2022 г. № 242 «Об утверждении Перечня документов, образующихся в процессе деятельности федеральных судов общей юрисдикции, с указанием сроков их хранения и Порядка хранения некоторых видов документов, предусмотренных Перечнем документов, образующихся в процессе деятельности федеральных судов общей юрисдикции, с указанием сроков их хранения», который введен в действие с 01.01.23.

Таблица 4

Фрагмент перечня документов федеральных судов общей юрисдикции с указанием сроков их хранения

Номер статьи	Вид документа	Срок хранения документа		
		в кассационных и апелляционных судах	в областных и равных им судах	в районных судах
275.	Об установлении факта родственных отношений	—	—	10 лет ЭПК[3]
277.	Об установлении факта регистрации рождения, усыновления (удочерения), брака, расторжения брака, смерти	—	—	10 лет ЭПК
279.	Об установлении факта принадлежности правоустанавливающих документов	—	—	5 лет
280.	Об установлении факта владения и пользования недвижимым имуществом	—	—	10 лет ЭПК
281.	Об установлении факта несчастного случая	—	—	30 лет ЭПК
283.	Об установлении факта репрессии	—	—	Постоянно
284.	Об установлении других фактов, имеющих юридическое значение (1)	—	—	5 лет ЭПК

в качестве подкатегорий к имеющимся категориям дел в справочник 9200. Например, в первичном учете и в статистической отчетности по гражданским делам особого производства выделяется следующие категории справочника 9200:

580000 «Дела об установлении фактов, имеющих юридическое значение»;

580012 «Дела об установлении факта признания отцовства»;

730012 «Дела об установлении факта принятия наследства»;

730013 «Дела об установлении факта нахождения на иждивении»;

730014 «Иные дела об установлении фактов, имеющих юридическое значение».

В Перечне по срокам хранения выделяются дополнительно дела по требованиям об установлении иных юридических фактов, при этом имеющие сроки хранения, отличные от общих по всем делам этой категории 5 лет[33], а именно до 10 или 30 лет, или постоянного хранения (*табл. 4*).

Таким образом, для решения задач *автоматизации расчета сроков хранения* необходимо дополнить учет категорий дел более детальными категориями, внеся их как подчиненные категории в узел (группу) 580000 «Дела об установлении фактов, имеющих юридическое значение».

[33] Пункт 284 Перечня.

Заключение

Утверждение нормативного правового акта, регулирующего ведение НСИ в программном изделии «Организационное обеспечение», позволит новым пользователям и разработчикам программных изделий ГАС РФ «Правосудие» использовать актуальные значения справочников при эксплуатации АИС судебного делопроизводства, урегулировать вопросы информационного взаимодействия между службой ведения НСИ, разработчиками программных изделий — потребителями справочников и пользователями.

Перспективой развития централизованных справочников НСИ в ПИ «ОО» является включение всех справочников по видам судопроизводства (например, по результатам рассмотрения дел в судебных инстанциях), которые в настоящее время ведутся локально в АИС. Использование общих централизованных справочников актуально для работы с аналитической *моделью судебного делопроизводства* по сведениям Единой картотеки судебных дел и Консолидированного банка

[34] ЭПК — экспертно-проверочная комиссия. В соответствии с п. 12. Приказа Судебного департамента от 21 декабря 2022 г. № 242 «отметка «ЭПК» означает, что указанные документы или часть указанных документов могут быть отобраны на постоянное хранение по результатам экспертизы их ценности».

[35] Относятся к делам об установлении фактов, имеющих юридическое значение.

судебных решений (например, отбор учтенных данных по значениям справочника).

Централизованное ведение справочников НСИ позволяет получать на основе содержания справочников судопроизводства заинтересованным пользователям *аналитическую* информацию: делать выборки из справочников по состоянию на определенную дату актуальности (например, списки составов, относящиеся к подсудности мировых судей или рассматриваемые судом с участием присяжных заседателей на определенную дату, и др.).

Как направление развития функционала ПИ «ОО» по использованию централизованного ведения справочников НСИ следует отметить формирование новых «преднастроенных» отчетов на основе справочников для использования в программных шаблонах статистических отчетов[36].

Представляется актуальным также централизованное ведение справочника мировых судей с возможностью связи с записями справочника федеральных судей (для идентификации конкретных судей) при переходе лиц из одного статуса в другой. Использование единого справочника мировых судей необходимо для учета в судебном делопроизводстве не только на судебных участках мировых судей в судебном районе, где исполняются обязанности мирового судьи, но и для выбора полного имени мирового судьи, чье судебное решение обжаловано в вышестоящих судебных инстанциях. И если для районных судов субъекта РФ возможно решение этого вопроса путем ведения локальных справочников в автоматизированном судебном делопроизводстве, то для кассационных судов общей юрисдикции или для Верховного Суда РФ такое техническое решение уже представляется некорректным.

Новым направлением модификации функционала программного изделия «Организационное обеспечение» становится взаимодействие с внешними АИС через государственный информационный ресурс Федеральной государственной информационной системы «Единая система нормативной справочной информации» (ФГИС ЕСНСИ)[37].

[36] В настоящее время используются отчеты для проверки средних сумм административных штрафов и раскраски в разделах форм отчетности № 1-АП, 01-АС, отчеты с раскраской неподсудных составов преступлений для программных шаблонов по судимости, на основе имеющихся сведений в справочнике для формирования логической раскраски в программных шаблонах форм статистической отчетности (могут быть данные — желтая ячейка, не могут быть — серая или оранжевая, требуют проверки с информационным контролем).

[37] ФГИС ЕСНСИ — федеральная государственная информационная система, целью создания которой является обеспечение автоматизированного формирования, актуализации и использования реестра базовых государственных информационных ресурсов, а также размещение, хранение и актуализация информации технического характера, используемой в межведомственном электронном взаимодействии для обеспечения единообразного представления объектов информационного обмена, сведения о которых содержатся в государственных и муниципальных информационных ресурсах и используются в деятельности органов государственной власти и органов местного самоуправления при исполнении государственных и муниципальных функций и предоставлении государственных и муниципальных услуг в электронном виде, и которая функционирует с учетом требований к информационной среде в сфере систематизации и кодирования информации. URL: http://digital.gov.ru/ru/activity/directions/491/?utm_referrer=https://www.google.com/

См. Приказ Минкомсвязи России «О внесении изменений в приказ Министерства связи и массовых коммуникаций Российской Федерации от 19 января 2015 г. № 7 «Об утверждении Положения о федеральной государственной информационной системе «Единая система нормативной справочной информации», а также Перечень нормативной справочной информации, подлежащей размещению в федеральной государственной информационной системе «Единая система нормативной справочной информации».

Рецензент: ***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

Литература

1. Андрюшечкина И.Н. Использование нормативно-справочной информации судебного делопроизводства для задач ведения судебной статистики // Правовая информатика. 2019. № 3. С. 21—40. DOI: 10.21681/1994-1404-2019-3-21-40 .
2. Андрюшечкина И.Н. Формирование нормативно-справочной информации для задач ведения уголовной судебной статистики // Правовая информатика. 2022. № 3. С. 40—50. DOI: 10.21681/1994-1404-2022-3-40-50 .
3. Андрюшечкина И.Н., Ниесов В.А. О создании единой системы классификации гражданских дел и материалов судов общей юрисдикции // Российская юстиция. 2007. № 4. С. 71—73.
4. Андрюшечкина И.Н., Ниесов В.А. Актуальные вопросы создания и организации использования единой системы классификации категорий судебных дел в судах общей юрисдикции // Российское правосудие. 2010. № 2 (46). С. 25—31.
5. 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 .

6. Ловцов Д.А. Информационная теория эргасистем. Тезаурус. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
7. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
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. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
10. Ловцов Д.А. Системный анализ. Часть. 1. Теоретические основы. М. : РГУП, 2018. 224 с. ISBN 978-5-93916-701-7.
11. Ловцов Д.А., Ниесов В.А. Актуальные проблемы создания и развития единого информационного пространства судебной системы России // Информационное право. 2013. № 5. С. 13—18.
12. Ловцов Д.А., Ниесов В.А. Формирование единого информационного пространства судебной системы России // Российское правосудие. 2008. № 11. С. 78—88.
13. 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 .
14. Негру Д.В., Холкин И.И. Ведение нормативно-справочной информации // Научный альманах МИРЭА. 2015. № 10-3 (12). С. 192—195.

REGULATORY REFERENCE INFORMATION IN COURT AUTOMATED SYSTEMS

Irina Andriushechkina, *Ph.D. (Law), Associate Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Head of the Department of Organisational and Methodological Support for Collecting Court Statistics of the Main Directorate for Organisational Support for the Activities of the Courts of the Judicial Department under the Supreme Court of the Russian Federation, Moscow, Russian Federation.*
E-mail: andr-home2008@yandex.ru

Oleg Zivenko, *Ph.D. (Technology), Senior Researcher, Projects Director of OOO (LLC/LLP) Iterion, the main contractor for modification and technical support of software products of the Government Automated System "Pravosudie" (GAS "Justice"), Moscow, Russian Federation.*
E-mail: zivenko@mail.ru

Keywords: *regulatory reference information, automated information system, automated court proceedings, information support, court information, anatylical information, centralised reference files, software products, information compatibility, Government Automated System "Pravosudie" [GAS "Justice"].*

Abstract

Purpose of the paper: studying the structure and content of regulatory reference information contained in court automated information systems with a view to maintain information support efficiency.

Methods used: system analysis, pragmatical classification and productive clusterisation, expert assessment.

Study findings: questions of legal regulation of maintaining regulatory reference information databases used in special software products included in the Government Automated System "Pravosudie" [GAS "Justice"] and other automated information systems used by the courts of the Russian Federation are studied. A conventional distribution of general system reference files between different software products of the GAS "Justice" is determined. Practical tasks and prospects for maintaining regulatory reference information databases in the subsystem "Organisational Support" of the GAS "Justice" are identified. The role of regulatory reference information in the inter-institutional interaction of automated information systems of government agencies is assessed.

References

1. Andriushechkina I.N. Ispol'zovanie normativno-spravochnoi informatsii sudebnogo deloproizvodstva dlia zadach vedeniia sudebnoi statistiki. Pravovaia informatika, 2019, No. 3, pp. 21–40. DOI: 10.21681/1994-1404-2019-3-21-40 .
2. Andriushechkina I.N. Formirovanie normativno-spravochnoi informatsii dlia zadach vedeniia ugolovnoi sudebnoi statistiki. Pravovaia informatika, 2022, No. 3, pp. 40–50. DOI: 10.21681/1994-1404-2022-3-40-50 .

3. Andriushechkina I.N., Niesov V.A. O sozdanii edinoi sistemy klassifikatsii grazhdanskikh del i materialov sudov obshchei iurisdiktsii. Rossiiskaia iustitsiia, 2007, No. 4, pp. 71–73.
4. Andriushechkina I.N., Niesov V.A. Aktual'nye voprosy sozdaniia i organizatsii ispol'zovaniia edinoi sistemy klassifikatsii kategorii sudebnykh del v sudakh obshchei iurisdiktsii. Rossiiskoe pravosudie, 2010, No. 2 (46), pp. 25–31.
5. 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 .
6. Lovtsov D.A. Informatsionnaia teoriia ergasistem. Tezaurus. M. : Nauka, 2005. 248 pp. ISBN 5-02- 033779-X.
7. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
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. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
10. Lovtsov D.A. Sistemnyi analiz. Chast'. 1. Teoreticheskie osnovy. M. : RGUP, 2018. 224 pp. ISBN 978-5-93916-701-7.
11. Lovtsov D.A., Niesov V.A. Aktual'nye problemy sozdaniia i razvitiia edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii. Informatsionnoe pravo, 2013, No. 5, pp. 13–18.
12. Lovtsov D.A., Niesov V.A. Formirovanie edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii. Rossiiskoe pravosudie, 2008, No. 11, pp. 78–88.
13. 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 .
14. Negru D.V., Kholkin I.I. Vedenie normativno-spravochnoi informatsii. Nauchnyi al'manakh MIREA, 2015, No. 10-3 (12), pp. 192–195.

ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИСПОЛЬЗОВАНИЯ МЕТОДА 3D-СКАНИРОВАНИЯ В СУДЕБНОЙ ЭКСПЕРТИЗЕ

Моисеева Т.Ф.[1]

Ключевые слова: *судебная экспертиза, 3D-сканеры, 3D-модели, метод 3D-сканирования, допустимость, реконструкция, принципы, условия, требования, вещественные доказательства, экспертная специальность.*

Аннотация

Цель работы: обоснование методических и правовых принципов использования 3D-сканирования в судебной экспертизе.

Методы исследования: системный анализ использования 3D-сканирования, сравнительно-правовой анализ статей законодательства, регулирующих использование методов и средств в судебной экспертизе, а также современных методик экспертного исследования внешнего строения объектов и практику использования 3D-сканирования в криминалистике и судебной экспертизе.

Результаты исследования: определено, что метод 3D-сканирования отвечает всем требованиям методологии судебной экспертизы, является научно-обоснованным, достоверным и эффективным и его применение в судебно-экспертных исследованиях не требует дополнительного правового регулирования; обоснована необходимость разработки профильных экспертных методик 3D-сканирования объектов судебной экспертизы и подготовки экспертов по данному направлению исследований.

DOI: 10.21681/1994-1404-2023-1-34-40

Введение

В последние годы развитие компьютерных технологий привело к их повсеместному внедрению, в том числе в криминалистику и судебную экспертизу. Одним из эффективных и перспективных является метод анализа изображения, основанный на 3D-сканировании и создании 3D-моделей. С его помощью возможно представлять материальные объекты в цифровом формате, анализировать их и при необходимости воссоздавать их в виде объемной модели. Внедрение этого метода связано с разработкой удобных в использовании 3D-сканеров, представляющих собой устройства, позволяющие создать 3D-модель материального объекта путем анализа его внешнего строения и использования специального программного обеспечения.

3D-сканеры используют как средство получения и фиксирования информации о внешнем строении объекта, которую можно рассматривать в качестве цифрового следа отображения внешнего строения объекта, т. е. как разновидность трасологических объектов — объектов отображения.

3D-сканеры можно также рассматривать как средство фиксации для создания цифровых моделей, используемых для создания систем криминалистической регистрации разных объектов. В настоящее время 3D-сканирование лежит в основе функционирования систем распознавания личности. Кроме того, распечатанные на 3D-принтере объемные 3D-модели могут быть использованы для исследования в качестве вещественных доказательств.

Анализ использования 3D-сканирования

Имеются данные компаний производителей, а также научные публикации, свидетельствующие об эффективном использовании 3D-сканирования при производстве следственных действий, главным образом при осмотре места происшествия [10]. Это позволяет в считанные минуты зафиксировать обстановку места происшествия с большой точностью и с последующим ее воспроизведением для тщательного изучения в удобных условиях. Особенно актуально применение данной технологии при расследовании убийств и дорожно-транспортных происшествий (ДТП). Доступность 3D-моделей ДТП приводит к существенному повышению *оперативности* и *результативности* работы правоохранительных органов.

Многие зарубежные страны, такие как Великобритания, США, Германия, с 2011 г. используют метод 3D-сканирования для более полного анализа, моде-

[1] ***Моисеева Татьяна Фёдоровна,*** *доктор юридических наук, профессор, заведующий кафедрой судебных экспертиз и криминалистики Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: moiseevatf@mail.ru

лирования и реконструкции ДТП[2]. Очень точная фиксация объемных следов преступления с помощью 3D-сканеров имеет существенные преимущества по сравнению с традиционными способами фиксации следов с помощью фотографии или слепков для объемных следов (например, обуви) и позволяет представлять следы в цифровой форме, что является в настоящее время определяющим для формирования баз данных для криминалистической регистрации. При этом оцифрованный объект при необходимости можно представить в виде объемной модели с использованием 3D-принтера.

Большие возможности использования 3D-сканеров видятся и в судебной экспертизе. Обзор зарубежных публикаций об использовании 3D-сканирования в судебной экспертизе и перспективных направлениях, сделанный еще в 2014 г. [13], позволял сделать вывод о несомненной целесообразности использования 3D-технологий в исследовании объектов судебной экспертизы.

В настоящее время технология 3D-сканирования используется при исследовании достаточно широкого круга объектов различных родов и видов судебных экспертиз: судебно-медицинской [3, 19]; судебной автотехнической [1, 15]; судебной баллистической [14]; инженерно-технической [16]; судебно-строительной [5], судебно-портретной [18]; трасологической [11] и др.

Однако возможности технологии 3D-сканирования в судебной экспертизе реализованы не в полной мере. Возможность получения объемной картины объекта с высокой точностью может быть использована и в почерковедческой экспертизе, где толщина штрихов позволяет получать информацию о нажимных характеристиках почерка, и в экспертизе материалов документов. Большие перспективы использования 3D-технологий имеются в трасологических исследованиях, основанных на изучении внешнего строения объектов и их следов отображения, поро- и эджескопии папиллярных линий, для фиксации и исследования других следов человека, а также следов орудий взлома и инструментов, животных, транспортных средств и др.

Ограниченное использование 3D-сканеров связано с достаточной дороговизной данного оборудования, однако эффективность их использования оправдывает затраты на их приобретение. Кроме того, с увеличением спроса и, соответственно, производства 3D-сканеров их стоимость постепенно снижается, что, несомненно, приведет к более широкому использованию 3D-сканеров в криминалистике и судебной экспертизе.

Внедрение этого метода связано с разработкой удобных в использовании 3D-сканеров и программного обеспечения.

3D-сканеры делятся на *контактные* (специальным щупом обводится поверхность исследуемого объекта с целью определения и передачи его трехмерных координат) и *бесконтактные*, основанные на сканировании поверхности объекта лазерным лучом.

Основными характеристиками сканера являются:

- точность воспроизведения объекта в модели (зависит от условий изменения и самого объекта измерения);
- плотность сканирования (количество точек на квадратный миллиметр);
- скорость сканирования;
- область сканирования (от 10 мм до 10 м).

Все эти параметры связаны и взаимозависимы. Увеличение скорости сканирования может привести к уменьшению точности и/или плотности.

На рынке имеется множество предложений 3D-сканеров не только зарубежного: фирмы *ScanTech*, *Shining 3D* (обе — Китай), *Solutionix* (Корея), *Creaform* (Канада), *Occipital* (США), *XYZPrinting* (Тайвань) и др., но и отечественного производства: фирмы *RangeVision*, *Up3D*, *Scanform*, *Artec 3D* и др.

Обзор 3D-сканеров и их использования в криминалистике был сделан в ряде публикаций, например, в [2]. Основные характеристики современных сканеров можно оценить на примере признанного одним из лучших 3D-сканеров стоимостью менее 50 000 долларов США по версии *iReviews* — 3*D*-сканер для профессионалов *Eva* фирмы *Artec*.

Легкий, быстрый и универсальный сканер *Eva* является самым популярным сканером и лидером на рынке портативных 3D-сканеров. Основанный на безопасной в использовании технологии сканирования со структурированным освещением, он представляет собой превосходное универсальное решение для съемки объектов практически любого типа, включая объекты с черной и блестящей поверхностью. Площадь сканирования: 214×148 мм на ближайшем расстоянии и 536×371 мм на дальнем расстоянии. 3D-разрешение — до 0,5 мм. Основные характеристики: масса — 850 г; точность — 0,1 мм; скорость — 16 кадров в секунду (кдр/с); захват — 2 000 000 точек.

Сканер *Eva* способен работать на расстоянии от 0,4 мм до 1 м от объекта с частотой до 16 кдр/с и не требует прогрева, что позволяет начать работу сразу после включения.

О необходимости дополнительного правового регулирования 3D-сканирования в криминалистике и судебной экспертизе говорится в ряде публикаций [4, 9].

Виды 3D-доказательств

Рассматривая возможное использование 3D-доказательств в российском уголовном процессе, Н.А. Иванов писал, что «*для успешной их легализации в общей системе уголовных доказательств необходимо решить очень много проблем, начиная с терминологии и вопросов правового регулирования их создания и применения в уголовном процессе*» [4]. Он выделял две основные группы таких доказательств: *первая* — это «*виртуальные 3D-доказательства*», в нее включаются

[2] См.: FARO Focus 3D Laser Scanner. URL: https://www.faro.com/products/construction-bim/faro-focus (дата обращения: 11.11.2022).

3D-фотографии, 3D-фильмы (в том числе созданные путем анимации), а также компьютерные программы, в результате работы которых создаются 3D-изображения. *Вторая* группа — это «*реальные 3D-доказательства*», к ней относятся копии материальных объектов (в том числе предварительно отсканированных с помощью 3D-сканеров), созданных с помощью 3D-принтеров.

Поскольку объектом исследования судебной экспертизы являются материальные носители информации о расследуемом событии, то рассмотрим необходимость дополнительного правового регулирования *второй* выделенной Н.А. Ивановым группы 3D-доказательств.

Поскольку судебная экспертиза — это процессуальное действие, результаты которого имеют значение доказательств, то использование при ее производстве методов и средств исследования должно быть процессуально допустимым.

Правовое обеспечение связано с решением двух основных *проблем*:

1. Допустимость использования сканеров и метода сканирования при производстве судебных экспертиз.

2. Допустимость использования результатов сканирования в качестве объектов судебной экспертизы, результаты которой являются доказательствами, а также использование полученных на 3D-принтерах объемных моделей в качестве вещественных доказательств (отображение вещественного доказательства).

В ч. 6 ст. 164 УПК РФ говорится о допустимости применять при производстве следственных действий технические средства для обнаружения, фиксации и изъятия следов преступления и вещественных доказательств. Использование 3D-сканеров в криминалистике как раз и связано со средствами одновременной фиксацией и изъятием следов преступления и вещественных доказательств.

Закон не устанавливает четкого перечня методов, допустимых в судопроизводстве, поскольку это могло бы привести к невозможности оперативного внедрения новых научных методов в практику судебно-экспертных исследований. Однако к ним предъявляются *требования*, характерные для методов любой науки: *научная обоснованность, эффективность, безопасность*, а также специфическое требование *этичности* и *законности*. Кроме того, желательно использование методов, не разрушающих или изменяющих объект исследования.

Метод 3D-сканирования полностью отвечает этим требованиям и не нуждается в дополнительном правовом обосновании его использования в криминалистике и судебной экспертизе. Он основан на научно обоснованных современных технологиях и уже несколько десятилетий успешно применяется в различных областях науки и техники. В его основе лежит *принцип оцифровки* любого объекта как контактным, так и бесконтактным способом.

При контактном способе механический щуп со специальным датчиком контактирует с объектом-прометом, проводит замеры, информация о которых поступает на сканер и преобразовывается с помощью программ в цифровой вид. При контакте со щупом есть небольшой риск повреждения объекта. Кроме того, иногда местонахождение объекта не дает возможность непосредственно его касаться.

Для судебно-экспертных исследований бесконтактный способ представляется наиболее приемлемым, поскольку сканирование осуществляется на расстоянии, что исключает повреждение объекта. Так, например, Е.В. Пискунова отмечает [13], что лазерное сканирование, которое осуществляется бесконтактным методом, не только облегчает фиксацию следов, но и позволяет один и тот же след исследовать разными методами, получить больше информации. Например, обнаруженная на месте происшествия жевательная резинка сохраняет и следы зубов, и ДНК, т. е. лазерное сканирование позволяет сделать слепки зубов, не повредив ДНК, в отличие от традиционных средств фиксации объемных следов.

Следовательно, использование 3D-сканеров позволяет выполнять одно из значимых для методов судебной экспертизы и криминалистики *условий* — не повреждать объект исследования, что позволяет исследовать его другими методами, использовать при необходимости для проведения повторных исследований, а при создании объемных моделей проводить повреждающие исследования на них, сохраняя тем самым сам объект — *вещественное доказательство* — для его непосредственного исследования в суде. Кроме того, цифровое интеллектуальное управление материальными доказательствами может эффективно решать проблемы, связанные с хранением, управлением и поиском доказательств. 3D-модели вещественных доказательств могут быть загружены на интеллектуальную платформу управления вещественными доказательствами, что позволяет сторонам в судебном процессе забрать свои вещественные доказательства для сохранения и представить их позже, если это необходимо.

Метод 3D-сканирования отвечает и *принципу эффективности*, поскольку с минимальными временными и трудовыми затратами позволяет одновременно фиксировать объекты с очень большой точностью и исследовать его, т. е. метод 3D-моделирования соответствует требованиям к методам криминалистики и судебной экспертизы.

Допустимость 3D-доказательств в России

Второй вопрос связан с *допустимостью* использования полученных с помощью 3D-сканирования результатов и моделей объектов в качестве вещественных доказательств.

За рубежом уже появилось такое понятие, как *3D printed evidence*, т. е. в качестве доказательств рассматриваются точные копии или масштабированные модели доказательств, которые помогают сотрудникам правоохранительных органов в процессе раскрытия

и расследования преступлений для установления картины произошедшего [14].

Выше уже говорилось о том, что с помощью 3D-сканирования мы фиксируем следы-отображения или следы предметов с большой точностью (около 0,1 мм). Классическим примером следов-отображений являются следы папиллярных узоров пальцев рук, которые традиционно фиксировали с помощью дактопленки либо фотографированием выявленных следов [6, 7]. По сравнению с фотофиксацией метод 3D-сканирования не только позволяет получать объемное и значительно более четкое изображение следа, но и детально исследовать его с помощью специальных программ.

Так, канадскими учеными Джануджи Сиванандана и Юджином Лисио (Университет Торонто) был проведен *эксперимент* с целью сравнения традиционных методов фиксации объектов судебной медицины с использованием технологии 3D-сканирования. Для своего эксперимента исследователи выбрали 3D-сканер *Artec Eva Structured Light,* чтобы определить, насколько хорошо он соответствует современным средствам фотографической документации. В частности, исследовались татуировки на теле человека, а также пулевые отверстия на трупе с целью установления траектории попадания пули. Было показано, что способность сканера *Artec Eva* воспроизводить сложные геометрические детали татуировки (собственно, любых повреждений кожи) оказалась значительно лучше, если сравнивать ее с традиционными методами фотофиксации. Ещё одно очевидное преимущество 3*D*-сканера — способность точно улавливать и передавать цвет. Кроме того, сканер *Artec Eva* превзошел традиционный метод по простоте и почти вдвое — по скорости фиксации. В то время как для завершения полной фотодокументации потребовалось ровно 54 мин 30 с, с помощью сканера *Artec Eva* это заняло 26 мин 1 с. В результате экспериментов исследователи пришли к *выводу*, что 3D-сканирование с помощью сканера *Artec Eva* обладает существенными преимуществами по сравнению с современными методами криминалистической документации[3].

Копирование потожировых следов рук на дактопленку исключает возможность исследования вещества следов, в том числе и ДНК. Отсканированные 3D-изображения различных видов трасологических следов (человека, животных, орудий взлома и инструментов, автотранспортных средств и др.), несомненно, являются объектами судебно-трасологической экспертизы. О преимуществе использования 3D-методов в судебной дактилоскопической экспертизе свидетельствует случай из экспертной практики штата Мичиган, где в 2016 г. с помощью мягкого пластика и 3D-принтера были воспроизведены копии пальцев жертвы убийства. Это было необходимо для того, чтобы снять блокировку со смартфона, который был защищен доступом по отпечатку пальца владельца [12].

Возможность использования вместо вещественных доказательств их изображений, полученных путем 3D-сканирования, с последующей печатью объемных моделей на 3D-принтере также не вызывает сомнений. Моделирование является одним из общенаучных методов и широко используется в криминалистике и судебной экспертизе для проведения модельных экспериментов. Цель применения данного метода заключается в замене исходного объекта его моделью, отражающей существенные для исследования свойства исходного объекта, и дальнейшем изучении данных свойств у модели [8].

Ведущий ученый в области трасологии Н.П. Майлис выделяет среди методов моделирования в судебной экспертизе методы 3D-моделирования, которые, в отличие от реставрации (восстановления) объекта, создают его модель, в качестве наиболее эффективных в доказывании [8]. В этом аспекте методы 3*D*-сканирования можно рассматривать как методы *реконструкции* объектов экспертизы.

Допустимость использования модели вместо вещественного доказательства определяется прежде всего тем, насколько адекватно модель соответствует объекту, как точно отражает его характеристики. В ряде случаев только 3D-модель позволяет сохранить значимые информативные признаки объекта. Это особенно актуально для судебно-медицинской экспертизы, объекты которой подвержены быстрому изменению. Так, трехмерная модель раневых каналов трупа надежно и полно фиксирует все особенности повреждений, в отличие от вербального описания в экспертном заключении, что имеет важное значение в случае необходимости проведения повторной судебно-медицинской экспертизы спустя длительное время. Большое значение метод 3D-моделирования имеет при производстве судебно-медицинских экспертиз для визуализации, идентификации и реконструкции объектов [17].

Кроме того, 3D-сканирование дает возможность получить *информацию* и зафиксировать ее в виде объемной модели для следов на специфических поверхностях — снег, пыль, масло, кожные покровы человека и др., для которых использование традиционных технологий достаточно проблематично[4].

Перспективы применения 3D-технологий в судебной экспертизе

Использование сложных современных инструментальных методов исследования объектов судебной экспертизы требует специальной подготовки. Несмотря на, казалось бы, простоту использования метода 3D-сканирования, его грамотное применение в судеб-

[3] См.: 3D scanning tested against photography in a study on forensic methods. URL: https://www.artec3d.com/cases/3d-scanning-tested-against-photography-in-autopsy

[4] См.: FARO Focus 3D Laser Scanner. URL: https://www.faro.com/products/construction-bim/faro-focus (дата обращения: 11.11.2022).

ной экспертизе требует специальных знаний в области цифровых технологий, и для получения необходимой информации о составе, внешнем строении и внутренней структуре объектов привлекаются специалисты в области научного знания, лежащего в их основе. Круг специальных знаний, которыми должны владеть специалисты, проводящие исследования методом 3D-сканирования и 3D-моделирования, не ограничивается только знанием цифровых технологий, а включает и знание экспертных методик, и правовых аспектов производства судебных экспертиз. Представляется, что есть основания говорить о возможности формирования новой *экспертной специальности* по судебно-экспертному исследованию объектов судебной экспертизы методами 3D-сканирования и 3D-моделирования.

В перечне экспертных специальностей судебно-экспертных учреждений Министерства юстиции РФ обозначен круг так называемых методных специальностей:

22.1 Применение методов молекулярной спектроскопии при исследовании объектов судебной экспертизы;

22.2 Применение методов атомной спектроскопии при исследовании объектов судебной экспертизы;

22.3 Применение рентгенографических методов при исследовании объектов судебной экспертизы;

22.4 Применение рентгеноспектральных методов и методов электронной микроскопии при исследовании объектов судебной экспертизы;

22.5 Применение хроматографических методов при исследовании объектов судебной экспертизы[5].

Этот перечень может быть дополнен специальностью 22.6 «Применение методов 3D-технологий при исследовании объектов судебной экспертизы».

При этом необходима разработка *методик* применения метода 3D-сканирования и получения объемных моделей для решения конкретных идентификационных и диагностических экспертных задач в отношении конкретных объектов судебной экспертизы, к которым могут относиться не только объекты самых разных родов и видов судебных экспертиз, но и сами 3D-сканеры и 3D-принтеры.

Таким образом, специфика использования 3D-сканеров в судебной экспертизе — несомненно, перспективна и не требует специального правового обеспечения, однако обусловливает необходимость разработки новых экспертных методик, а также целесообразность формирования новой экспертной специальности по применению в судебной экспертизе 3D-технологий и анализа результатов использования искусственного интеллекта.

[5] Перечень экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России. Приказ Минюста РФ от 27 декабря 2012 г. № 237 «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России» (с изменениями на 28 декабря 2021 г.) URL:https://docs.cntd.ru/document/902392151#6560IO

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

Литература

1. Думнов С.Н. К вопросу применения метода лазерного 3D-сканирования при производстве судебной автотехнической экспертизы // Вестник Вост.-Сиб. института МВД России. 2019. № 3 (90). С. 133—145.
2. Еремченко В.И. Практика использования 3D-сканирования местности в деятельности правоохранительных органов // Труды VII МНК «Актуальные проблемы уголовного процесса и криминалистики» (30 апреля 2021 г.) / МИ МВД Республики Беларусь. Могилев : МИ МВД РБ, 2021. С. 56—61.
3. Ерофеев С.В., Федорова А.С., Ковалев А.В., Шишкин Ю.Ю., Фетисов В.А. Трехмерное сканирование судебно-медицинских объектов: приборное обеспечение и особенности технологии // Судебно-медицинская экспертиза. 2018. № 61 (6). С. 39—42.
4. Иванов Н.А. 3D-доказательства: понятие и классификация // Российский следователь. 2013. № 15. С. 5—7.
5. Карнаухова О.Г., Дондукова Т.Б., Самусенко Е.М. Теоретические и практические основы применения технологии трехмерного лазерного сканирования в судебной строительно-технической экспертизе // Социология и право. 2022. № 14 (4). С. 456—466.
6. Ловцов Д.А., Князев К.В. Защищённая биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100—103.
7. Ловцов Д.А., Князев К.В. Защищённая биометрическая идентификация в системах контроля доступа. II. Качество информационно-математического обеспечения // Информация и космос. 2013. № 2. С. 95—100.

8. Майлис Н.П. Методы моделирования при производстве судебных экспертиз как эффективное средство в доказывании // Вестник Московского университета МВД России. 2018. № 4. С. 71—73.
9. Маннова А.А., Рожкова В.Р. 3D-сканер: инновации в области криминалистики // Вопросы российской юстиции. 2019. № 3. С. 929—934.
10. Моисеева Т.Ф. Инновационные технологии осмотра места происшествия // Вестник экономической безопасности. 2021. № 3. С. 170—174.
11. Несмиянова И.О. Современные методы фиксации и изъятия трасологических следов как эффективное средство идентификации личности // Криминологический журнал. 2018. № 3. С. 239—242.
12. Новикова Т.Б. Метод 3D-моделирования в современной судебно-экспертной деятельности // Международный журнал гуманитарных и естественных наук. 2020. Т. 12-4 (51). С. 32—35.
13. Пискунова Е.В. Использование 3D-технологий в криминалистике и судебной экспертизе : реферативный обзор. М. : ИНИОН РАН, 2014. С. 153—164.
14. Полякова А.В. Перспективы развития судебной баллистики в свете применения современных способов фиксации криминалистической информации // Законность и правопорядок. 2019. № 4 (24). С. 36—41.
15. Суденко В.Е. Новейшие технико-криминалистические средства в борьбе с транспортными преступлениями // Вестник Московского университета МВД России. 2017. № 2. С. 97—99.
16. Харченко В.Б. Особенности применения 3D-лазерного сканирования в судебной инженерно-технической экспертизе // Юридическая наука. 2019. № 10. С. 109—110.
17. Шакирьянова Ю.П. Трёхмерное моделирование в судебной медицине: визуализация, идентификация, реконструкция : автореф. дис. ... д-ра мед. наук: 14.03.05 — Судебная медицина. М., 2021. 32 с.
18. Шакирьянова Ю.П., Леонов С.В. Портретная экспертиза с применением трехмерного моделирования // Судебная медицина. 2019. № 1s. С. 165.
19. Guangyu He, Jacob M. Ricca, Amos Z. Dai, et al. A novel bone registration method using impression molding and structured-light 3D scanning technology // J. Orthop. Res. 2022. 40 (10), pp. 2340–2349.

INFORMATION AND LEGAL SUPPORT FOR USING THE 3D SCANNING METHOD IN FORENSICS

Tat'iana Moiseeva, *Dr.Sc. (Law), Professor, Head of the Department of Forensics and Criminalistics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: moiseevatf@mail.ru

Keywords: *forensic examination, 3D scanners, 3D models, 3D scanning method, admissibility, reconstruction, principles, conditions, requirements, physical evidence, expert specialty.*

Abstract

Purpose of the paper: justifying the methodological and legal principles of using 3D scanning in forensics.

Methods of study: system analysis of using 3D scanning, comparative legal analysis of the provisions of law that regulate the use of different methods and means in forensics as well as modern methodologies of expert examination of external structure of objects and the practice of using 3D scanning in criminalistics and forensics.

Study findings: it was determined that the 3D scanning method meets all requirements set by the forensic methodology, is scientifically justified, reliable and efficient, and its use in forensic examinations does not require any additional legal regulation. A justification is given for the need to work out specialised expert methodologies for 3D scanning of objects of forensic examination and to train experts in this area of research.

References

1. Dumnov S.N. K voprosu primeneniia metoda lazernogo 3D-skanirovaniia pri proizvodstve sudebnoi avtotekhnicheskoi ekspertizy. Vestnik Vost.-Sib. instituta MVD Rossii, 2019, No. 3 (90), pp. 133–145.
2. Eremchenko V.I. Praktika ispol'zovaniia 3D-skanirovaniia mestnosti v deiatel'nosti pravookhranitel'nykh organov. Trudy VII MNK "Aktual'nye problemy ugolovnogo protsessa i kriminalistiki" (30 aprelia 2021 g.). MI MVD Respubliki Belarus'. Mogilev : MI MVD RB, 2021, pp. 56–61.
3. Erofeev S.V., Fedorova A.S., Kovalev A.V., Shishkin Iu.Iu., Fetisov V.A. Trekhmernoe skanirovanie sudebno-meditsinskikh ob"ektov: pribornoe obespechenie i osobennosti tekhnologii. Sudebno-meditsinskaia ekspertiza, 2018, No. 61 (6), pp. 39–42.

4. Ivanov N.A. 3D-dokazatel'stva: poniatie i klassifikatsiia. Rossiiskii sledovatel', 2013, No. 15, pp. 5–7.
5. Karnaukhova O.G., Dondukova T.B., Samusenko E.M. Teoreticheskie i prakticheskie osnovy primeneniia tekhnologii trekhmernogo lazernogo skanirovaniia v sudebnoi stroitel'no-tekhnicheskoi ekspertize. Sotsiologiia i pravo, 2022, No. 14 (4), pp. 456–466.
6. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2013, No. 1, pp. 100–103.
7. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. II. Kachestvo informatsionno-matematicheskogo obespecheniia. Informatsiia i kosmos, 2013, No. 2, pp. 95–100.
8. Mailis N.P. Metody modelirovaniia pri proizvodstve sudebnykh ekspertiz kak effektivnoe sredstvo v dokazyvanii. Vestnik Moskovskogo universiteta MVD Rossii, 2018, No. 4, pp. 71–73.
9. Mannova A.A., Rozhkova V.R. 3D-skaner: innovatsii v oblasti kriminalistiki. Voprosy rossiiskoi iustitsii, 2019, No. 3, pp. 929–934.
10. Moiseeva T.F. Innovatsionnye tekhnologii osmotra mesta proisshestviia. Vestnik ekonomicheskoi bezopasnosti, 2021, No. 3, pp. 170–174.
11. Nesmiianova I.O. Sovremennye metody fiksatsii i iz"iatiia trasologicheskikh sledov kak effektivnoe sredstvo identifikatsii lichnosti. Kriminologicheskii zhurnal, 2018, No. 3, pp. 239–242.
12. Novikova T.B. Metod 3D-modelirovaniia v sovremennoi sudebno-ekspertnoi deiatel'nosti. Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk, 2020, t. 12-4 (51), pp. 32–35.
13. Piskunova E.V. Ispol'zovanie 3D-tekhnologii v kriminalistike i sudebnoi ekspertize : referativnyi obzor. M. : INION RAN, 2014, pp. 153–164.
14. Poliakova A.V. Perspektivy razvitiia sudebnoi ballistiki v svete primeneniia sovremennykh sposobov fiksatsii kriminalisticheskoi informatsii. Zakonnost' i pravoporiadok, 2019, No. 4 (24), pp. 36–41.
15. Sudenko V.E. Noveishie tekhniko-kriminalisticheskie sredstva v bor'be s transportnymi prestupleniiami. Vestnik Moskovskogo universiteta MVD Rossii, 2017, No. 2, pp. 97–99.
16. Kharchenko V.B. Osobennosti primeneniia 3D-lazernogo skanirovaniia v sudebnoi inzhenerno-tekhnicheskoi ekspertize. Iuridicheskaia nauka, 2019, No. 10, pp. 109–110.
17. Shakir'ianova Iu.P. Trekhmernoe modelirovanie v sudebnoi meditsine: vizualizatsiia, identifikatsiia, rekonstruktsiia : avtoref. dis. ... d-ra med. nauk: 14.03.05 – Sudebnaia meditsina. M., 2021. 32 pp.
18. Shakir'ianova Iu.P., Leonov S.V. Portretnaia ekspertiza s primeneniem trekhmernogo modelirovaniia. Sudebnaia meditsina, 2019, No. 1s, p. 165.
19. Guangyu He, Jacob M. Ricca, Amos Z. Dai, et al. A novel bone registration method using impression molding and structured-light 3D scanning technology. J. Orthop. Res. 2022. 40 (10), pp. 2340–2349.

МОДЕЛИРОВАНИЕ ОБНАРУЖЕНИЯ ИНФОРМАЦИОННЫХ АТАК НА ОСНОВЕ ТЕОРИИ КОНЕЧНЫХ АВТОМАТОВ

Гончаров В.В.[1], Гончаров А.В.[2], Мишенина О.В.[3]

Ключевые слова: *корпоративная сеть, сетевые технологии, сетевой запрос, информационная атака, информационная безопасность, конечный автомат, элемент, множество, подмножество элементов, графовая модель, случайная величина, функция и плотность распределения случайной величины.*

Аннотация

Цель работы: совершенствование научно-методических основ повышения качества контроля безопасности базовых протоколов сетевого взаимодействия на узлах корпоративной сети.

Методы: системный анализ и математический аппарат порождения и распознавания «правильно построенных» цепочек, образующих регулярные множества, задаваемые выражениями, позволяющими строить конечный автомат, допускающий в точности повторение цепочки соответствующего регулярного множества.

Результаты: разработана модель, описывающая базовый протокол сетевого взаимодействия узлов компьютерной сети, на автоматном языке P, каждый элемент которого соответствует базовому сетевому запросу и может быть корректно обработан аппаратно-программным комплексом сети; при этом язык P описывается с помощью конечных автоматов-распознавателей, выявляющих потенциально опасные запросы, элементы которых не соответствуют стандартам, описанным на базе данного языка. Обоснован вывод: включение в сигнатуру запроса времени инициирования и максимально допустимого времени его обработки позволит существенно сократить возможности реализации компьютерных атак данного типа.

Полученные результаты являются основой для создания соответствующего эффективного информационно-математического обеспечения аппаратно-программного комплекса безопасности сложных компьютерных сетей.

DOI: 10.21681/1994-1404-2023-1-41-51

Введение

Международная компания *Positive Technologies*, являющаяся крупнейшей организацией в сфере анализа защищенности [6] информационных систем, представила статистические данные об уязвимостях корпоративных информационных сетей: прикладное программное обеспечение — 56%; *web*-серверы — 44%; *web*-приложения — 13%; СУБД — 6%. То есть большинство уязвимостей в сети приходится на *web*-серверы, являющиеся неотъемлемой частью корпоративных сетей. На них могут быть реализованы как внешние, так и внутренние *web*-сервисы, приложения, базы данных, в которых может храниться конфиденциальная информация [1, 6, 8]. Часто почтовые серверы совмещаются с *web*-сервером. Около 28% успешных атак реализуются, используя уязвимости при эксплуатации *web*-приложений. В ходе нескольких внешних тестирований выявлены уязвимости, позволяющие в один шаг, без необходимости авторизации, удаленно выполнять команды операционной системы (ОС) с привилегиями *web*-приложения. Наиболее существенными атаками преодоления сетевого периметра являются: словарные пароли — 44%; уязвимости *web*-приложений — 28%; отсутствие актуальных обновлений — 16%; недостатки конфигурации — 8%; *web*-интерпретатор командной строки — 4%.

Общеизвестно, что *web*-сервисы и приложения работают с протоколами *HTTP* (*Hyper Text Transfer Protocol*):

[1] ***Гончаров Владимир Васильевич,*** *доктор технических наук, профессор, заслуженный работник высшей школы Российской Федерации, заведующий кафедрой математики Военной академии имени Петра Великого, г. Москва, Российская Федерация.*
E-mail: v_v_goncharov@mail.ru

[2] ***Гончаров Александр Владимирович,*** *соискатель Военной академии имени Петра Великого, г. Москва, Российская Федерация.*
E-mail: dinozavp@inbox.ru

[3] ***Мишенина Ольга Викторовна,*** *кандидат педагогических наук, доцент, профессор кафедры математики Военной академии имени Петра Великого, г. Москва, Российская Федерация.*
E-mail: o.v.mishenina@gmail.com

они составляют 50% от количества всех обрабатываемых протоколов на *web*-серверах. Поэтому актуальной практической задачей является разработка комплекса математических моделей защиты *web*-сервера [5, 9, 14], основанного на фильтрации *HTTP*-пакетов, не подходящих по своим семантическим параметрам под стандарты *HTTP*-запросов, описанных в стандарте *RFC* 2616 (*Request for Comments*).

Комплекс математических моделей имеет сложную иерархическую структуру взаимосвязанных программных модулей, обеспечивающих соответствующее управление доступом к сети, т. е. осуществляет идентификацию, аутентификацию и авторизацию запросов [1—3]. При этом одной из задач рассматриваемого комплекса является контроль легитимности поступающих на *web*-сервер сетевых запросов, в том числе информационных атак, маскируемых под запрос.

Поведенческая модель обнаружения информационных атак позволяет обнаружить атаку с помощью сетевых запросов, нарушающих базовый протокол сетевого взаимодействия на узлах корпоративной сети [4, 13].

Разработанная модель основывается на регулярном языке ***P***[4], представляющем собой формальный язык, удовлетворяющий определенным свойствам и позволяющий математически описывать механизмы порождения и распознавания «правильно построенных» цепочек, образующих регулярные множества[5]. В свою очередь, регулярные множества и регулярные выражения весьма близки. Но они представляют собой разные сущности: регулярное множество — множество, в общем случае бесконечное, а *регулярное выражение — это формула, схематично показывающая, как было построено соответствующее ей регулярное множество с помощью операций языка* (и эта формула конечна).

Американский математик Стивен Клини доказал[6], что каждый автоматный язык может быть задан формулой (регулярным выражением) и каждое регулярное множество может быть распознано конечным автоматом. Отсюда следуют два важных *следствия*:

– любой автоматный язык является регулярным множеством (или: для любого конечного автомата можно построить регулярное выражение, задающее распознаваемый этим автоматом язык);
– любое регулярное множество является автоматным языком (или: по любому регулярному выражению можно построить конечный автомат, допускающий в точности цепочки соответствующего регулярного множества).

Математической моделью процесса распознавания регулярного языка является вычислительное устройство, называемое конечным автоматом (КА). Термин «конечный» подчеркивает то, что вычислительное устройство имеет фиксированный и конечный объем памяти и обрабатывает последовательность входных символов, принадлежащих некоторому конечному множеству. Существуют различные типы КА; если функцией выхода КА (результатом работы) является лишь указание на то, допустима или нет входная последовательность символов, такой КА называют *конечным распознавателем*.

Формальная постановка задачи исследования

Разработанная модель основывается на регулярном (автоматном) языке ***P***, с помощью которого описывается базовый протокол сетевого взаимодействия узлов компьютерной сети[7]. Каждый элемент языка ***P*** соответствует базовому сетевому запросу и может быть корректно обработан программным обеспечением аппаратного комплекса на сети. Это значит, что такой запрос не является угрозой безопасности для сети. При этом язык ***P*** описывается с помощью конечных автоматов-распознавателей типа:

$$A =< S, X, Y, s_0, \delta, \gamma, F, s_a >,$$

где S — множество состояний; X — множество входных параметров; Y — множество семантических операторов, анализирующих данные на входе системы; $s_0 \in S$ — начальное состояние; $\delta: S \times X \to S$ — переходная функция; $\gamma: S \times X \to Y$ — функция распознавания семантических операторов, анализируемых на входе автомата; $F \subseteq S$ — множество конечных состояний, в которые переходит система при правильном распознавании элементов языка ***P***; $s_a \in S$ — конечное состояние, в которое переходит автомат при поступлении ей на вход элементов, не входящих в язык ***P***.

Предположим, что на вход конечного автомата для анализа поступает группа элементов, входящих в язык ***P,*** соответствующая сетевому запросу, поступающему на узел сети. Если после обработки группы элементов автомат перейдет в одно из конечных состояний F, это значит, что поступивший сетевой запрос может обрабатываться узлом сети, не несет в себе угрозу и не является элементом компьютерной атаки. Иначе, при переходе автомата в состояние s_a, необходимо констатировать факт обнаружения информационной атаки на сеть.

[4] Пентус А.Е., Пентус М. Теория формальных языков : учеб. пособие. М. : Изд-во ЦПИ при мехмате МГУ, 2004. 80 с.

[5] Суховеров В.С. Система автоматической обработки тематически ориентированных текстов с терминологическим словарем в формате регулярных выражений // Проблемы управления. 2019. Вып. 2. С. 41—46.

[6] Клини С.К. Введение в метаматематику. Математическая логика и рекурсивные функции // Физико-математическое наследие. М. : Юрайт, 2009. 528 с.

[7] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Теория автоматов : учебник. М. : Юрайт, 2018. 320 с.; Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы : учебник. СПб. : ИД «Питер», 2010. 944 с.

```
<Метод запроса> <Идентификатор ресурса> <Параметры доступа> <Версия HTTP> <CRFL>
[<Заголовок 1>:<Значение> <CRFL>
<Заголовок 2>:<Значение> < CRFL>
  ...
<Заголовок n>:<Значение> < CRFL>]
< CRFL>
```

Рис. 1. Формат HTTP–запроса

Этапы решения задачи

Примером поведенческой модели, в основе которой лежит работа конечных автоматов-распознавателей, служит типовая модель обнаружения компьютерной атаки на *web*-сервер. Известно, что конечный автомат будет выявлять потенциально опасные запросы, в данном случае это *HTTP*-запросы, элементы которых не соответствуют стандартам, описанным на базе языка P_{http}. На рис. 1 изображен формат *HTTP*-запроса, состоящий из нескольких полей и соответствующий стандарту *RFC* 2616[8].

Метод формирования *HTTP*-запроса: в стандартах *RFC* указаны основные методы запросов, такие как *POST, DELETE, GET, HEAD, PUT, TRACE, OPTIONS* [5, 9]. Идентификатор ресурса, которому направлен запрос, представляет собой запись в формате *URL* (*Uniform Resource Locator*). Параметры доступа используются для обработки входных данных на различных программах со стороны *web*-сервера.

Существуют различные версии *HTTP*-протокола, с помощью которого создан запрос: *HTTP* 0.9, *HTTP* 1.0, *HTTP* 1.1. Завершается первая строка запроса параметром *CRFL* (*CaReFuL mnemonic*), что означает переход на новую строку или возврат.

Далее в *HTTP*-запросе могут появляться строки с заголовками формата «Имя заголовка», «Значение», при этом разделение заголовков происходит при помощи параметра *CRFL*. Если в конце *HTTP*-запроса стоят два подряд символа *CRFL*, это значит, что запрос завершен.

Используя данную поведенческую модель, имеется возможность отфильтровывать в большом потоке данных определенные *HTTP*-запросы, которые могут предоставлять угрозу элементам сети, в частности, *web*-серверу. Такими могут быть запросы:

- не соответствующие синтаксису, стандартизированному в рамках стандартов RFC;
- которые не могут быть обработаны аппаратным комплексом сети на основе ПО;
- адресованные к несуществующим элементам web-сервера;
- с неподдерживаемой web-сервером версией протокола;
- с запрещенными заголовками.

Если в процессе анализа входящего трафика будет обнаружен хотя бы один из вышеперечисленных запросов, имеется основание констатировать факт обнаружения атаки на *web*-сервер. Чтобы отфильтровать такие *HTTP*-запросы, в разработанной модели будут использоваться конечный автомат AV_{http}, который определяет язык P_{http}. Последовательные элементы языка P_{http} включают в себя все типы *HTTP*-запросов, направленные *web*-серверу. Последовательность символов X языка P_{http}, которая описывает *HTTP*-запрос, поступает на вход автомата AV_{http}. Если в результате обработки последовательных элементов автомат переходит в конечное состояние F, то полученные *HTTP*-запросы не несут угрозы для сети. В противном случае будет определено существование информационной атаки.

Архитектура конечного автомата AV_{http}, распознающего элементы языка P_{http}, состоит из пяти составных узлов (рис. 2):

1 — узел распознавания и анализа типа метода формирования *HTTP*-запроса;

2 — узел распознавания и анализа идентификатора ресурса;

3 — узел распознавания и анализа параметров доступа к ресурсу;

4 — узел распознавания и анализа версии *HTTP*-протокола;

5 — узел распознавания и анализа заголовков *HTTP*-запроса.

Для выполнения семантических операций в процессе работы конечного автомата используются следующие служебные переменные[9] [9]:

S_{method} — одномерный строковый массив, элементы которого содержат символьные идентификаторы разрешенных методов формирования *HTTP*-запросов;

L_{URL} — числовая переменная, определяющая максимальную длину идентификатора ресурса *web*-сервера;

S_{URL} — одномерный строковый массив, элементы которого содержат идентификаторы ресурсов, хранящихся на *web*-сервере;

L_{Nquery} — числовая переменная, определяющая максимальное количество параметров доступа к ресурсу *web*-сервера;

[8] URL: https://www.ietf.org/rfc/rfc2616.txt

[9] Кудрявцев В.Б., Алешин С. В., Подколзин А. С. Теория автоматов : учебник. М. : Юрайт, 2018. 320 с.

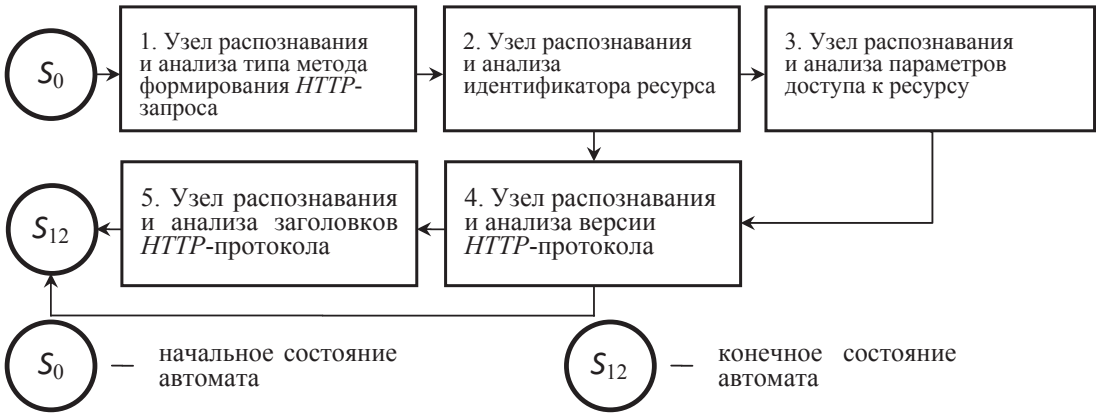

Рис. 2. Архитектура конечного автомата

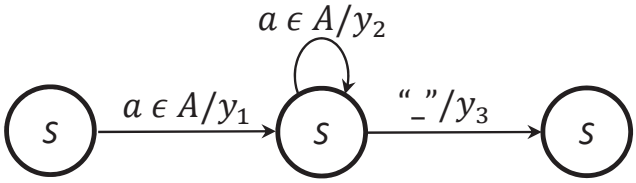

Рис. 3. Графовая модель узла распознавания и анализа типа метода формирования HTTP-запроса

$L_{VarLength}$ — числовая переменная, определяющая максимальную длину строкового имени параметра доступа к ресурсу *web*-сервера и имени заголовка *HTTP*-запроса;

$L_{ValLength}$ — числовая переменная, определяющая максимальную длину строкового значения параметра доступа к ресурсу *web*-сервера и значения заголовка *HTTP*-запроса;

$L_{NHeaders}$ — числовая переменная, определяющая максимальное количество заголовков в *HTTP*-запросе;

$S_{Versions}$ — одномерный строковый массив, содержащий номера версий протокола *HTTP*, которые могут обрабатываться защищаемым web-сервером;

$S_{Headers}$ — одномерный строковый массив, содержащий допустимые символьные имена заголовков *HTTP*-запроса, которые могут обрабатываться *web*-сервером;

Z — строковая переменная, предназначенная для временного хранения фрагментов анализируемого HTTP-запроса;

i, j ,k — числовые переменные, которые используются в качестве счётчиков.

Значения переменных Z, i, j, k формируются в процессе работы конечного автомата AV_{http}, а значения переменных L_{Nquery}, L_{URL}, $L_{VarLength}$, $L_{NHeaders}$, $S_{Versions}$, $S_{Headers}$ должны задаваться оператором перед началом работы автомата, с учётом требований стандартов *RFC* и специфики используемого ПО *web*-сервера. Для наглядности графового отображения[10] [3] блоков конечного автомата AV_{http} введём следующие обозначения: A — множество буквенных символов английского алфавита; N — множество, включающее в себя числовые символы от «0» до «9», символы «.», «#», «?», «/» и «%», а также символ подчеркивания; *NOP* — семантический оператор, не выполняющий никаких действий; «_» — пробельный символ; «*CRLF*» — символ, обозначающий возврат и перевод каретки на новую строку.

Описание условий перехода и семантические операторы, которые выполняются при каждом из возможных переходов в каждого узле конечного автомата AV_{http} (см. рис. 2), подробно представлены в Интернете[11] и соответствующих версиях *HTTP*-протокола.

Узел распознавания и анализа типа метода формирования HTTP-запроса первым начинает обработку входных символов, поступающих на вход автомата . Узел обеспечивает проверку того, что анализируемый *HTTP*-запрос сформирован на основе одного из методов, идентификаторы которых содержатся в переменной S_{method}. Графовая модель [10, 15] узла показана на рис. 3.

В первом блоке конечного автомата AV_{http} определено три состояния: $s_0, s_1, s_2 \in S$ и три семантических оператора: $y_2, y_3 \in Y$, которые выполняются при переходе автомата из одного состояния в другое. При условии перехода первого блока автомата AV_{http} в состояние s_2 обработка входных символов осуществляется узлом распознавания и анализа идентификатора ресурса.

[10] Гайдук А.Р., Плаксиенко Е.А. Анализ и аналитический синтез цифровых систем управления : учеб. пособие. М. : Лань, 2018. 272 с.

[11] URL: https://www.ietf.org/rfc/rfc2616.txt

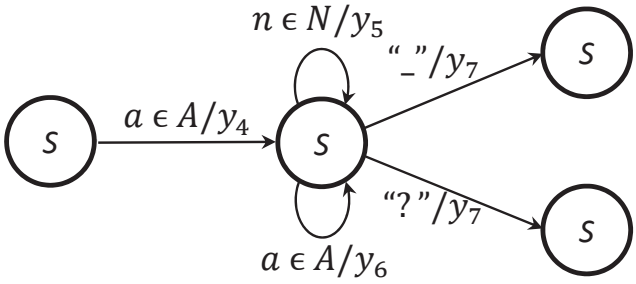

Рис. 4. Графовая модель распознавания и анализа идентификатора ресурса

Узел распознавания и анализа идентификатора ресурса предназначен для выделения из текста *HTTP*-запроса значения адреса ресурса и проверки его длины. Длина идентификатора ресурса, содержащегося в анализируемом *HTTP*-запросе, не должна превышать значения переменной L_{URL}. В процессе своей работы автомат узла также проверяет, что *HTTP*-запрос направлен одному из существующих ресурсов *web*-сервера, определённых в переменной. Графовая модель данного узла показана на рис. 4.

Во втором узле конечного автомата AV_{http} определено четыре состояния: $s_2, s_3, s_4, s_7 \in S$ и четыре семантических оператора: $y_4, y_5, y_6, y_7 \in Y$, которые выполняются при переходе автомата из одного состояние в другое.

Если второй узел автомата AV_{http} переходит в состояние s_4, то это означает, что в HTTP-запросе, кроме идентификатора ресурса, также содержатся параметры доступа, обработка которых осуществляется узлом распознавания и анализа параметров доступа к ресурсу. Переход автомата в состояние s_5 означает, что вслед за идентификатором ресурса сразу следует версия протокола *HTTP*, значение которой обрабатывается четвёртым узлом автомата AV_{http}.

Третий *узел распознавания и анализа параметров доступа к ресурсам web*-сервера выполняет следующие функции:

– проверку строковой длины имён и значений параметров доступа к ресурсам *web*-сервера. Максимальная длина имени параметра и его значения не должна превышать значений, определённых в переменных $L_{VarLength}$ и $L_{ValLength}$ соответственно;
– контроль числа параметров доступа, присутствующих в *HTTP*-запросе. Количество параметров не должно превышать значения, указанного в переменной L_{Nquery}.

Графовая модель узла распознавания и анализа параметров доступа показана на рис. 5.

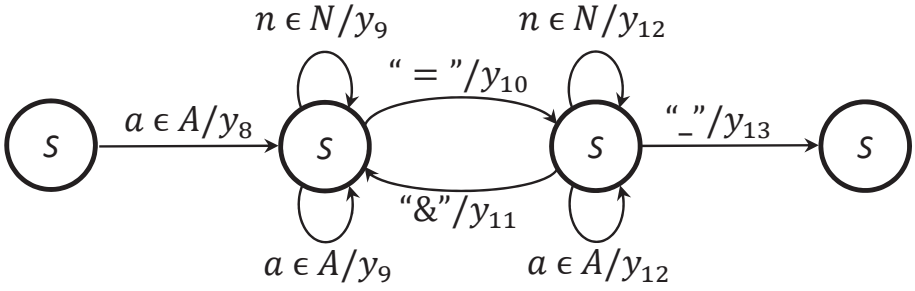

Рис. 5. Графовая модель узла распознавания и анализа параметров доступа

При условии, что третий узел автомата AV_{http} переходит в состояние s_7, автомат начинает обработку номера версии протокола, определённой в заголовке *HTTP*-запроса.

Четвёртый узел конечного автомата распознавания и анализа заголовков *HTTP*-протокола предназначен для проверки корректности номера версии, который указан в анализируемом *HTTP*-запросе. Номер версии считается корректным, если версия протокола, указанная в анализируемом *HTTP*-запросе, совпадает с одним из элементов строкового массива $S_{Versions}$. Графовая модель узла распознавания и анализа версии *HTTP*-протокола показана на рис. 6.

При условии, что четвёртый узел автомата AV_{http} переходит в состояние s_9, автомат начинает обработку оставшейся части *HTTP*-запроса.

Пятый узел конечного автомата AV_{http} (*узел распознавания и анализа заголовков HTTP-запроса*) предназначен для проверки длины имён и значений заголовков, содержащихся в *HTTP*-запросе. Блок проверяет, что количество заголовков *HTTP*-запроса не превышает значение переменной $L_{NHeaders}$, строковая длина имени каждого из параметров не превышает $L_{VarLength}$, а строковая длина значения параметра не превышает $L_{ValLength}$. Узел также обеспечивает проверку того, что в *HTTP*-запросе присутствуют

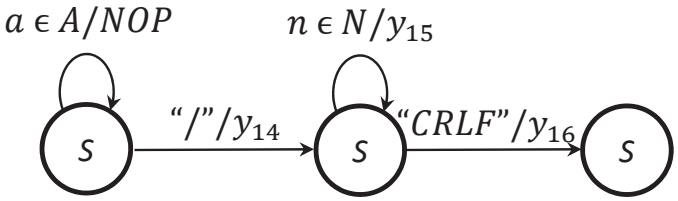

Рис. 6. Графовая модель узла распознавания и анализа версии HTTP-протокола

только те заголовки, которые определены в переменной $S_{Headers}$. Графовая модель узла распознавания и анализа параметров *HTTP*-запроса показана на рис. 7.

Если последний узел автомата переходит в состояние S_{12}, то это означает, что анализируемый *HTTP*-запрос не представляет опасности для *web*-сервера и не является частью сетевой атаки.

Обобщённая структура конечного автомата AV_{http}, который используется для анализа *HTTP*-запросов, показана на рис. 8.

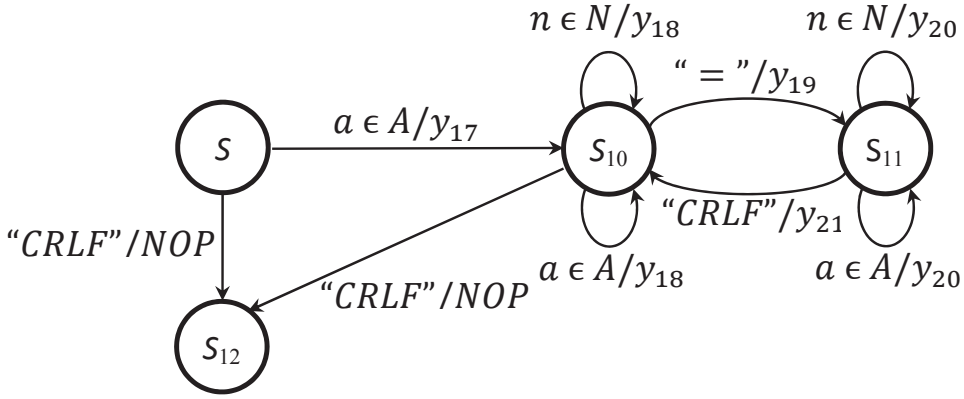

Рис. 7. Графовая модель узла распознавания и анализа параметров HTTP-запроса

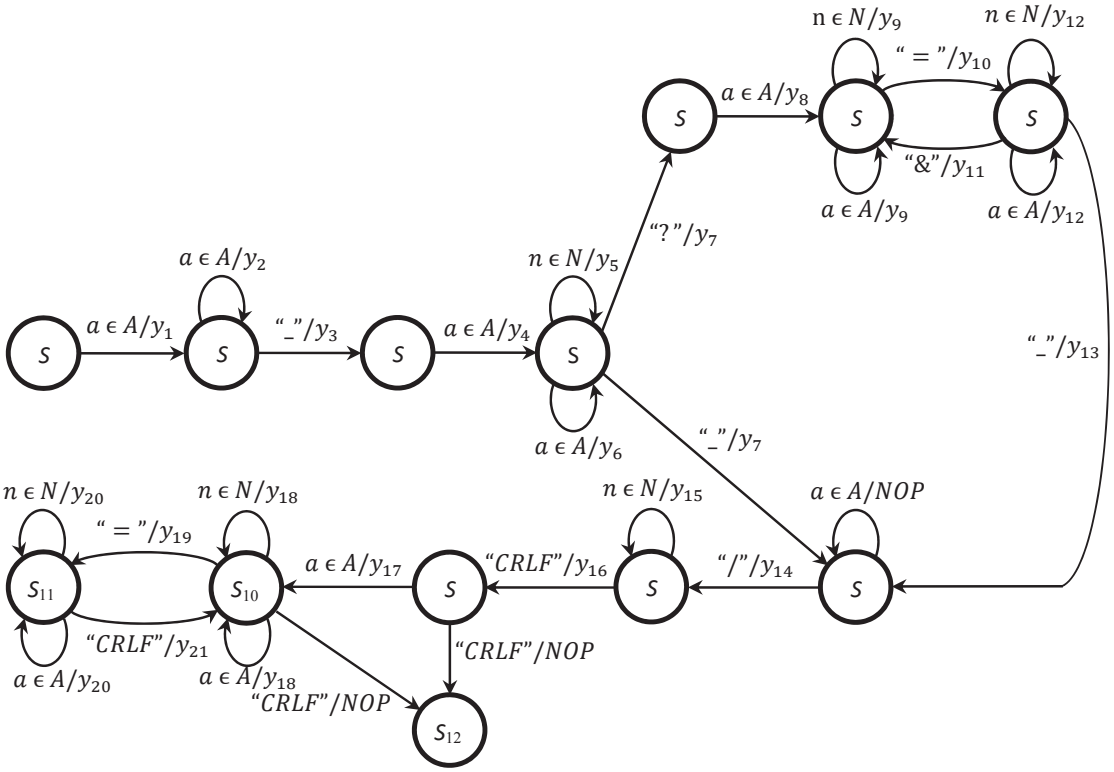

Рис. 8. Обобщенная структура конечного автомата AV_{http}, реализующего разработанную поведенческую модель процесса выявления атак на ресурсы web-серверов

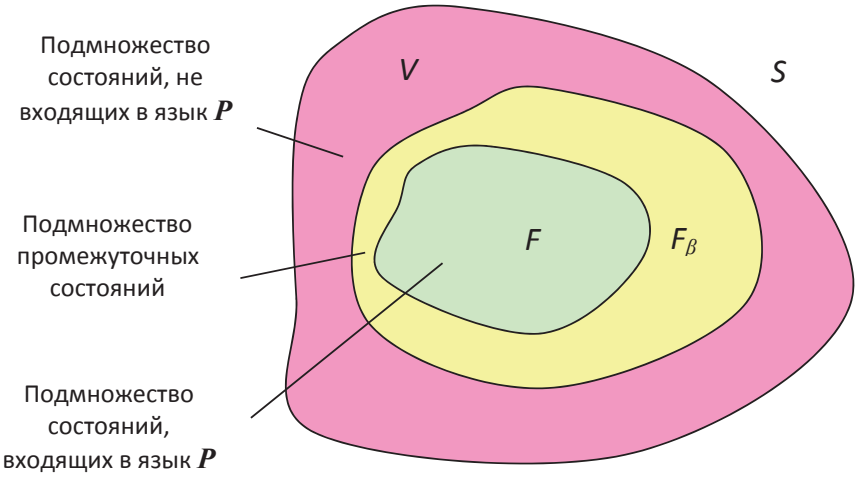

Рис. 9. Множество состояний конечного автомата

Рассмотренный подход к выявлению информационных атак на web-серверы путём анализа поступающих *HTTP*-запросов может быть использован для построения моделей защиты узлов других типов [12]. В этом случае должны подвергаться анализу запросы, сформированные на основе тех протоколов, по которым осуществляется взаимодействие с узлами автоматизированных систем передачи данных (АСПД). Так, например, для защиты почтовых серверов должны анализироваться запросы протоколов *SMTP (Simple Mail Transfer Protocol)* и POP*3 (Post Office Protocol Version 3)*, а для защиты файловых серверов — запросы протокола *FTP* (*File Transfer Protocol*).

Определение времени обнаружения информационной атаки

Многообразие протоколов, осуществляющих взаимодействие с элементами и узлами АСПД, в ряде случаев приводит к неоправданным задержкам обработки поступающих запросов[12] [5] и выдачи *незапланированного результата* (НЗР). Однозначно судить о причинах НЗР, который был сформирован web-сервером, без проведения дополнительных исследований не представляется возможным. Это могут быть как информационная атака, предполагающая «бесконечный цикл», так и ошибки программного обеспечения, алгоритмические сбои и др. Исходя из этого, целесообразно определить максимальное время обработки запроса, т. е. включить в его сигнатуру, наряду со временем инициирования, допустимое время его обработки, которое должно быть намного меньше выполнения деструктивных функций предполагаемой возможной информационной атаки заданного класса.

Рассмотрим процесс функционирования КА как дискретный марковский случайный процесс с непрерывным временем[13], состояния которого составляют множество $S = \{s_0, s_1, \ldots, s_n\}$. Из множества состояний S выделяется некоторое подмножество состояний $F = \{s_l, s_{l+1}, \ldots, s_n\}$, $F \subset S$, которое не является замкнутым и, в свою очередь, не содержит в себе замкнутых подмножеств (рис. 9), а также подмножество F_β, являющееся промежуточным между множествами $V = (S - F)$ и F. В общем случае подмножество F_β может быть пустым, замкнутым и содержать замкнутые подмножества. «Физически» это означает, *во-первых* (когда подмножество пустое), мгновенный переход из подмножества F в подмножество V (нет промежуточных состояний), а *во-вторых* (в остальных случаях), переход в подмножество V запрещен, что на практике не всегда выполнимо.

Другими словами, если известно, что в какой-то момент $t = 0$ КА находился в одном из состояний $s_i \in F$, то при $t \to \infty$ процесс хотя бы один раз перейдет из подмножества состояний F в подмножество состояний $V = (S - F)$ $(V \subset S)$, которое не является пустым: $\lim_{t \to \infty} p_f(t) = 0$, где $p_f(t)$ — вероятность непрерывного пребывания системы в момент времени t в состояниях подмножества F $[p_f(0) = 1]$. Следовательно, в составе подмножества состояний F нет отдельных состояний или группы состояний без выхода. Состояния $(s_0, s_1, \ldots, s_{l-1})$ составляют подмножество $V = S - F$, а состояния $(s_l, \ldots, s_n)$ — множество $F = S - V$[14].

Известно, что в момент $t = 0$ дискретный марковский случайный процесс находился в подмножестве состояний *F*,

$$\sum_{i=1}^{n} \tilde{p}_i(0) = 1. \quad (1)$$

[12] Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы : учебник. СПб. : ИД «Питер», 2010. 944 с.

[13] Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и её инженерные приложения. 4-е изд. стер. М. : Высш. шк., 2007. 479 с.; Гайдук А.Р., Плаксиенко Е.А. Анализ и аналитический синтез цифровых систем управления : учеб. пособие. М. : Лань, 2018. 272 с.

[14] См.: Тараканов К.В., Овчаров Л.А., Тырышкин А.Н. Аналитические методы исследования систем. М. : Сов. радио, 1974. 240 с.

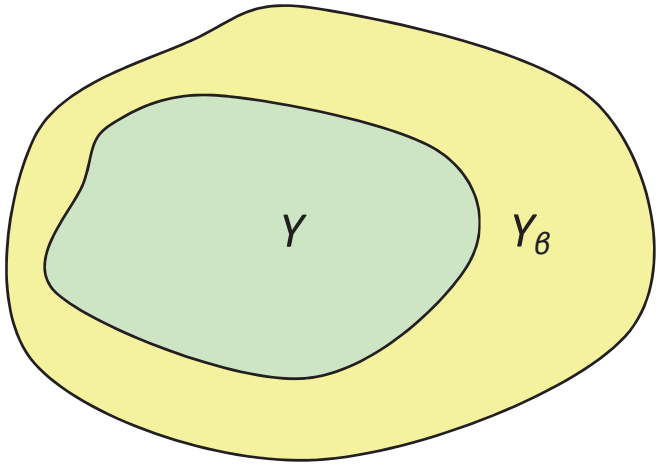

Рис. 10. Преобразованное состояние конечного автомата

Знак ~ над обозначениями вероятностей поставлен для того, чтобы отличить эти вероятности от обозначения вероятностей пребывания КА в любом состоянии s, принадлежащем множеству S.

Обозначим T случайную величину — время процесса обработки запроса по состояниям подмножества F до первого выхода из этого подмножества. Ввиду того, что само подмножество состояний F не является замкнутым и не содержит в себе замкнутых подмножеств, процесс при $t \to \infty$ может покинуть подмножество состояний F. В рассматриваемом случае случайное время T отсчитывается от момента $t = 0$.

Из множества состояний $V = S - F$ выделим подмножество состояний F_β $\{s_k,\ldots, s_{l-1}\}$ $(F_\beta \subset V)$. Не исключается и случай, когда $F_\beta = V$ (в этом случае $k = 0$). К состояниям подмножества $(F_\beta \subset V)$ отнесем лишь те, в которые возможен непосредственный переход из состояний подмножества F в состояния подмножества $V = S - F$, т. е. для любого состояния $s_j \in F_\beta$ найдется хотя бы одно такое состояние $s_i \in F$, что $L(s_i, s_j) = 1$, где L — маршрут из s_i в s_j.

Подмножество состояний F_β является «входными воротами» подмножества состояний V, через которые процесс функционирования переходит из подмножества состояний F в подмножество состояний V. Другими словами, к состояниям $(s_k,\ldots,s_{l-1})$, которые составляют подмножество F_β, отнесем лишь те состояния подмножества $V = S - F$, для которых выполняется условие:

$$\lambda_{ij}(t) \neq 0,\ (i=l,\ l+1,\ldots,\ n;\ j=0,\ 1,\ \ldots,\ l-1;\ t>0). \quad (2)$$

Назовем подмножество F_β β-окрестностью подмножества F. Тогда время T «блуждания» процесса по состояниям подмножества F до первого выхода из него равно времени, которое отсчитывается от начала «блуждания» $(t=0)$ до первого попадания процесса в β-окрестность подмножества F, т. е. в одно из состояний подмножества F_β.

Очевидно, что закон распределения случайной величины T не изменится, если все состояния множества F_β сделать поглощающими (концевыми). Следовательно, при нахождении закона распределения случайной величины T можно ограничиться рассмотрением процесса блуждания системы по преобразованным состояниям множества $F + F_\beta$. Преобразование состоит в том, что подмножество F_β образуется только из поглощающих состояний.

Чтобы состояния подмножества $F_\beta = \{s_k,\ldots,s_{l-1}\}$ были поглощающими, достаточно положить

$$\lambda_{ji}(t) \equiv 0 \quad (3)$$

для всех $j = k, \ldots, l - 1$. В этом случае выход из подмножества состояний F_β будет невозможен.

Таким образом, для определения закона распределения случайной величины T достаточно рассмотреть процесс «блуждания» по преобразованным состояниям подмножества $F + F_\beta$, при этом все состояния подмножества F_β состоят только из поглощающих состояний (рис. 10). Это утверждение равносильно тому, что рассматривается преобразованный подграф состояний подмножества $F + F_\beta$. При этом все ребра, выходящие из вершин графа, составляющих подмножество состояний F_β, исключаются (преобразуются). Преобразование сводится к тому, что вершины $(s_k,\ldots,s_{l-1})$ не имеют выходящих ребер.

Функция распределения случайной величины T (по определению) равна вероятности того, что к моменту времени t $(t>0)$ процесс уже покинет состояния, образующие множество F, и, следовательно, попадёт в состояния, образующие подмножество F_β, так как в преобразованном подмножестве состояний $F + F_\beta$ он (процесс) никуда (кроме подмножества состояний F_β) в конце концов попасть не может. Ввиду того, что подмножество состояний F_β состоит только из поглощающих состояний, процесс, попав однажды в одно из состояний F_β, так там и останется.

Следовательно, функция распределения времени T равна вероятности того, что к моменту времени t процесс «блуждания» окажется в одном из состояний, принадлежащих подмножеству F_β для преобразованного подмножества состояний $F + F_\beta$:

$$F(t) = \sum_{s \in F_\beta} \tilde{p}_s(t),$$

$$F(t) = \sum_{j=k}^{l-1} \tilde{p}_j(t), \quad (4)$$

где индекс суммирования распространяется на все состояния подмножества F_β (β-окрестность подмножества F).

Найдем плотность распределения случайной величины T:

$$f(t) = \frac{d}{dt} F(t),$$

$$f(t) = \sum_{j=k}^{l-1} \dot{\tilde{p}}_j(t). \quad (5)$$

С другой стороны, на основании общего правила составления системы дифференциальных уравнений для вероятностей состояний с учетом (3) имеем

$$\dot{\tilde{p}}_j(t) = \sum_{i=l}^{n} \lambda_{ij}(t) \tilde{p}_i(t), \ (j = k, k+1, \ldots, l-1) \quad (6)$$

Таким образом, плотность распределения случайной величины T можно найти из выражения

$$f(t) = \sum_{j=k}^{l-1} \sum_{i=l}^{n} \lambda_{ij}(t) \tilde{p}_i(t). \quad (7)$$

Для отыскания вероятностей $\tilde{p}_i(t)$ достаточно проинтегрировать систему уравнений для вероятностей пребывания процесса в состоянии подмножества F с учетом того, что переход из подмножества состояний F возможен только в подмножество состояний F_β, а последнее подмножество состоит из одних поглощающих состояний

$$\dot{\tilde{p}}_i(t) = -\sum_{h=l}^{n} \lambda_{ih}(t) \tilde{p}_i(t) - \sum_{h=k}^{l-1} \lambda_{ih}(t) \tilde{p}_i + \\ + \sum_{h=l}^{n} \lambda_{hi}(t) \tilde{p}_h(t), \quad (8)$$

где $i = l, l+1, \ldots, n$.

Начальными условиями для этой системы дифференциальных уравнений являются условия (1).

Итак, для определения закона распределения времени «блуждания» процесса в незамкнутом подмножестве состояний F до первого выхода за пределы этого подмножества достаточно проинтегрировать систему дифференциальных уравнений для вероятностей состояний (9) при начальных условиях (1).

Очевидно, что таким образом можно решать задачу для любого дискретного марковского случайного процесса с непрерывным временем, для которого подмножество состояний F не является замкнутым и не содержит замкнутых подмножеств.

Иногда существует необходимость рассмотрения и более жесткого условия, состоящего в том, что математическое ожидание времени T пребывания в подмножестве состояний F должно быть конечным. В этом случае должно выполняться следующее неравенство[15]:

$$\lim_{t \to \infty} \int_0^t [1 - \sum_{j=k}^{l-1} \tilde{p}_j(\tau)] d\tau = \\ = \lim_{t \to \infty} \int_0^t [1 - \sum_{j=k}^{l-1} \sum_{i=l}^{\infty} \lambda_{ij}(\xi) p_i(\xi) d\xi] d\tau, \quad (9)$$

$$\lim_{t \to \infty} \int_0^t [1 - \sum_{j=k}^{l-1} \sum_{i=l}^{\infty} \lambda_{ij}(\xi) p_i(\xi) d\xi] d\tau < \infty.$$

При этом также возможен случай, когда подмножество состояний F_β является бесконечным. Даже когда незамкнутое подмножество состояний F является конечным и для любого t выполняется неравенство (2), равенство (9) может не выполняться. Поэтому полученный закон распределения времени в заданном подмножестве состояний конечного автомата необходимо проверять, чтобы выяснить, выполняется ли условие (9). Вместе с тем он позволяет получить приближенную оценку, удовлетворяющую решению общей задачи исследования.

Заключение

Современные вычислительные средства и построенные на их основе компьютерные сети различного назначения должны обладать надежной, своевременной, актуальной и адекватной информационной защитой [7, 11]. Практика показывает, что ущерб от нарушений информационной безопасности может привести к крупным финансовым потерям и даже краху компании, он растет из года в год, и отнюдь не линейно [4]. Исходя из этого, вопросы обнаружения информационных атак на основе формирования сетевых запросов требуют научно обоснованного решения. Математической основой разработанной модели аппаратно-программного комплекса является теория конечных автоматов. При этом обязательное условие — учет времени обработки поступающего запроса и времени его инициализации.

Перспективным направлением является создание интеллектуальных аппаратно-программных комплексов, в основу которых положен принцип структурной организации высокоорганизованных материй (например, аппарат теории нейронных сетей) [12]. Однако в этом случае возникает другая проблема — увеличение времени обработки сетевого запроса (при существующих в настоящее время вычислительных средствах), оказывающее непосредственное влияние на комплексные показатели

[15] Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и её инженерные приложения. 4-е изд. стер. М. : Высш. шк., 2007. 479 с.

надежности (коэффициенты готовности, технического использования, оперативной готовности) АСПД в целом. Разумное соотношение этих параметров — сложная многокритериальная задача поиска рационального решения, обеспечивающих баланс требуемой защищённости и высоких комплексных показателей надежности.

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. Анин Б.Ю. Защита компьютерной информации. СПб. : БХВ-Санкт-Петербург, 2016. 384 с.
2. Гончаров В.В., Гончаров А.В. Методика обоснования рационального варианта проверки телекоммуникационных систем и сетей // Правовая информатика. 2022. № 4. С. 39—48. DOI: 10.21681/1994-1404-2022-4-39-48 .
3. Додонов А.Г., Ландэ Д.В. Живучесть информационных систем. К. : Наукова думка, 2011. 256 с.
4. Кульба В.В., Ковалевский С.С., Шелков А.Б. Достоверность и сохранность информации в АСУ. М. : Синтег, 2004. 496 с.
5. Куроуз Дж., Росс К. Компьютерные сети. Нисходящий подход. М. : Эксмо, 2016. 912 с.
6. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
7. Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3—7.
8. Ловцов Д.А. Информационная безопасность и нетрадиционные угрозы // Федеральный справочник. Т. 8. Оборонно-промышленный комплекс России. М. : Центр стратег. исследований, 2013. С. 507—512.
9. Низамутдинов М.Ф. Тактика защиты и нападения на web-приложения. СПб. : БХВ-Петербург, 2005. 480 с.
10. Оре О. Графы и их применение. М. : Ленанд, 2015. 208 с.
11. Системный анализ и аналитические исследования: руководство для профессиональных аналитиков / А.И. Ракитов, Д.А. Бондяев, И.Б. Романов, С.В. Егерев, А.Ю. Щербаков. Под. ред. А.И. Ракитова. М. : РГГУ, 2009. 448 с.
12. Сети следующего поколения NGN / Под ред. А.В. Рослякова. М. : Эко-Трендз, 2008. 420 с.
13. Таненбаум Э.С., Уэзеролл Д. Компьютерные сети. СПб. : ИД «Питер», 2022. 900 с.
14. Фленов М.Е. Web-сервер глазами хакера. СПб. : БХВ-Санкт-Петербург, 2021. 257 с.
15. Харари Ф. Теория графов. М. : Ленанд, 2018. 304 с.

INFORMATION ATTACK DETECTION MODELLING BASED ON THE FINITE AUTOMATA THEORY

Vladimir Goncharov, *Dr.Sc. (Technology), Professor, Honoured Figure of Higher School of the Russian Federation, Head of the Department of Mathematics of the Peter the Great Military Academy, Moscow, Russian Federation.*
E-mail: v_v_goncharov@mail.ru

Aleksandr Goncharov, *external Ph.D. student at the Peter the Great Military Academy, Moscow, Russian Federation.*
E-mail: dinozavp@inbox.ru

Ol'ga Mishenina, *Ph.D. (Paedagogy), Associate Professor, Professor at the Department of Mathematics of the Peter the Great Military Academy, Moscow, Russian Federation.*
E-mail: o.v.mishenina@gmail.com

Keywords: *corporate network, network technologies, network request, information attack, information security, finite automaton, element, set, elements subset, graph model, random variable, random variable's distribution and density function.*

Abstract

Purpose of the paper: improving the research and methodological foundations for raising the quality of basic network interaction protocols security control in corporate network nodes.

Methods of study: system analysis and the mathematical apparatus for generation and recognition of 'regularly built' chains forming regular sets defined by expressions making it possible to build a finite automaton allowing to precisely repeat the chain of the corresponding regular set.

Study findings: a model was developed describing the basic computer network nodes interaction protocol using an automaton language P each element of which corresponds to a basic network request and can be correctly processed by the hard- and software system of the network. The language P is described using finite recognising automata detecting potentially dangerous requests whose elements do not comply with the standards described based on this language. A conclusion is justified that including the request initialisation and maximum permitted processing time in the request signature will make it possible to considerably reduce the possibilities for carrying out computer attacks of this type.

The results obtained are the base for developing appropriate efficient information and mathematical support for the hard- and software system for complex computer networks security.

References

1. Anin B.Iu. Zashchita komp'iuternoi informatsii. SPb. : BKhV-Sankt-Peterburg, 2016. 384 pp.
2. Goncharov V.V., Goncharov A.V. Metodika obosnovaniia ratsional'nogo varianta proverki telekommunikatsionnykh sistem i setei. Pravovaia informatika, 2022, No. 4, pp. 39—48. DOI: 10.21681/1994-1404-2022-4-39-48 .
3. Dodonov A.G., Lande D.V. Zhivuchest' informatsionnykh sistem. K. : Naukova dumka, 2011. 256 pp.
4. Kul'ba V.V., Kovalevskii S.S., Shelkov A.B. Dostovernost' i sokhrannost' informatsii v ASU. M. : Sinteg, 2004. 496 pp.
5. Kurouz Dzh., Ross K. Komp'iuternye seti. Niskhodiashchii podkhod. M. : Eksmo, 2016. 912 pp.
6. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
7. Lovtsov D.A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh. Informatsionnoe pravo, 2012, No. 4, pp. 3—7.
8. Lovtsov D.A. Informatsionnaia bezopasnost' i netraditsionnye ugrozy. Federal'nyi spravochnik, t. 8. Oboronno-promyshlennyi kompleks Rossii. M. : Tsentr strateg. issledovanii, 2013, pp. 507—512.
9. Nizamutdinov M.F. Taktika zashchity i napadeniia na web-prilozheniia. SPb. : BKhV-Peterburg, 2005. 480 pp.
10. Ore O. Grafy i ikh primenenie. M. : Lenand, 2015. 208 pp.
11. Sistemnyi analiz i analiticheskie issledovaniia: rukovodstvo dlia professional'nykh analitikov. A.I. Rakitov, D.A. Bondiaev, I.B. Romanov, S.V. Egerev, A.Iu. Shcherbakov. Pod. red. A.I. Rakitova. M. : RGGU, 2009. 448 pp.
12. Seti sleduiushchego pokoleniia NGN. Pod red. A.V. Rosliakova. M. : Eko-Trendz, 2008. 420 pp.
13. Tanenbaum E.S., Uezeroll D. Komp'iuternye seti. SPb. : ID "Piter", 2022. 900 pp.
14. Flenov M.E. Web-server glazami khakera. SPb. : BKhV-Sankt-Peterburg, 2021. 257 pp.
15. Kharari F. Teoriia grafov. M. : Lenand, 2018. 304 pp.

СТРУКТУРИЗАЦИЯ СИСТЕМ МОНИТОРИНГА ИНФОРМАЦИОННЫХ РЕСУРСОВ

Бурый А.С.[1]

Ключевые слова: *мониторинг, информационно-коммуникационная технология, предметная область, интеграция данных и знаний, наблюдаемость данных, классификаторы.*

Аннотация

Цель работы: совершенствование научной и методической базы при разработке концепции формирования элементов информационной среды для предметной области исследования путем мониторинга информационных ресурсов для поддержания актуальности объектов правоотношений.

Методы: комплексное использование системного и сравнительного анализа, концептуально-логическое моделирование, формально-логическая разработка и обоснование структур построения распределенных информационных систем.

Результаты: предложен концептуальный подход к формированию объектов классификации на основе мониторинга информационных ресурсов заданной предметной области в рамках государственных информационных систем; исследовано взаимодействие киберфизической и социальной среды на уровнях переработки данных, информационного анализа и выявления знаний в целях получения интегрированных информационных структур и выявления синергетических свойств информационных систем; сформулирован тезис о тенденции сближения киберфизических и социальных процессов, для структурирования и анализа которых целесообразно использовать проблемно-ориентированный вариант комплексного «информационно-кибернетически-синергетического» подхода (ИКС-подхода) в парадигме технологий цифровой трансформации.

DOI: 10.21681/1994-1404-2023-1-52-61

Введение

Набирающая темпы цифровая трансформация (ЦТ) полностью форматирует облик современного общества. В основе ЦТ лежат четыре прорывных *технологии*: облачные вычисления, большие данные, Интернет вещей и искусственный интеллект (ИИ). Возможность получения больших объемов данных заставила по-новому посмотреть на их применение, хранение, переработку. Это тесно связано с разработкой и внедрением новых методов и алгоритмов на основе процедур ИИ в системах поддержки принятия решений, поиска информации [13], государственных информационных системах (ИС) [5], многочисленных автоматизированных информационных системах (АИС) городских служб [8, 9] и др. Традиционно каждая АИС опирается на разработанную базу данных и знаний (БДЗ). Однако в условиях интенсивного информационного взаимодействия в масштабе городской инфраструктуры возникает проблема интеграции ряда ИС, построенных под конкретные предметные области (здравоохранение, образование, науку, транспорт и др.).

Масштабная автоматизация различных сфер деятельности как в рамках определенных *предметных областей исследования* (ПОИ), так и в интегрированных сущностях требует формирования соответствующих БДЗ, что представляет собой довольно трудоемкий процесс, требующий определенных экспертных навыков [11], разработки моделей интеграции данных и систем управления данными [13].

Интеграция данных и знаний представляет собой наиболее динамично развивающееся направление современных информационных и коммуникационных технологий (ИКТ), связанное с обеспечением интероперабельности АИС [3, 20].

Результатом интеграции могут выступать новые цифровые пространства научных знаний, требующие структуризации и формализации в соответствии с направленностью исследований [2]. Большинство информационных процессов, технологий, коммуникаций, необходимых ресурсов, а, следовательно, и БДЗ, ориентированы на определенные ПОИ и находятся в постоянном развитии, связанном с подключением новых

[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

данных, разработкой дополнительных сервисных приложений, оптимизацией структуры и другими процессами. Повсеместное увлечение термином «умный» (город, дом, парковка, вещи и др.) не всегда оказывается уместным, так как автоматизация одной-двух функций в системе управления любого уровня лишь с большой долей условности позволяет отнести технологию в разряд «умной». Однако нельзя не упомянуть об активной тенденции в представлении инфосферы общества [16, 19] как *умного пространства* или некоторой киберфизической среды, в которой человеко-машинное взаимодействие благодаря развитию и внедрению ИКТ и технологий ИИ [22, 23] обеспечивает создание распределенных, хорошо скоординированных интеллектуальных экосистем[2].

Примером динамично развивающихся умных пространств являются умные города [8, 9], в которых на основе интеллектуальных технологических шаблонов формируется городская инфраструктура, деловые, образовательные, научные узлы (ядра, площадки, подсистемы) коммуникационной среды.

Обеспеченность АИС различного уровня согласованными стандартизированными данными является залогом эффективности ИКТ. С этой целью осуществляется мониторинг как технических систем, так и данных (измерительной информации при решении задач контроля и управления сложными динамическими объектами [17, 18, 24], организационно-техническими структурами городской среды [8, 9], нормативного и правового сопровождения в ряде областей социальной сферы [10, 15, 16] и др.).

Мониторинг в информационно-телекоммуникационной среде, учитывая возрастающую роль АИС и процессов ЦТ, актуален как никогда. При этом это не только своевременное оповещение о проблемах в сетевой инфраструктуре, но и получение прогнозных оценок о состоянии и качестве организации хранилищ данных [1, 14]. Усложнение объектов контроля, функционирование которых осуществляется часто в конфликтной среде, включая сетевые, противоборствующие и даже враждебные факторы, приводит к необходимости организации когнитивного мониторинга объектов, основанного на процедурах адаптации, методах самообучения, машинной перестройки моделей и интеллектуальной поддержки [14].

Предметной *целью* предлагаемого исследования является развитие концептуального подхода к формированию элементов информационной среды предметной области исследования, представляемой как объединение физического, кибернетического и социального пространства путем мониторинга информационных ресурсов с целью поддержания актуальности объектов правоотношений для поддержки действующих государственных АИС.

Киберфизический и социальный контекст данных

Для формирования понятийного пространства [7, 10] заданной предметной области исследования ключевым элементом является модель знаний, которая в существующих условиях ЦТ выступает связующим элементом между киберпространством (КП) — область $O_{\text{КП}}$ и социальным пространством (СП) — область $O_{\text{СП}}$. В КП осуществляется сбор данных, управление ресурсами, предоставление вычислительных услуг, например, в облачных сервисах [6]. Обработка данных/больших данных направлена на преобразование: данных в информацию, информации в знания, знаний в понимание (объяснение, прогноз) или мудрость [25].

Социальное пространство относится к человеческому обществу, полному мышления, познания, знаний и коллективного разума. Социальная сеть или платформа объединяет заинтересованных пользователей для осуществления социальной коммуникации, сотрудничества (взаимодействия).

Физическое пространство (ФП) или область $O_{\text{ФП}}$ представляет собой реальный мир, подлежащий изучению, мониторингу или контролю. Это физические объекты (устройства, оборудование) в виде первичных потенциальных источников данных, существующая информация (документы, книги, отчеты и др.), выступающая источником знаний, а также интерфейсное оборудование (датчики, регистраторы, контроллеры) для поддержки взаимодействия между КП и СП:

$$O_{\text{ФП}} : O_{\text{КП}} \leftrightarrows O_{\text{СП}}. \quad (1)$$

Киберфизические системы (КФС) являются основными источниками разнотипных данных, наряду с Интернетом вещей, высокоавтоматизированным транспортом, беспилотными воздушными судами, «умными» медицинскими устройствами и др.

На рис. 1 представлено взаимодействие киберфизической и социальной среды.

Для управления процессами взаимодействия и интеграции ИКТ, достижения согласованной координации данных, информации и знаний и надежной адаптации, ориентированной на максимизацию информационной эффективности, предлагается использовать методику «двунаправленного вычислительного моста» между указанными сферами, основанную на *пирамиде знаний* Р. Акоффа[3]. К традиционным уровням данных, информации, знаний и мудрости или понимания («Д-И-З-М») [25] добавлены три переходных уровня (2, 4, 6):

– уровень преобразования данных в информацию (на рис. 1 — уровень 2, инструментами которого являются методы и алгоритмы анализа данных для выявления скрытых данных — предпочтения

[2] URL: https://решение-верное.рф/Gartner-Top-10-Strategic-Technology-Trends-for-2019 (дата обращения: 12.11.2022).

[3] Ackoff R.L. From data to wisdom // Journal of Applied Systems Analysis. 1989. Vol. 16. P. 3—9.

Рис. 1. Взаимодействие киберфизической и социальной среды

покупателей, взаимосвязи различных видов данных и др. [28]);

– уровень 4 — преобразования информации в знания или генерация знаний (различная пользовательская информация);
– уровень 6 — преобразования знаний в понимание (мудрость) или генерация когнитивного качества (например, за счет осуществления протоколов взаимодействия между интеллектуальными продуктами и пользователями, включая при необходимости этапы обучения).

Оставшиеся уровни целевой функциональности «Д-И-З-М» соответствуют своим названиям и обеспечивают:

– сбор данных из разных пространств (уровень 1);
– обмен информацией между пространствами КП, СП, ФП и облегчение коммуникации (уровень 3);
– формирование когнитивных способностей и обмен знаниями (например, в интернет-среде; уровень 5);
– развитие когнитивных функций, позволяя интеллектуальным продуктам самостоятельно адаптироваться к изменению контекста, а также использования знаний для задач принятия решений (уровень 7).

Киберфизическую предметную область представим пятиуровневой структурой 5С (от *англ.* ***C****onnection,* ***C****onversion,* ***C****yber,* ***C****ognition,* ***C****onfiguration*) на рис. 1, где стрелками показаны взаимодействия между уровнями рассматриваемых моделей: пирамиды знаний и киберфизико-социальной системы (КФСС).

Относительно уровней архитектуры КФС типа 5С отметим следующее:

– на уровне У1 «коммуникационной среды» реализуются технологии на основе «умных» датчиков, которые обеспечивают включение регистрации или любых других исполнительных устройств по времени при обнаружении движения объектов контроля или срабатывании различных сенсоров (температурных или других датчиков контроля параметров окружающей среды);
– на уровне У2 «конверсии» производится анализ данных на основе глубокой аналитики, включая облачные вычислительные приложения, для задач контроля сроков службы оборудования, планирования обслуживания, управления ресурсами, самоопределения критических сроков и точек (например, для устранения аварийных ситуаций);
– на киберуровне У3 разрабатываются цифровые модели физических сущностей, которые совместно с системой двусторонних информационных связей с реальным объектом образуют понятие цифрового двойника (digital twin), применяемого как на этапе проектирования изделий, так и в ходе эксплуатации;
– на уровне У4 «самопознания» формируются результаты самоконтроля (самооценки), полученные в ходе диагностирования объекта, принятые самим объектом решения, а также возможные рекомендации по дальнейшему управлению, если обнаруженные нештатные ситуации не учтены в существующей конструкторской документации;
– на уровне У5 «самоконфигурации» реализуются интеллектуальные решения, принятые КФС автономно в ходе оптимизации своего состояния, исходя из целевых факторов применения КФС, на основе заложенного программного обеспечения и возможностей БДЗ.

Элементы социосферы представлены структурой КФСС в контексте социального производства [28]:

– на уровне «подключения» осуществляется сбор данных от возможных источников данных (Интернета всего — *IoE*, включая СП, ФП и КП);
– на уровне «конверсии» из разнородных данных (структурированных, полуструктурированных, неструктурированных), хранящихся в различных распределенных БДЗ, формируется полезная информация, используя соответствующую аналитику;
– на уровне «коммуникации» осуществляются коммуникации типа *P2P* (между людьми-пользователями, разработчиками, потребителями информации), *P2M* — человеко-машинные (социофизическое взаимодействие) и межмашинные — взаимодействие вида *M2M*, характерное для физического пространства;
– уровень «вычислений» является ядром структуры КФСС; вычисления относятся к процессам последовательных преобразований данных:

$$\text{УВ} := \text{данные} \rightarrow \text{информация} \rightarrow \text{знания}$$

и возникновения инсайтов[4] — новых знаний; на этом уровне особую роль играют облачные вычисления и аналитика данных, которые доступны практически для пользователей в большинстве случаев и позволяют решать широкий круг задач, включая диагностику, прогнозирование и текущее управление;
– уровень «познания» — это когнитивный уровень, отвечающий за обмен знаниями, которые после их генерации на вычислительном уровне используются как в социальном, так и физическом пространстве: в СП экспертные знания могут явиться причиной получения инсайтов, а в ФП автоматизация знаний позволяет интеллектуальным устройствам реализовывать свойства самоадаптации, самообучения, самостоятельного принятия решений; применительно к социальному и физическому пространству уровень познания играет роль Интернета мышления;
– уровень «конфигурации» — представляет собой управляющую и обратную связь вида (1) из КП в социальное и физическое пространство; цель этого уровня — преобразовать знания в *понимание* для принятия решений, включая задачи диагностирования, прогноза и предписывающей аналитики, представляющей собой объединение темпоральных данных с алгоритмами прогнозирования, используя вычислительные (компьютерные) науки[5] (информатику) и математику;
– уровень «коллективного интеллекта», где объединяются данные киберпространства, социопространства и физического пространства. В ФП решение принимается в соответствии с машинным интеллектом через Интернет интеллекта (*IoI* — *Internet of Intelligence*). При этом важную роль на этом уровне играют алгоритмы машинного обучения, эволюционного обучения, трансфертного обучения и многозадачного обучения.

Киберфизические системы соединяют киберпространство и физическое пространство, так как входящие в них физические датчики, регистраторы и другие устройства формируют массивы данных, которые на вычислительном уровне (в киберпространстве) используются для вычислений, мониторинга и управления (выработки управляющих решений) [9].

Пример — разработка эргатических систем под требуемую задачу, когда необходимо обеспечить оптимальные или рациональные показатели информационных, технических, программных признаков проектируемых объектов [18, 19, 24].

Цифровые аспекты правовой сферы

Доступная цифровая среда, удобство представления информации, связанное с оперативностью получения, преобразования и анализа данных, за счет управления оцифрованными административными процедурами, профилями клиентов, цифровой идентификацией, общими и конфиденциальными данными неизбежно подвергает каждую компанию (организацию) различным формам *киберрисков*. Здесь вступают в действие *цифровые правила*: работая в цифровой среде, управляя данными, необходимо предотвращать любые киберугрозы, выбирая цифровые решения, платформы или инструменты, соответствующие законодательству.

Правительство и регулирующие органы играют ключевую роль в поощрении предприятий к цифровой трансформации в рамках продвижения технологического развития организаций, могут способствовать инновациям, предоставляя правовые нормы, отражающие общественные ценности, такие как права людей и потребителей, обеспечивая защиту персональных данных и информации. Цифровые правила должны удовлетворять потребности пользователей, давая правильные указания по созданию надежной правовой базы, внушая доверие к внедрению новых технологий, которые должны обеспечивать[6]:
– защиту пользователей в случае ошибочного удаления их данных платформами;
– меры прозрачности для цифровых платформ, в том числе в отношении онлайн-рекламы и алгоритмов, используемых для рекомендации контента пользователям;
– новые стандарты для тщательного изучения того, как работают платформы, включая доступ исследователей к ключевым данным крупнейших

[4] Инсайт (от англ. insight — озарение) — это спонтанное и не имеющее ничего общего с прошлым опытом человека решение; свойство человеческого разума, помогающее умозрительно постигать целое.

[5] Вычислительные науки основаны на применении принципов информатики и программной инженерии для решения научных задач.

[6] Цифровое регулирование: правовые аспекты цифровой эпохи. URL: https://www.euronovategroup.com/digital-regulations-legal-aspects-of-the-digital-era/ (дата обращения: 17.12.2022).

платформ, чтобы понять и оценить возможные онлайн-риски;
- новые правила отслеживания бизнес-пользователей на онлайн-рынках для выявления продавцов нелегальных товаров или услуг;
- инновационный процесс сотрудничества между государственными органами для обеспечения эффективного правоприменения на едином рынке.

Следующим направлением исследования цифровой социальной сферы выступают *социальные сети*. В настоящее время правительства во всем мире становятся все более зависимыми от общественного мнения в отношении разработки и реализации социальной политики. Роль социальных сетей жизненно важна для этой новой тенденции [27].

Интеллектуальный мониторинг и контроль государственной политики с использованием социальных сетей и облачных вычислений весьма востребован в наши дни. Однако экспоненциальный рост использования платформ социальных сетей широкой общественностью дал правительству более широкое представление о том, как преодолеть эту давно назревавшую дилемму. Облачное электронное управление в настоящее время реализуется благодаря доступности ИТ-инфраструктуры и активному распространению современных методов переработки данных.

Методы аналитики социальных сетей включают следующие методы анализа данных [27]:
- описательный анализ дает статистику о количестве твитов (сообщений в Twitter) и новых пользователей, числе упоминаний (ссылок) вашего информационного ресурса, облаке слов и др., но надо учитывать, что это анализ только конкретной выборки данных, а не всей совокупности данных, из которой выборка взята;
- контент-анализ занимается получением смыслового содержания из данного текста, что достигается с помощью таких методов, как анализ настроений, эмоций, тематическое моделирование и др.;
- сетевой анализ позволяет идентифицировать различные сообщества и группы пользователей на основе их мнения об объекте (событии);
- геопространственный анализ связан с анализом на основе местоположения объекта (продукта, логистики, маркетинга).

Таблица 1

Сопоставление понятий наблюдаемости и мониторинга данных

Признак сравнения	Мониторинг (М)	Наблюдаемость (Н)
Определение	**Мониторинг** — это инструмент или техническое решение, позволяющее инженерам по данным отслеживать и понимать состояние своих систем. **М.** основан на сборе предопределенных наборов метрик или журналов.	**Наблюдаемость** — это инструмент или техническое решение, которое позволяет инженерам по данным активно отлаживать свою систему. **Н.** основана на изучении свойств и шаблонов, не определенных заранее.
Особенности процесса	**М.** является реактивным процессом, как ответ на обстоятельства.	**Н.** — проактивный процесс, когда известны модели обстоятельств и принимается решение по выбору оптимального варианта.
Инструменты относительно переработки данных	Инструменты **М.** настроены на сбор информации, большая часть которой оказывается фактически не востребованной; **М.** фокусируется на инфраструктуре и на точечных наблюдениях; данные, доступные благодаря **М.**, часто являются единственным ожидаемым результатом.	**Н.** активно собирает данные, чтобы сосредоточиться на том, что важно; например, на факторах, которые определяют операционные решения и действия; **Н.** фокусируется на приложениях, акцент делается на технологические процессы; **Н.** предполагает, что источники данных будут способствовать аналитическому процессу, который затем будет оптимально отображать состояние приложения или системы.
Преимущества наблюдаемости	**М.** устанавливает факт того или иного события (сбоя, нарушения).	**Н.** помогает понять, почему это произошло; - именно наблюдаемость данных позволяет проводить их мониторинг; - **Н.** позволяет поддерживать данные в актуальном состоянии; - полная или сквозная **Н.** позволяет организациям намного быстрее разобраться в проблемах работы приложений, включая облачные среды и микросервисы.
Перспективы развития	Когнитивный **М.** — использование обучаемых и самообучаемых методов и моделей, подстройка которых осуществляется из контекста объекта управления и ранее полученных результатов.	В условиях усложнения данных, вызванного развитием экосистем, перспективным является применение методов ИИ и машинного обучения, обеспечивая управляемость сложных динамических объектов, в том числе и при снижении качества данных.

Новые взгляды на данные

Растущие объемы данных, производимых в мире, которые, по некоторым оценкам, достигнут уровня 175 *Зеттабайт* в 2025 г.[7], сопровождаются и большими технологическими изменениями в способах хранения и обработки данных. Сегодня 80% обработки и анализа данных происходит в центрах обработки данных и централизованных вычислительных мощностях, а 20% — в интеллектуальных подключенных объектах.

Благодаря доступности вычислительных мощностей и развитию программной аналитики в новых направлениях науки о данных активно развивается, например, такое направление статистики, как разведочный анализ данных (*exploratory data analysis — EDA*) [4].

Для больших объемов данных актуальной становится организация поиска, интеграции, очистки и подготовки данных для анализа. Для описания программных процессов, которые обеспечивают отделение *критической* информации от *рутинной*, используется понятие «наблюдаемость данных».

Наблюдаемость данных — это новый уровень в современном стеке технологий обработки данных, обеспечивающий специалистам по работе с данными видимость, автоматизацию и оповещение о поврежденных данных (т. е. о дрейфе данных, повторяющихся значениях, повреждениях данных). Это способность понимать, оценивать и управлять состоянием данных, потребляемых различными технологиями на протяжении всего жизненного цикла данных, поэтому определяющими свойствами данных при этом являются их *актуальность*, *полнота*, *структурированность*, *распределенность*, *происхождение* или *принадлежность* к источнику данных.

Наблюдаемость как элемент (базовое свойство) системы управления выступает совместно со свойством *управляемости*, важнейшим условием информационно-технической функциональности объекта управления, в качестве которого обычно рассматриваются сложные динамические объекты [16, 17, 26]. В этом случае наблюдаемость характеризует наличие информационных связей между пространством состояний объекта и пространством изменений, т. е. формируемыми измерительными данными. Проблема наблюдаемости заключается не столько в получении внутреннего состояния из наблюдений, сколько в сборе «правильных» наблюдений[8].

В табл. 1 представлено сопоставление понятий наблюдаемости и мониторинга данных по выделенным признакам сравнения.

Основным направлением в развитии методов мониторинга и наблюдаемости данных должен стать подход, основанный на знаниях (см. рис. 1), как при разработке приложений на уровне модельно-алгоритмического или математического обеспечения задач управления, принятия решений, обработки знаний, распознавания образов, интеллектуального анализа данных, так и на уровне их программного обеспечения.

Система мониторинга информационно-правовой предметной области исследования

Поскольку цифровая трансформация — это непрерывный процесс, цифровые правила необходимо обновлять, вводить новые объекты правоотношений, появляющиеся в документах, в нормативных правовых актах, а на их основе — и в АИС различного уровня [5].

Для определения статуса системы, процесса, продукции, услуги проводится мониторинг[9] объектов с целью *управления качеством*. Мониторинг используется в тех случаях, когда при построении какого-либо процесса необходимо постоянно отслеживать происходящие в реальной предметной среде явления, с тем чтобы включать результаты текущих наблюдений в процесс управления.

На рис. 2 представлена структура взаимовлияния физического, социального и киберпространства. По мере развития информационно-коммуникационных технологий можно говорить об устойчивой тенденции к сближению этих пространств, т. е. о расширении совместной *Области 1*, для которой справедливо:

$$O_1 := O_{\text{ФП}} \cap O_{\text{КП}} \cap O_{\text{СП}},\ O_1 \neq \emptyset. \qquad (2)$$

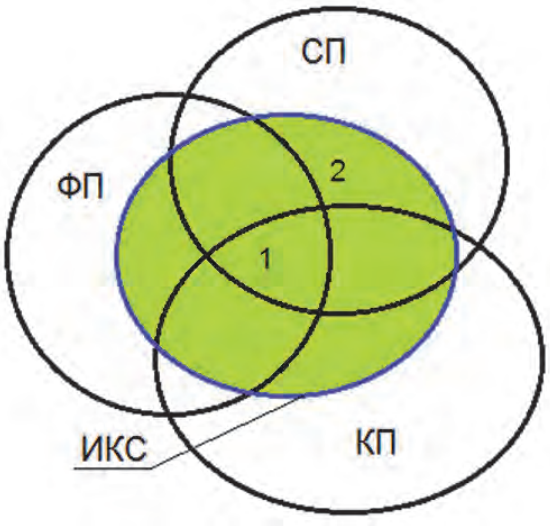

Рис. 2. Интегративная роль ИКС-подхода в объединении КП, ФП и СП

Скорость сближения указанных пространств во многом определяется уровнем развития ИКТ, которые обеспечивают *единое информационное пространство*, инфраструктуру которого, как и структу-

[7] URL: https://rspectr.com/novosti/ (дата обращения 19.12.2022)

[8] Bigelow S.J., Nolle T. What is observability? A beginner's guide. URL: https://www.techtarget.com/searchitoperations/definition/observability (дата обращения: 17.12.2022).

[9] ГОСТ Р ИСО 9000-2015. Системы менеджмента качества. Основные положения и словарь (п. 3.11.3). Введ. 2015-09-28.

рирование *Области 2* взаимодействия, целесообразно проводить на основе комплексного ИКС-подхода («информационно-кибернетического-синергетического») [8, 17—19].

Комплексный ИКС-подход может найти приложение при разработке стандартов комплексирования данных и знаний в ходе их интеграции в областях пересечения указанных на рис. 2 пространств. Так, с позиций информационного взаимодействия *Область 2* может ассоциироваться с технико-экономической информацией:

$$O_2 := O_{\text{КП}} \cap O_{\text{СП}}. \quad (3)$$

Рассмотрим задачу мониторинга информационного пространства с целью поиска объектов *технико-экономической и социальной информации* (ТЭСИ), составляющих суть общероссийских классификаторов ТЭСИ [10, 11], для формирования *концептуальной модели* мониторинга, целью которого является поиск новых потенциальных объектов для включения в состав классификаторов. Особенность данных объектов классификации — в том, что одним из необходимых *условий* их включения в состав классификаторов является публикация информации о них в *нормативных правовых актах* (НПА) заданного уровня.

Представим *систему мониторинга* (СМ) в информационной среде Σ в виде алгебраической структурно-функциональной динамической модели взаимодействия по определенным правилам совокупности универсальных алгебр и гомоморфизма φ:

$$\begin{cases} \Sigma = \langle E, a_i^* \in A^* \rangle; \\ \varphi: \ D \to A^*, \end{cases} \quad (4)$$

где $E = \langle D, R \rangle$ — внешняя информационная среда (например, различные информационные ресурсы заданной ПОИ, выбранные для мониторинга); $D = \{d_l\}$ — множество документов НПА, анализируемых в ходе мониторинга, причем $l = 1, \dots, |D|$; $R = \{r_u\}, u = 1, \dots, |R|$ — ресурсы (БДЗ, библиотеки, АИС), доступные для мониторинга; a_i^* — результат мониторинга: новый объект правоотношений, информация о котором обнаружена в анализируемых НПА; φ — отображение множества документов D во множество $A^* = \{\emptyset, 1, \dots\}$ результатов мониторинга.

Элементами (объектами) множества D могут быть законодательные акты (постановления, указы, решения и др.) и ряд других документов, выбранных для информационного поиска. Именно документы такого уровня служат обоснованием для включения объектов в состав общероссийских классификаторов ТЭСИ, являющимися обязательными для применения в государственных АИС и при межведомственном обмене информацией[10].

Таким образом, рассматриваемая СМ контролирует заданную ПОИ, объекты которой составляют соответствующий классификатор, который можно характеризовать *состоянием* в виде следующего кортежа:

$$\bar{a}(t) = \langle a_1, a_2, \dots, a_i, \dots, a_{N^t} \rangle, \quad (5)$$

размер N^t которого определен на момент времени t последнего проведенного мониторинга данной ПОИ.

Любое состояние из выражения (5):

$$a_i: \{\mathrm{C}(Q_j)\} \quad (6)$$

соответствует множеству объектов классификации мощности $|C|$ для заданной ПОИ классификатора Q_j, где j — номер классификатора. Для ряда ПОИ количество объектов классификации (6) пополняется редко (например, классификаторы валют, стран мира и др.).

Определение. Состояние $\bar{a}(t)$ предметной области называется *наблюдаемым*, если все объекты классификатора являются обоснованными и актуальными для применения в АИС.

Положительный исход — когда в результате мониторинга обнаружен новый объект, что можно представить следующим выражением:

$$a_{N^t}^* := \{\mathrm{C}(Q_j)\} + c^*(N^t),$$

где $c^*(\cdot)$ — новый объект (или группа объектов) классификации, выявленная на момент времени t.

ПОИ становится *частично* наблюдаемой, если на момент времени $(t+1) = t + \Delta t$ в результате очередного мониторинга выявлены новые объекты классификации — $c^*(\cdot)$ для включения в состав классификатора путем внесения изменений в соответствии с процедурой, установленной действующими *правилами стандартизации*, но пока еще (в соответствии с процедурой внесения изменений в общероссийские классификаторы) официально в них не включены. Частичная наблюдаемость может привести к рискам, связанным с учетной политикой, статистическими оценками секторов экономики, которые формируют экономические *индикаторы* и на основе которых строится процесс управления.

Высокая экономическая динамика как способ развития хозяйственной системы характеризуется процессами смены состояний, появлением новых объектов (продуктов и услуг). В этой связи экономическая статистика постоянно выступает в роли «догоняющего», стремясь своевременно включить в анализ новые объекты, чтобы обеспечить некоторое постоянство анализируемой ПОИ для выявления роли факторов, влияющих на выбранную систему показателей и оценок. Поэтому в рассматриваемом подходе к организации мониторинга предметных областей особого внимания заслуживает вопрос выбора интервала (периодичности) проведения мониторинга — Δt.

[10] Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации» (ст. 2, п. 7).

Заключение

С учетом роста объемов и разнообразия измерительных данных дальнейшие направления развития приложений АИС и ИКТ представляется целесообразным строить на основе интеграции данных и интеллектуализации методов и моделей переработки данных, сокращая тем самым границы между *физическим* пространством объектов управления — источников данных и *кибернетическим* пространством — анализа и принятия решений по управлению данными объектами.

Основным направлением в развитии методов мониторинга на основе наблюдаемости данных должен стать подход на базе выявления новых знаний, полученных в ходе реализации методов машинного обучения для анализа получаемых данных.

Разработка когнитивных систем мониторинга *нормативно-правовой базы* для постоянного контроля нормативно-правовой среды позволит своевременно выявлять новые объектов правоотношений для включения в состав общероссийских классификаторов, обеспечивая актуализацию баз данных и знаний ведомственных информационных ресурсов.

Одним из актуальных направлений дальнейших исследований видится разработка автоматизированных информационных систем мониторинга предметных областей на основе методов построения онтологических структур существующих классификаторов для сокращения области поиска и ускорения его проведения.

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. Аллакин В.В., Будко Н.П., Васильев Н.В. Общий подход к построению перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей // Системы управления, связи и безопасности. 2021. № 4. С. 125—227. DOI: 10.24412/2410-9916-2021-4-125-227 .
2. Антопольский А.Б., Каленов Н.Е., Серебряков В.А., Сотников А.Н. О едином цифровом пространстве научных знаний // Вестник РАН. 2019. Т. 89. № 7. С. 728—735. DOI: 10.31857/S0869-5873897728-735 .
3. Бова В.В. Онтологическая модель интеграции данных и знаний в интеллектуальных информационных системах // Известия ЮФУ. Технические науки. 2015. № 4 (165). С. 225—237.
4. Брюс П., Брюс Э. Практическая статистика для специалистов Data Science. СПб. : БХВ-Петербург, 2019. 304 с. ISBN 978-5-9775-3974-6.
5. Бурый А.С. Совершенствование государственных информационных систем как тренд цифрового общества // Правовая информатика. 2020. № 3. С. 19—28. DOI: 10.21681/1994-1404-2020-3-19-28 .
6. Бурый А.С. Облачные вычисления в цифровой трансформации информационных технологий // Правовая информатика. 2021. № 2. С. 4—14. DOI: 10.21681/1994-1404-2021-2-04-14 .
7. Бурый А.С. Формирование терминосистем на основе онтологий // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 1 (65). С. 4—11.
8. 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 .
9. 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 .
10. Бурый А.С., Слепынцева Л.И. Цифровизация контента документов по стандартизации. Часть 1. Состояние и современные тенденции // Информационно-экономические аспекты стандартизации и технического регулирования. 2021. № 1 (59). С. 105—113.
11. Джумайло Е.С., Баранюк В.В. Методика онтологического связывания объектов в автоматизированных системах с использованием классификаторов // International Journal of Open Information Technologies. 2018. Т. 6. № 6. С. 97—102.
12. Жукова Н.А., Андриянова Н.Р. Проблема когнитивного мониторинга распределенных объектов // НТИ. Сер. 2: Информационные процессы и системы. 2019. № 2. С. 18—29.
13. Кашников А., Лядова Л. Интеграция гетерогенных источников данных на основе рекурсивной декомпозиции // International Journal "Information Technologies & Knowledge". 2011. № 3 (5). С. 274—284.
14. Кучукова Н.Н., Вершков Н.А. Математическая модель подсистемы поиска и ранжирования документов в информационно-поисковых системах // Научные ведомости Белгородского гос. ун-та. Сер. Экономика. Информатика. 2018. Т. 45. № 1. С. 176—183. DOI: 10.18413/2411-3808-2018-45-1-176-183 .
15. Ловцов Д.А. Теоретические основы системной информатизации правового регулирования // Правовая информатика. 2019. № 4. С. 12—28. DOI: 10.21681/1994-1404-2019-4-12-28 .

16. 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 .
17. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
18. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
19. Ловцов Д.А. Системология информационного права // Правосудие. 2022. Т. 4. № 1. С. 41—70. DOI: 10.37399/2686-9241.2022.1.41-70 .
20. Макаренко С.И., Соловьева О.С. Основные положения концепции семантической интероперабельности сетецентрических систем // Журнал радиоэлектроники. 2021. № 4. DOI: 10.30898/1684-1719.2021.4.10 .
21. Миков А.И. Информационные процессы и нормативные системы в IT: Математические модели. Проблемы проектирования. Новые подходы. М. : Либроком, 2020. 256 с. ISBN 978-5-397-07358-5.
22. Осипов Г.С. Лекции по искусственному интеллекту. М. : Ленанд, 2022. 272 с. ISBN 978-5-9710-5520-4.
23. Тарасов В.Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика. М. : Эдиториал УРСС, 2002. 352 с. ISBN 5-8360-0330-0.
24. Buryi A.S. Structure complexity of distributed information-control systems. Izvestiya Rossiiskoi Akademii Nauk. Teoriya i Sistemy Upravleniya, 1994, No. 5, pp. 160–167.
25. Duan Y, Zhan L, Zhang X, Zhang Y. Formalizing DIKW architecture for modeling security and privacy as typed resources. In: International Conference on Testbeds and Research Infrastructures, 2019, pp. 157–168. Springer, Cham.
26. Fatemi M., Setoodeh P., Haykin S. Observability of stochastic complex networks under the supervision of cognitive dynamic systems. Journal of Complex Networks, 2014, No. 5, pp. 433–460.
27. Singh P., Dwivedi Y. K., Kahlon K.S. et al. Smart Monitoring and Controlling of Government Policies Using Social Media and Cloud Computing. Information Systems Frontiers, 2020, 22, pp. 315–337. DOI: 10.1007/S10796-019-09916-Y .
28. Yin D, Ming X, Zhang X. Understanding Data-Driven Cyber-Physical-Social System (D-CPSS) Using a 7C Framework in Social Manufacturing Context. Sensors, 2020, No. 20 (18), art. no. 5319. DOI: 10.3390/s20185319 .

STRUCTURING INFORMATION RESOURCES MONITORING SYSTEMS

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

Keywords: *monitoring, information and telecommunication technology, subject area, data and knowledge integration, data observability, classifiers.*

Abstract

Purpose of the paper: improving the research and methodological foundations for developing the concept of forming the information medium elements for the studied subject area using monitoring information resources for maintaining the topicality of objects of legal relations.

Methods of study: multi-faceted use of system and comparative analysis, logical concept modelling, formal logical development and justification of structures for building distributed information systems.

Study findings: a conceptual approach is put forward for forming the objects of classification based on monitoring information resources of the specified subject area within the framework of government information systems. The interaction between the cyber-physical and social medium at the levels of data processing, information analysis and knowledge elicitation with a view to generating integrated information structures and identifying synergetic properties of information systems is studied. A proposition is put forward that there exists a tendency of tendency of rapprochement between cyber-physical and social processes, and for structuring them it is advisable to use the problem-oriented variant of the multi-faceted information, cybernetics and synergetics approach within the digital transformation technologies paradigm.

References

1. Allakin V.V., Budko N.P., Vasil'ev N.V. Obshchii podkhod k postroeniiu perspektivnykh sistem monitoringa raspredelennykh informatsionno-telekommunikatsionnykh setei. Sistemy upravleniia, sviazi i bezopasnosti, 2021, No. 4, pp. 125–227. DOI: 10.24412/2410-9916-2021-4-125-227 .

2. Antopol'skii A.B., Kalenov N.E., Serebriakov V.A., Sotnikov A.N. O edinom tsifrovom prostranstve nauchnykh znanii. Vestnik RAN, 2019, t. 89, No. 7, pp. 728–735. DOI: 10.31857/S0869-5873897728-735 .
3. Bova V.V. Ontologicheskaia model' integratsii dannykh i znanii v intellektual'nykh informatsionnykh sistemakh. Izvestiia IuFU. Tekhnicheskie nauki, 2015, No. 4 (165), pp. 225–237.
4. Brius P., Brius E. Prakticheskaia statistika dlia spetsialistov Data Science. SPb. : BKhV-Peterburg, 2019. 304 pp. ISBN 978-5-9775-3974-6.
5. Buryi A.S. Sovershenstvovanie gosudarstvennykh informatsionnykh sistem kak trend tsifrovogo obshchestva. Pravovaia informatika, 2020, No. 3, pp. 19–28. DOI: 10.21681/1994-1404-2020-3-19-28 .
6. Buryi A.S. Oblachnye vychisleniia v tsifrovoi transformatsii informatsionnykh tekhnologii. Pravovaia informatika, 2021, No. 2, pp. 4–14. DOI: 10.21681/1994-1404-2021-2-04-14 .
7. Buryi A.S. Formirovanie terminosistem na osnove ontologii. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia, 2022, No. 1 (65), pp. 4–11.
8. 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 .
9. 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 .
10. Buryi A.S., Slepyntseva L.I. Tsifrovizatsiia kontenta dokumentov po standartizatsii. Chast' 1. Sostoianie i sovremennye tendentsii. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia, 2021, No. 1 (59), pp. 105–113.
11. Dzhumailo E.S., Baraniuk V.V. Metodika ontologicheskogo sviazyvaniia ob"ektov v avtomatizirovannykh sistemakh s ispol'zovaniem klassifikatorov. International Journal of Open Information Technologies, 2018, t. 6, No. 6, pp. 97–102.
12. Zhukova N.A., Andriianova N.R. Problema kognitivnogo monitoringa raspredelennykh ob"ektov. NTI, ser. 2: Informatsionnye protsessy i sistemy, 2019, No. 2, pp. 18–29.
13. Kashnikov A., Liadova L. Integratsiia geterogennykh istochnikov dannykh na osnove rekursivnoi dekompozitsii. International Journal "Information Technologies & Knowledge", 2011, No. 3 (5), pp. 274–284.
14. Kuchukova N.N., Vershkov N.A. Matematicheskaia model' podsistemy poiska i ranzhirovaniia dokumentov v informatsionno-poiskovykh sistemakh. Nauchnye vedomosti Belgorodskogo gos. un-ta, ser. Ekonomika. Informatika, 2018, t. 45, No. 1, pp. 176–183. DOI: 10.18413/2411-3808-2018-45-1-176-183 .
15. Lovtsov D.A. Teoreticheskie osnovy sistemnoi informatizatsii pravovogo regulirovaniia. Pravovaia informatika, 2019, No. 4, pp. 12–28. DOI: 10.21681/1994-1404-2019-4-12-28 .
16. 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 .
17. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
18. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
19. Lovtsov D.A. Sistemologiia informatsionnogo prava. Pravosudie, 2022, t. 4, No. 1, pp. 41–70. DOI: 10.37399/2686-9241.2022.1.41-70 .
20. Makarenko S.I., Solov'eva O.S. Osnovnye polozheniia kontseptsii semanticheskoi interoperabel'nosti setetsentricheskikh sistem. Zhurnal radioelektroniki, 2021, No. 4. DOI: 10.30898/1684-1719.2021.4.10 .
21. Mikov A.I. Informatsionnye protsessy i normativnye sistemy v IT: Matematicheskie modeli. Problemy proektirovaniia. Novye podkhody. M. : Librokom, 2020. 256 pp. ISBN 978-5-397-07358-5.
22. Osipov G.S. Lektsii po iskusstvennomu intellektu. M. : Lenand, 2022. 272 pp. ISBN 978-5-9710-5520-4.
23. Tarasov V.B. Ot mnogoagentnykh sistem k intellektual'nym organizatsiiam: filosofiia, psikhologiia, informatika. M. : Editorial URSS, 2002. 352 pp. ISBN 5-8360-0330-0.
24. Buryi A.S. Structure complexity of distributed information-control systems. Izvestiya Rossiiskoi Akademii Nauk. Teoriya i Sistemy Upravleniya, 1994, No. 5, pp. 160–167.
25. Duan Y, Zhan L, Zhang X, Zhang Y. Formalizing DIKW architecture for modeling security and privacy as typed resources. In: International Conference on Testbeds and Research Infrastructures, 2019, pp. 157–168. Springer, Cham.
26. Fatemi M., Setoodeh P., Haykin S. Observability of stochastic complex networks under the supervision of cognitive dynamic systems. Journal of Complex Networks, 2014, No. 5, pp. 433–460.
27. Singh P., Dwivedi Y. K., Kahlon K.S. et al. Smart Monitoring and Controlling of Government Policies Using Social Media and Cloud Computing. Information Systems Frontiers, 2020, 22, pp. 315–337. DOI: 10.1007/S10796-019-09916-Y .
28. Yin D, Ming X, Zhang X. Understanding Data-Driven Cyber-Physical-Social System (D-CPSS) Using a 7C Framework in Social Manufacturing Context. Sensors, 2020, No. 20 (18), art. no. 5319. DOI: 10.3390/s20185319 .

ВЫЯВЛЕНИЕ АНОМАЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ ВУЗОВ

Котенко И.В.[1], Саенко И.Б.[2], Аль-Барри М.Х.[3]

***Ключевые слова**: информационная безопасность, инсайдер, компьютерная атака, база данных, SQL-инъекция, машинное обучение, классификатор, регистрационный журнал, набор данных.*

Аннотация

Цель: сформировать постановку задачи обеспечения требуемой точности выявления аномального поведения пользователей центров обработки данных вузов и получить ее решение с помощью методов машинного обучения.

Методы: системный анализ проблемы выявления аномального поведения пользователей центров обработки данных вузов и методы контролируемого машинного обучения.

Результаты: предложена оригинальная формальная постановка задачи обнаружения аномальных действий пользователей центров обработки данных вуза, ориентированная на применение методов машинного обучения; разработан подход к снижению размерности первоначального признакового пространства и реализующий его алгоритм, который основан на типизации имен таблиц данных, присутствующих в тексте SQL-запросов; проведена реализация предложенного подхода с использованием множества моделей машинного обучения; выполнена экспериментальная оценка предложенного подхода, которая подтвердила его высокую эффективность и позволила выявить наиболее приемлемые для решения данной задачи классификаторы, которыми являются дерево решений, метод k-ближайших соседей и многослойная нейронная сеть.

DOI: 10.21681/1994-1404-2023-1-62-71

Введение

В результате широкого распространения облачных сервисов существенно возросла популярность использования *центров обработки данных* (ЦОД) [1] в системах управления. ЦОД являются, по сути, хранилищами больших массивов разнородной информации. Они обеспечивают своим пользователям возможность совместного устойчивого и своевременного использования информационных ресурсов в интересах решения различных задач [2, 3]. Нарушители безопасности ЦОД могут быть как внутренними, так и внешними [4, 5]. Внутренние нарушители (инсайдеры) оказывают негативное влияние на безопасность ЦОД путем выполнения вредоносных действий, которые не удается зафиксировать имеющимися средствами защиты. Внешние нарушители, как правило, оказывают негативное влияние на безопасность ЦОД с помощью компьютерных атак различного вида.

При построении систем защиты информации ЦОД могут использоваться различные методы поиска аномалий, обладающие той или иной степенью эффективности. Обычно аномалии обнаруживаются в *сетевом трафике*. Для этой цели разработаны и используются различные сетевые средства защиты, например, системы обнаружения вторжений, межсетевые экраны, антивирусные средства и др. Однако аномалии сетевого трафика не в полной мере отражают неправильное или аномальное поведение пользователей при работе с *базами данных* ЦОД. Аномальное поведение пользователей ЦОД проявляется в виде обращения к базам данных

[1] ***Котенко Игорь Витальевич,*** *доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности Санкт-Петерургского Федерального исследовательского центра Российской академии наук, г. Санкт-Петербург, Российская Федерация.*
E-mail: ivkote@comsec.spb.ru

[2] ***Саенко Игорь Борисович,*** *доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, г. Санкт-Петербург, Российская Федерация.*
E-mail: ibsaen@comsec.spb.ru

[3] ***Аль-Барри Мазен Хамед,*** *адъюнкт Военной академии связи имени маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Российская Федерация.*
E-mail: mazenb51@gmail.com

с неправильными, аномальными запросами. Аномальные запросы могут быть сформированы специальным образом, позволяющим произвести либо вредоносное изменение содержимого баз данных, либо несанкционированный доступ (НСД) к информации баз данных. Такие запросы являются особым типом компьютерных атак, которые называются *SQL-инъекциями* [6]. Кроме того, аномальные запросы могут иметь обычный вид и не содержать *SQL*-инъекций, но обращаться к неразрешенным областям баз данных. Защита от таких обращений обычно возлагается на имеющуюся в ЦОД систему разграничения доступа к базам данных. Для этого могут использоваться различные модели контроля доступа, такие как *ролевая* (*Role-Based Access Control*) или *атрибутивная* (*Attribute-Based Access Control*). Однако для сложных баз данных, содержащих большое количество таблиц данных, построить схему контроля доступа, полностью запрещающую аномальные запросы, является сложной задачей.

Предлагаемый *подход*, основанный на машинном обучении, предназначен для решения данной задачи. При этом в качестве исходных данных, на основе которых формируются применяемые в методах машинного обучения наборы данных, предлагается использовать регистрационные журналы баз данных. В этих журналах фиксируются тексты запросов, с которыми пользователи обращались к базам данных. Если базы данных основаны на *реляционной* модели, то запросы записываются на языке *SQL*. Если в ЦОД присутствуют базы данных других моделей (так называемые *NoSQL* базы данных), то возможна запись запросов на других языках.

В статье рассматривается возможность применения методов машинного обучения для обнаружения аномального поведения пользователей в ЦОД, используемого для хранения информации и решения на ее основе задач, связанных с учебным процессом в высшем учебном заведении (вузе). Выбор такого типа ЦОД объясняется двумя причинами [7]. *Во-первых*, в базах данных для учебного процесса содержится очень большое количество таблиц данных. Так, отдельные таблицы создаются для каждого преподавателя, каждого студента и для каждой учебной дисциплины. В результате, если использовать имена таблиц для формирования признакового пространства, то количество признаков в нем будет очень большим. Это делает применение машинного обучения невозможным или чрезвычайно затруднительным. *Во-вторых*, в ЦОД вуза существует достаточно большое количество инсайдерских угроз безопасности. В качестве потенциальных инсайдеров можно рассматривать студентов, многие из которых через некоторое время обучения начинают обладать навыками работы с *SQL*-запросами. Поэтому разработка для ЦОД вуза дополнительного рубежа безопасности, позволяющего обнаруживать аномальные запросы к его базам данных, является актуальной задачей. При этом следует заметить, что тематике обнаружения или анализа возможного вредоносного поведения пользователей ЦОД в настоящее время посвящено недостаточное количество работ.

Таким образом, предлагается новый подход к обнаружению аномального поведения пользователей ЦОД, основанный на использовании методов машинного обучения и их применении к регистрационным журналам баз данных.

Обзор работ по тематике исследования

Работы, связанные с тематикой обнаружения аномалий в работе ЦОД, можно разделить на две группы: по обнаружению аномалий в функционировании ЦОД и по обнаружению компьютерных атак типа *SQL*-инъекции.

Во всех работах *первой* группы подчеркивается, что процедуры обнаружения аномалий в работе ЦОД основываются на анализе регистрационных журналов. В [8] обращается внимание на то, что записи журналов в ЦОД являются стохастическими и нестационарными по своей природе. Поэтому эта работа предлагает подход, в котором атрибуты извлекаются из временных окон и используются для обучения и дообучения «на лету» классификатора, задействованного в процедуре анализа данных, в качестве которого используется развивающийся нечеткий классификатор Гаусса. В [9] для извлечения признаков из записей регистрационных файлов предлагается использовать методы обработки естественного языка, в частности, алгоритм *word2vec*, а для обнаружения аномальных регистрационных записей — автокодировщик с нейронной сетью вида *LSTM*. Это, несомненно, продуктивная идея, однако ее применение для обнаружения аномальных запросов к базам данных ЦОД вуза приводит к существенному увеличению размерности признакового пространства. Это значительно снижает эффективность применения методов глубокого обучения, к которым относятся *LSTM*-сети, и, в частности, значительно увеличивает время, требуемое на их обучение.

В [10] предлагается использовать методы неконтролируемого (*unsupervised*) машинного обучения для определения нормального и ненормального поведения систем охлаждения в ЦОД. Вопросы предотвращения враждебного влияния на обнаружение аномалий в ЦОД рассматриваются в [11]. Эта работа предлагает подход к оптимизации модели линейной регрессии с возможностью изменять данные на этапе обучения. В [12] предлагается выявлять аномалии в работе ЦОД путем сопоставления отклонений прогнозных и реальных данных с использованием различных методов машинного обучения. В [13] для обнаружения и классификации атаки в сетевом трафике ЦОД предлагается использовать модели линейной регрессии и случайного леса.

Несмотря на хорошие результаты, полученные в указанных выше работах по обнаружению аномалий, свойственных функционированию ЦОД, следует заметить, что в этих работах не рассматривались аномалии в *SQL*-запросах и обнаружение *SQL*-инъекций.

Этому посвящены работы *второй* группы, например, работы [14—18]. Так, в [14] подчеркивается, что *SQL*-инъекции стали возможными из-за отсутствия проверки вводимых запросов. Эта работа предлагает подход к обнаружению *SQL*-инъекций, основанный на выделении токенов запроса и их сравнении с зарезервированным словарем. В [15] предлагается предсказывать *SQL*-инъекции с помощью модели обучения ансамблю семантических запросов. В этой модели обучения использовался ансамбль из девяти базовых классификаторов, обеспечивающий максимальную точность прогнозирования с помощью голосования. В [16] для обнаружения аномалий в поведении пользователей ЦОД предлагается использовать многомерные статистические тесты. В [17] представлен метод обнаружения *SQL*-инъекций в веб-приложениях на основе сверхточной нейронной сети. Работа [18] предлагает подход к обнаружению *SQL*-инъекций, основанный на анализе реакции и состояния веб-приложения при различных атаках. В [19] рассматривается основанный на машинном обучении подход к предотвращению *SQL*-атак, в котором тестируется свыше 20 различных классификаторов и выбираются 5 наилучших. Эти идеи также использованы в нашей работе.

Постановка задачи

Рассмотрим вначале постановку задачи обнаружения аномальных *SQL*-запросов в ЦОД вуза на основе применения методов машинного обучения. Будем считать, что работа пользователей ЦОД сводится к обращениям к имеющимся в ЦОД базам данных с помощью запросов, составленных на языке *SQL*. Запросы к базам данных фиксируются в регистрационных журналах *системы управления базами данных* (СУБД). Примерами *SQL*-СУБД, которые являются открытыми и могут использоваться в вузовских ЦОД, являются *PostgreSQL*, *MySQL* и др.

Регистрационный журнал состоит из отдельных записей. Каждая запись отражает факт обращения некоторого пользователя к базе данных и содержит следующие поля: дату, время, идентификатор пользователя и текст *SQL*-запроса, который был сформирован пользователем и выполнен со стороны СУБД. Поэтому можно считать, что задача выявления аномального поведения пользователей ЦОД вуза сводится к обнаружению аномальных *SQL*-запросов к базам данных ЦОД, что приводит в конечном итоге к поиску аномальных записей в регистрационных журналах.

Если представить регистрационный журнал СУБД как набор данных, состоящих из записей, то возможная методика анализа такого набора данных на предмет выявления аномалий предполагает следующие этапы:

1) формирование множества признаков, которыми характеризуются *SQL*-запросы;

2) преобразование журнального набора данных в набор данных, записи которого содержат значения сформированных признаков;

3) формирование обучающей выборки, на которой будет осуществляться процесс машинного обучения;

4) использование обученных средств для непосредственного выявления аномальных запросов.

Исходными данными задачи являются:

- множество регистрационных журналов: $\boldsymbol{L} = \{L_1, L_2, ..., L_M\}$;
- множество пользователей: $\boldsymbol{U} = \{U_1, U_2, ..., U_N\}$;
- каждый журнал представляется в виде множества записей: $L_m = \{l_{mi}\}$;
- каждая запись журнала представлена в виде кортежа:

$$l_{mi} = <Date_{mi}, TimeStamp_{mi}, User_{mi}, Op_{mi}>,$$

где $Date_{mi}$ — дата i-го запроса в m-м журнале: $TimeStamp_{mi}$ — временна́я метка запроса; $User_{mi} \in U$ — пользователь запроса; Op_{mi} — текст *SQL*-запроса (*SQL*-инструкция);

- каждая *SQL*-инструкция может быть представлена в виде:

$$Op_{mi} = <Operator, \{Tables\}, \{Fields\}, \{Values\}>,$$

где *Operator* — оператор языка *SQL*; $\{Tables\}$ — множество имен таблиц, которые присутствуют в *SQL*-инструкции; $\{Fields\}$ — множество имен полей; $\{Values\}$ — множество значений полей;

- модели машинного обучения (бинарные классификаторы), которые наиболее часто используются для обнаружения аномалий в наборах данных [20, 21, 22];
- требования по обнаружению атак на базы данных типа *SQL*-инъекции: вероятность правильного обнаружения атаки: $P_{\text{det}} \geq 0{,}95$; вероятность пропуска атаки: $P_{\text{mis}} \leq 0{,}1$.

Для расчета вероятностей предлагается использовать следующие формулы:

$$P_{\text{det}} \approx TP/(TP + FP + FN) \quad (1)$$

$$P_{\text{mis}} \approx FN/(FN + TP) \quad (2)$$

где TP — количество правильно обнаруженных аномалий в наборе данных (True Positive); FP — количество ложно обнаруженных аномалий в наборе данных (*False Positive*); FN — количество ложно обнаруженных нормальных записей в наборе данных (*False Negative*).

В результате решения поставленной задачи требуется построить модель признакового пространства, характеризующую нормальную и аномальную деятельность пользователей БД при отсутствии и наличии атак, и определить методику обнаружения аномальных *SQL*-запросов на основе применения моделей бинарной классификации.

В предлагаемой *модели признакового пространства* признаки разделены на три категории. Признаки *первой* категории определяют количество вхождений того или иного ключевого слова языка *SQL* в *SQL*-инструкцию. Всего отобрано 30 ключевых слов-операторов, таких как SELECT, INSERT, UPDATE, DELETE, RENAME, CREATE, GRANT, ALTER и др.

Вторую категорию признаков составляют количества вхождений тех или иных сигнатур, свойственных *SQL*-инъекциям. Для этой цели были отобраны следующие сигнатуры: "Execute", "or", "txtUserId", "getRequestString", "1=1", "- -", "CHAR", "#" и ";". Появление таких сигнатур в *SQL*-запросах может быть вызвано реализацией *SQL*-инъекций. Всего было использовано 10 сигнатур.

Третью категорию формируют количества вхождений в записи тех или иных имен таблиц данных. В базе данных ЦОД вуза, которая использовалась для экспериментальной оценки предлагаемого подхода, присутствовало свыше 4 000 таблиц данных. Это было вызвано ненормализованным характером ее структуры. Около 2 000 таблиц хранили данные о преподавателях, по одной таблице на каждого преподавателя. Каждому учебному курсу, учебной дисциплине и учебной группе также соответствовала отдельная таблица данных.

Таблица 1

Состав признакового пространства

№ п/п	Категория	Название	Описание
1	1	SELECT_COUNT	Количество вхождений SELECT
2		INSERT_COUNT	Количество вхождений INSERT
…		…	…
30		HAVING_COUNT	Количество вхождений HAVING
31	2	Execute_COUNT	Количество вхождений "Execute"
32		"1=1" _COUNT	Количество вхождений "1=1"
…		…	…
40		txtUserId_COUNT	Количество вхождений "txtUserId"
41	3	Table_1_COUNT	Количество вхождений имени таблицы данных 1
42		Table_2_COUNT	Количество вхождений имени таблицы данных 2
…		…	…
181		Table_141_COUNT	Количество вхождений имени таблицы данных 141

Из-за такого большого количества таблиц были приняты два допущения. *Во-первых*, было решено при формировании признакового пространства не использовать имена полей и их значения, а ограничиться только именами таблиц данных. *Во-вторых*, было решено сократить количество учитываемых в признаковом пространстве имен таблиц, заменяя их общим типовым именем. Так, все имена таблиц для преподавателей были заменены на типовое имя "Teacher_Table", имена таблиц для учебных групп — "Group_Table" и др. В итоге количество учитываемых имен таблиц данных удалось снизить до 141.

Состав сформированного признакового пространства представлен в табл. 1. Из нее видно, что общее количество признаков стало равным 181. Из них 30 признаков относятся к *первой* категории, 10 — ко *второй* категории и 141 — к *третьей* категории.

Реализация предложенного подхода

Для реализации и проверки предлагаемого подхода был использован язык *Python v*.3.8.8 с наборами следующих библиотек: *sklearn, numpy, pandas, matplotlib, Scipy, Re, Pylab*, *Math*. Вычислительная среда была организована на ноутбуке *Jupyter*. В ЦОД вуза для создания базы данных использовалась СУБД *PostgreSQL v*. 13.4, работающая под операционной системой *Ubuntu v*. 13.4. Исследовались следующие наиболее популярные модели контролируемого (*supervised*) машинного обучения, которые являются бинарными классификаторами [20, 21]: машина опорных векторов (*SVM*), дерево решений (*DT*), логистическая регрессия (*LR*), случайный лес (*RF*), гауссов наивный Байес (*GNB*); метод *k*-ближайших соседей (*KNN*) и многослойная нейронная сеть (*NN*).

Для формирования набора данных, который применялся для обучения классификаторов, был выбран фрагмент регистрационного журнала, отображающий работу пользователей с базой данных в течение 15 минут. Всего в этом фрагменте первоначально находилось 82 192 инструкций. На рис. 1 показан вид отдельных инструкций, входящих в этот фрагмент.

Из рис. 1 видно, что запись данного фрагмента была произведена 18 января 2022 г. Она началась в 12:44:09

```
2022-01-18 12:44:09.749 UTC [1174] LOG:  database system is ready to accept connections
2022-01-18 12:44:10.986 UTC [1187] postgres@template1 LOG:  statement:
2022-01-18 12:44:37.957 UTC [1211] postgres@2122 LOG:  statement: SELECT DISTINCT "groups" FROM
"p_learn_plan" ORDER BY "groups"
...
2022-01-18 12:45:01.514 UTC [1230] postgres@2122 LOG:  statement: SELECT "potok_num" FROM "p_group"
WHERE groups='1123'
2022-01-18 12:45:01.514 UTC [1230] postgres@2122 LOG:  statement: SELECT "groups" FROM "p_group"
WHERE potok_num='112'
2022-01-18 12:45:01.567 UTC [1234] postgres@2122 LOG:  statement: SELECT "23" FROM "1123" ORDER BY
count;
...
2022-01-18 12:46:41.250 UTC [1276] postgres@2122 LOG:  statement: select * from pg_tables where
tablename='IvanovDA';
2022-01-18 12:46:41.254 UTC [1276] postgres@2122 LOG:  statement: select * from "IvanovDA" where
"count"='2'
...
2022-01-18 12:47:20.926 UTC [1276] postgres@2122 LOG:  statement: select "n_aud" from "D-0406" where
"prep"='5' and "groups"='5811'
...
2022-01-18 13:00:33.497 UTC [1656] postgres@2122 LOG:  statement: SELECT "groups" FROM "p_group"
WHERE potok_num='534'
2022-01-18 13:00:33.498 UTC [1587] postgres@2122 LOG:  statement: select "n_aud" from "D-2006" where
"prep"='38' and "groups"='3882'
```

Рис.1. Фрагмент регистрационного журнала базы данных ЦОД вуза

и закончилась в 13:00:33. С базой данных работало несколько пользователей. Пользователи, чьи запросы отражает рисунок, имели идентификаторы 1174, 1187, 1211, 1230, 1234, 1276, 1565, 1587. Запросы обращались к различным таблицам данных. Так, запрос со временем 12:44:37 обращался к системной таблице “p_learn_plan” (в ней находилась планирующая информация по учебному процессу). Имя этой таблицы стоит в инструкции после ключевого слова FROM. Другие запросы обращались к следующим таблицам: “p_group”, “1123”, “pg_tables”, “IvanovDA”, “D-0406”, “D-2006”. Таблицы “p_group” и “pg_tables” являются *системными*. Они были созданы системой при создании самой базы данных. Остальные таблицы являются *пользовательскими*. Пользовательские таблицы создаются пользователями с помощью команды CREATE в процессе работы с базой данных. Таблица “IvanovDA” содержит данные о преподавателе с именем «Д.А. Иванов». Таблица “1123” содержит данные об учебной группе с номером 1123. Таблицы “D-0406” и “D-2006” содержат данные об учебных дисциплинах, которые имеют идентификаторы Д-0406 и Д-2006 соответственно.

Всего в базе данных ЦОД вуза на момент создания набора данных, как было сказано, имелось свыше 2 000 таблиц с данными о преподавателях, около 1 000 таблиц с данными об учебных группах, несколько сотен таблиц с данными об учебных дисциплинах. Поэтому при формировании набора данных было принято решение о типизации таких имен таблиц, т. е. об их замене на типовые имена.

Эта процедура стала одним из начальных шагов разработанного алгоритма формирования набора данных, состоящего в следующем:

Шаг 1. Извлечение из фрагмента регистрационного журнала всех имен таблиц и формирование множества имен таблиц, используемых во фрагменте. Всего из фрагмента, представленного на рис. 1, было извлечено 310 имен таблиц.

Шаг 2. Формирование множества новых, типовых имен таблиц. Для имен таблиц с данными о преподавателях использовалось имя “Teacher_Table”, для имен таблиц с данными об учебных группах — имя “Group_Table” и др. Всего в это множество вошло 141 имя, включая имена системных таблиц.

Шаг 3. Замена исходных имен таблиц во фрагменте регистрационного журнала на типовые имена. При этом количество инструкций во фрагменте попрежнему равнялось 82 192.

Шаг 4. Формирование начальной версии набора данных в формате *CSV*. Для каждой инструкции из исходного фрагмента создавалась *CSV*-запись. Полями этой записи служили признаки, которые были включены в модель признакового пространства (см. *табл.* 1). Включение в начальную версию набора данных поля *Result*, значение которого играет роль метки нормальной или аномальной записи, причем *Result* = 0, если запись является нормальной, *Result* = 1, если запись является аномальной.

Шаг 5. Исключение из набора данных дублирующих записей и внесение в него аномалий.

Так как дата и время запроса на текущем этапе исследований были исключены из признакового пространства (это было сделано осознанно, чтобы проверить эффективность машинного обучения на структурах *SQL*-запросов), то в начальной версии набора данных после *Шага* 4 появилось много дублирующих записей, которые

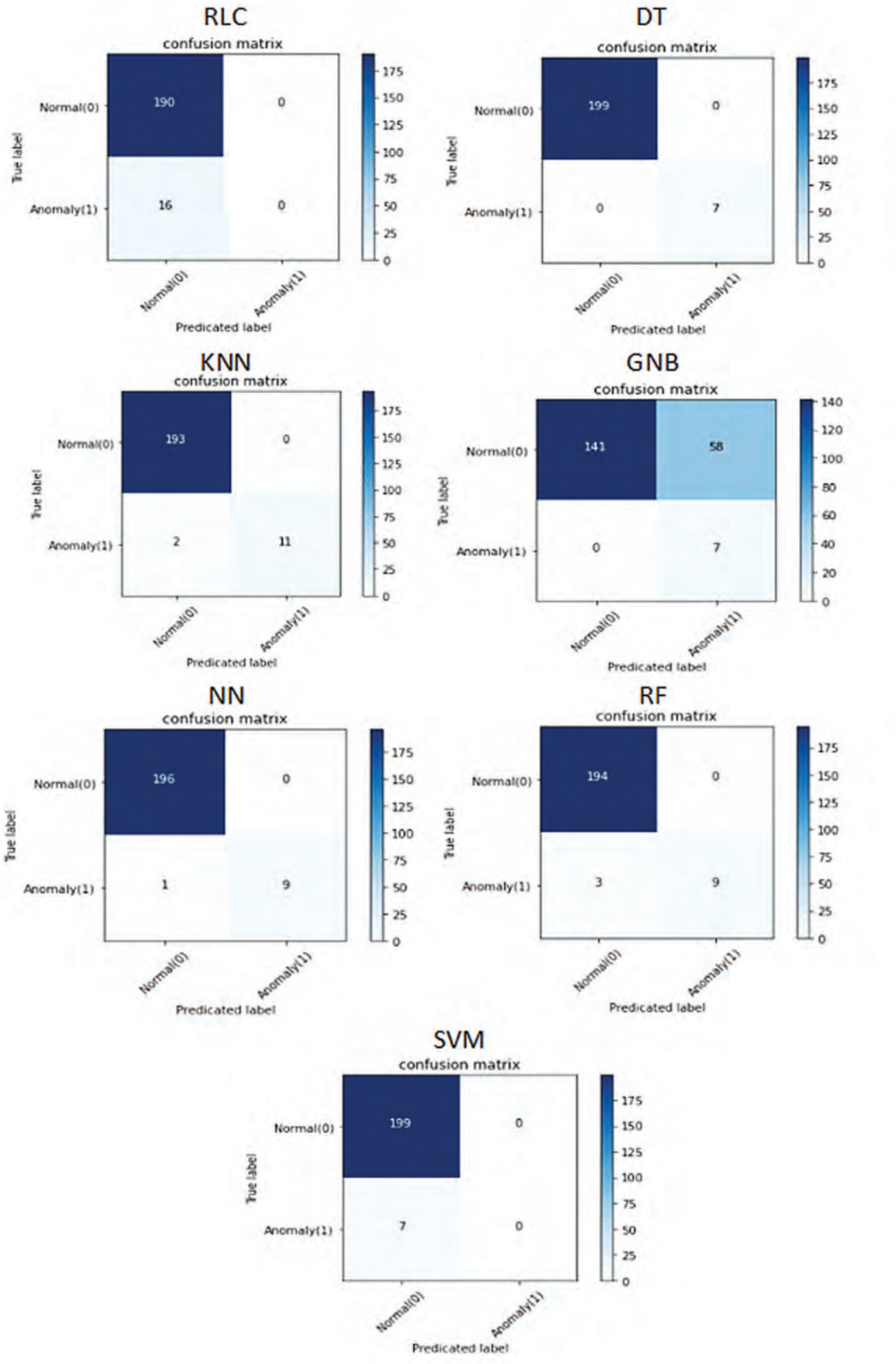

Рис.2. Результаты тестирования на различных классификаторах

никак не влияют на точность, но могут негативно влиять на скорость обнаружения аномалий. Поэтому на *Шаге* 5 такие записи удалялись. После их удаления в наборе данных осталось всего 1026 записей. Кроме того, несколько случайно выбранных записей были модифицированы таким образом, чтобы они соответствовали различными возможным аномалиям (*SQL*-инъекциям и попыткам несанкционированного доступа). Всего было модифицировано 50 таких записей, которые были помечены в поле *Result* как аномальные.

Набор данных, сформированный с помощью описанного выше алгоритма, далее подвергался анализу с помощью выбранных бинарных классификаторов.

Экспериментальные результаты

Экспериментальные исследования были разделены на два этапа — этап обучения и этап тестирования. *Первый* этап был посвящен обучению классификаторов и контрольной проверке точности их работы. На *втором* этапе использовались обученные классификаторы для непосредственного обнаружения аномалий.

На *первом* этапе набор данных, описанный выше, разбивался на две части. В *первую* часть, предназначенную для обучения, входили 80% записей. Во *вторую* часть, предназначенную для контрольного тестирования, вошли остальные 20% записей. Результаты тестирования (в виде матрицы ошибок) представлены на рис. 2.

Анализируя результаты (см. рис. 2), можно сделать следующие *выводы*. Наивысшую точность показал классификатор *DT*. Он без ошибок обнаружил как нормальные, так и аномальные записи. Удовлетворительные результаты продемонстрировали классификаторы *KNN*, *NN*, *RF*, которые без ошибок обнаружили все нормальные записи, а при обнаружении аномалий имели 10—25% ошибок. Классификаторы *RLC*, *SVM* также без ошибок обнаружили все нормальные записи, однако они не смогли правильно обнаружить ни одну аномалию. Наконец, классификатор *GNB* правильно обнаружил все аномалии, однако сделал очень большое количество ошибок при обнаружении нормальных записей — 29%.

На *втором* этапе обученные классификаторы использовались для тестирования нового набора данных, сформированного исходя из нового фрагмента регистрационного журнала. В этом фрагменте журнала содержалось 78 880 записей, записанных в течение 40 минут работы с базой данных. После его обработки рассмотренным выше алгоритмом в новом наборе данных осталось 1852 записи. В этот набор данных также было внесено 50 аномалий путем модификации имеющихся в нем записей.

Результаты тестирования нового набора данных, позволяющие оценить точность работы классификаторов, представлены в табл. 2.

Таблица 2

Результаты оценки точности работы классификаторов

Классификатор	TN	TP	FN	FP	P_{del}	P_{mis}
RLC	1807	5	45	0	0.10	0.90
DT	**1807**	**50**	**0**	**0**	**1.00**	**0.00**
KNN	**1807**	**48**	**2**	**0**	**0.96**	**0.04**
GNB	1256	50	0	551	0.08	0.00
NN	**1807**	**48**	**2**	**0**	**0.96**	**0.04**
RF	1807	38	12	0	0.76	0.24
SVM	1807	1	49	0	0.02	0.98

Как видно из табл. 2, из семи рассмотренных классификаторов только три удовлетворяют *требованиям* по обнаружению атак на базы данных, приведенным в постановке задачи. Таковыми классификаторами являются *DT, KNN, NN*. Для них выполняются требования по вероятностям P_{del} и P_{mis}. При этом классификатор *DT* является наилучшим. У классификатора *GBN* выполняются требования по P_{mis}, но он имеет очень плохие значения по вероятности P_{del}.

Остальные классификаторы (*RLC, RF, SVM*) не отвечают требованиям по P_{del} и по P_{mis}. Возможно, это связано с тем, что использовалась обучающая выборка очень малого объема. Однако для того, чтобы получить обучающую выборку объемом в несколько десятков или даже сотен тысяч записей, необходимо использовать фрагмент регистрационного журнала, соответствующий одному дню работы.

По этой же причине оказались нерезультативными исследования временны́х характеристик процессов обучения и тестирования. На использованном в экспериментах компьютере эти временны́е значения находились в пределах нескольких секунд, что соответствует «вычислительному шуму». Мы рассчитываем, что в дальнейших исследованиях на больших массивах данных удастся построить временны́е зависимости для всех используемых классификаторов.

Заключение

Таким образом, представлены: оригинальная формальная постановка задачи, алгоритмы, аспекты реализации и результаты экспериментальной оценки подхода к выявлению аномального поведения пользователей ЦОД вуза, основанного на эвристическом алгоритме снижения размерности признакового пространства наборов данных, используемых для машинного обучения, и применении моделей бинарной классификации. Исходными данными задачи являются множество регистрационных журналов, множество пользователей базы данных, множество отобранных бинарных классификаторов и требования по точности обнаружения аномальных *SQL*-запросов к базам данных ЦОД вуза. Результатом реализации предложенного подхода являются модель признакового пространства наборов данных, содержащих нормальные и аномальные записи со значениями сформированных признаков, и методика поиска аномальных запросов, содержащая этапы обучения и тестирования классификаторов.

Экспериментальная оценка предложенного подхода была проведена на реальных наборах данных, сформированных в ходе работы пользователей ЦОД вуза с базой данных учебного процесса, с использованием множества бинарных классификаторов, включающего классификаторы типов SVM, DT, LR, RF, GNB, BN, ANN. Результаты оценки подтвердили результативность предложенного подхода и его высокую эффективность. Три модели машинного обучения показали точность, отвечающую предъявляемым требованиям.

Дальнейшие исследования направлены на повышение точности обнаружения аномальных *SQL*-запросов за счет совершенствования параметров классификаторов и их комбинирования.

Рецензент: ***Лаута Олег Сергеевич,*** *доктор технических наук, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Российская Федерация.*
E-mail: laos-82@yandex.ru

Литература

1. Воронцов Д.А., Видманов Д.В. Центры обработки данных // Colloquium-Journal. 2020. № 7-1 (59). С. 15—16.
2. Котенко И.В., Саенко И.Б., Чернов А.В., Бутакова М.А. Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта // Труды СПИИ РАН. 2013. № 7 (30). С. 7—25.
3. Чешейко С.И. Особенности архитектуры центра обработки данных в медицинском учреждении // Информационные и телекоммуникационные технологии. 2021. № 49. С. 12—19.
4. Касенова Д.А. Необходимость обеспечения информационной безопасности центра обработки данных // Modern Science. 2021. № 10-1. С. 436—439.
5. Асадуллин Я.Я. Управление информационной безопасностью центра обработки данных // Защита информации. Инсайд. 2020. № 6 (96). С. 12—22.
6. Белянская О.В., Привалов А.Н. О модели угроз информационной безопасности в центрах обработки данных // Изв. Тульского гос. ун-та. Технические науки. 2021. № 9. С. 12—16.
7. Мартышкин А.И. Вариант реализации вычислительного кластера центра обработки данных на примере интернет-центра вуза // XXI век: итоги прошлого и проблемы настоящего плюс. 2022. Т. 11. № 1 (57). С. 28—33.
8. Decker L., Leite D., Giommi L., Bonacorsi D. Real-time anomaly detection in data centers for log-based predictive maintenance using an evolving fuzzy-rule-based approach // 2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). 2020. Pp. 1—8.
9. Shahid N., Ali Shah M. Anomaly detection in system logs in the sphere of digital economy // Competitive Advantage in the Digital Economy (CADE 2021). Online Conference. 2021. Pp. 185—190. DOI: 10.1049/icp.2021.2432 .
10. Nanekaran N.P., Esmalifalak M., Narimani M. Fast anomaly detection in micro data centers using machine learning techniques // 2020 IEEE 18th International Conference on Industrial Informatics (INDIN). 2020. Pp. 86—93. DOI: 10.1109/INDIN45582.2020.9442233 .
11. Deka P.K., Bhuyan M.H., Kadobayashi Y., Elmroth E. Adversarial impact on anomaly detection in cloud datacenters // 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC). 2019. Pp. 188—18809. DOI: 10.1109/PRDC47002.2019.00049 .
12. Chen J., Wang L., Hu Q. Machine learning-based anomaly detection of ganglia monitoring data in HEP data center // EPJ Web Conf. 2020. Vol. 245. Article No. 07061. DOI: 10.1051/epjconf/202024507061 .
13. Salman T., Bhamare D., Erbad A., Jain R., Samaka M. Machine learning for anomaly detection and categorization in multi-cloud environments // 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). 2017. Pp. 97—103. DOI: 10.1109/CSCloud.2017.15 .

14. Hlaing Z. C. S. S., Khaing M. A detection and prevention technique on SQL injection attacks // 2020 IEEE Conference on Computer Applications (ICCA). 2020. Pp. 1—6. DOI: 10.1109/ICCA49400.2020.9022833 .
15. M G., H B P. Semantic query-featured ensemble learning model for SQL-injection attack detection in IoT-ecosystems // IEEE Transactions on Reliability. 2022. Vol. 71. No. 2. Pp. 1057—1074. DOI: 10.1109/TR.2021.3124331 .
16. Prarthana T.S., Gangadhar N.D. User behaviour anomaly detection in multidimensional data // 2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM). 2017. Pp. 3—10. DOI: 10.1109/CCEM.2017.19 .
17. Xie X., Ren C., Fu Y., Xu J., Guo J. SQL injection detection for web applications based on elastic-pooling CNN // IEEE Access. 2019. Vol. 7. Pp. 151475—151481. DOI: 10.1109/ACCESS.2019.2947527 .
18. Xiao Z., Zhou Z., Yang W., Deng C. An approach for SQL injection detection based on behavior and response analysis // 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN). 2017. Pp. 1437—1442. DOI: 10.1109/ICCSN.2017.8230346 .
19. Hasan M., Balbahaith Z., Tarique M. Detection of SQL injection attacks: a machine learning approach // 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA). 2019. Pp. 1—6. DOI: 10.1109/ICECTA48151.2019.8959617 .
20. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИ РАН. 2016. № 2 (45). С. 207—244.
21. Котенко И.В., Саенко И.Б., Браницкий А.А., Паращук И.Б., Гайфулина Д.А. Интеллектуальная система аналитической обработки цифрового сетевого контента для защиты от нежелательной информации // Информатика и Автоматизация. 2021. № 4. С. 755—788. DOI: 10.15622/ia.20.4.1 .
22. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access, 2018, Vol. 6, pp. 72714—72723. DOI: 10.1109/ACCESS.2018.2881 998 .

DETECTING ABNORMAL BEHAVIOUR OF USERS OF DATA PROCESSING CENTRES OF HIGHER EDUCATION INSTITUTIONS

Igor' Kotenko, *Dr.Sc. (Technology), Professor, Chief Researcher and Head of the Computer Security Problems Laboratory of the Saint Petersburg Federal Research Centre of the Russian Academy of Sciences, Saint Petersburg, Russian Federation.*
E-mail: ivkote@comsec.spb.ru

Igor' Saenko, *Dr.Sc. (Technology), Professor, Leading Researcher at the Computer Security Problems Laboratory of the Saint Petersburg Federal Research Centre of the Russian Academy of Sciences, Saint Petersburg, Russian Federation.*
E-mail: ibsaen@comsec.spb.ru

Mazen Hamed Al-Barri, *postgraduate student at the S. Budyonnyi Military Academy of Communications, Saint Petersburg, Russian Federation.*
E-mail: mazenb51@gmail.com

Keywords: *information security, insider, computer attack, database, SQL injection, machine learning, classifier, registration journal, data set.*

Abstract

Purpose of the paper: setting up the problem of ensuring the required precision of detecting abnormal behaviour of users of data processing centres of higher education institutions (HEI) and find its solution using machine learning methods.

Methods of study: system analysis of the problem of detecting abnormal behaviour of users of data processing centres of HEI and supervised machine learning methods.

Study findings: an original setup of the problem of detecting abnormal behaviour of users of data processing centres of a HEI is proposed which is oriented towards using machine learning methods. An approach to reducing the dimensionality of the initial feature space as well as an algorithm implementing it is developed based on typing of data table names present in SQL query texts. An implementation of the proposed approach using different machine learning models was carried out.

An experimental assessment evaluation of the proposed approach was performed which confirmed its high efficiency and made it possible to identify the most appropriate classifiers for solving this problem, which are: the decision tree, k-nearest neighbours method and multilayer neural network.

References

1. Vorontsov D.A., Vidmanov D.V. Tsentry obrabotki dannykh. Colloquium-Journal, 2020, No. 7-1 (59), pp. 15—16.
2. Kotenko I.V., Saenko I.B., Chernov A.V., Butakova M.A. Postroenie mnogourovnevoi intellektual'noi sistemy obespecheniia informatsionnoi bezopasnosti dlia avtomatizirovannykh sistem zheleznodorozhnogo transporta. Trudy SPII RAN, 2013, No. 7 (30), pp. 7—25.
3. Chesheiko S.I. Osobennosti arkhitektury tsentra obrabotki dannykh v meditsinskom uchrezhdenii. Informatsionnye i telekommunikatsionnye tekhnologii, 2021, No. 49, pp. 12—19.
4. Kasenova D.A. Neobkhodimost' obespecheniia informatsionnoi bezopasnosti tsentra obrabotki dannykh. Modern Science, 2021, No. 10-1, pp. 436—439.
5. Asadullin Ia.Ia. Upravlenie informatsionnoi bezopasnost'iu tsentra obrabotki dannykh. Zashchita informatsii. Insaid, 2020, No. 6 (96), pp. 12—22.
6. Belianskaia O.V., Privalov A.N. O modeli ugroz informatsionnoi bezopasnosti v tsentrakh obrabotki dannykh. Izv. Tul'skogo gos. un-ta. Tekhnicheskie nauki, 2021, No. 9, pp. 12—16.
7. Martyshkin A.I. Variant realizatsii vychislitel'nogo klastera tsentra obrabotki dannykh na primere internet-tsentra vuza. XXI vek: itogi proshlogo i problemy nastoiashchego plius, 2022, t. 11, No. 1 (57), pp. 28—33.
8. Decker L., Leite D., Giommi L., Bonacorsi D. Real-time anomaly detection in data centers for log-based predictive maintenance using an evolving fuzzy-rule-based approach. 2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2020, pp. 1—8.
9. Shahid N., Ali Shah M. Anomaly detection in system logs in the sphere of digital economy. Competitive Advantage in the Digital Economy (CADE 2021). Online Conference, 2021, pp. 185—190. DOI: 10.1049/icp.2021.2432 .
10. Nanekaran N.P., Esmalifalak M., Narimani M. Fast anomaly detection in micro data centers using machine learning techniques. 2020 IEEE 18th International Conference on Industrial Informatics (INDIN), 2020, pp. 86—93. DOI: 10.1109/INDIN45582.2020.9442233 .
11. Deka P.K., Bhuyan M.H., Kadobayashi Y., Elmroth E. Adversarial impact on anomaly detection in cloud datacenters. 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), 2019, pp. 188—18809. DOI: 10.1109/PRDC47002.2019.00049 .
12. Chen J., Wang L., Hu Q. Machine learning-based anomaly detection of ganglia monitoring data in HEP data center. EPJ Web Conf, 2020, Vol. 245, Article No. 07061. DOI: 10.1051/epjconf/202024507061 .
13. Salman T., Bhamare D., Erbad A., Jain R., Samaka M. Machine learning for anomaly detection and categorization in multi-cloud environments. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 97—103. DOI: 10.1109/CSCloud.2017.15 .
14. Hlaing Z. C. S. S., Khaing M. A detection and prevention technique on SQL injection attacks. 2020 IEEE Conference on Computer Applications (ICCA), 2020, pp. 1—6. DOI: 10.1109/ICCA49400.2020.9022833 .
15. M G., H B P. Semantic query-featured ensemble learning model for SQL-injection attack detection in IoT-ecosystems. IEEE Transactions on Reliability, 2022, Vol. 71, No. 2, pp. 1057—1074. DOI: 10.1109/TR.2021.3124331 .
16. Prarthana T.S., Gangadhar N.D. User behaviour anomaly detection in multidimensional data. 2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2017, pp. 3—10. DOI: 10.1109/CCEM.2017.19 .
17. Xie X., Ren C., Fu Y., Xu J., Guo J. SQL injection detection for web applications based on elastic-pooling CNN. IEEE Access, 2019, Vol. 7, pp. 151475—151481. DOI: 10.1109/ACCESS.2019.2947527 .
18. Xiao Z., Zhou Z., Yang W., Deng C. An approach for SQL injection detection based on behavior and response analysis. 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN), 2017, pp. 1437—1442. DOI: 10.1109/ICCSN.2017.8230346 .
19. Hasan M., Balbahaith Z., Tarique M. Detection of SQL injection attacks: a machine learning approach. 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), 2019, pp. 1—6. DOI: 10.1109/ICECTA48151.2019.8959617 .
20. Branitskii A.A., Kotenko I.V. Analiz i klassifikatsiia metodov obnaruzheniia setevykh atak. Trudy SPII RAN, 2016, No. 2 (45), pp. 207—244.
21. Kotenko I.V., Saenko I.B., Branitskii A.A., Parashchuk I.B., Gaifulina D.A. Intellektual'naia sistema analiticheskoi obrabotki tsifrovogo setevogo kontenta dlia zashchity ot nezhelatel'noi informatsii. Informatika i Avtomatizatsiia, 2021, No. 4, pp. 755—788. DOI: 10.15622/ia.20.4.1 .
22. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning. IEEE Access, 2018, Vol. 6, pp. 72714—72723. DOI: 10.1109/ACCESS.2018.2881 998 .

РИСК-ОРИЕНТИРОВАННАЯ АТРИБУТИВНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ ОРГАНИЗАЦИЙ ВЫСШЕГО ОБРАЗОВАНИЯ

Магомедов Ш.Г.[1], Козачок А.В.[2], Тарланов А.Т.[3]

Ключевые слова: *безопасность на основе рисков, динамические модели, риск-ориентированная модель управления доступом, ИТ-инфраструктура сервисов в сфере образования, атрибуты, модели управления доступом.*

Аннотация

Цель статьи: разработка риск-ориентированной модели управления доступом, изменяющей правила доступа в зависимости от текущего уровня риска реализации угроз информационной безопасности на основе анализа ключевых процессов в ИТ-инфраструктуре и событий информационной безопасности.

Методы исследований: анализ моделей управления доступом, теоретическая формализация, моделирование.

Результат: подход показал перспективность применения по сравнению с традиционными моделями управления доступом, а результаты исследований позволили выдвинуть предложения по дальнейшему развитию данного направления.

Научная новизна: предложена риск-ориентированная атрибутивная модель управления доступом на примере сервисов системы высшего образования и разработана политика управления доступом на основе промышленного стандарта XACML, изменяющая правила доступа с учетом оценки риска в реальном времени.

DOI: 10.21681/1994-1404-2023-1-72-82

1. Введение

Изменение геополитической обстановки в последние годы привело к необходимости пересмотра не только текущих аспектов защиты информации, но и фундаментальных основ в области информационной безопасности. Одним из базовых принципов в процессе обеспечения информационной безопасности является применение политик безопасности, позволяющих реализовывать на практике технические, организационные и правовые меры по обеспечению защищенности как объектов критической информационной инфраструктуры и государственных информационных систем, так и обрабатываемой информации. Существующие подходы к управлению безопасностью основаны на применении статических или частных политик безопасности (средств защиты) на объектах критической информационной инфраструктуры, информационных системах и других объектах информатизации.

Применение статических подходов безопасности позволяет обеспечить требуемый уровень защиты от известных и существующих угроз безопасности, однако требует внесения изменений в существующую конфигурацию средств защиты при модификации или реконфигурировании технических средств объектов информатизации при существенном изменении внешних условий.

Традиционные модели управления доступом используют логику доступа к ресурсам на основе правил управления доступом. Подобный подход решает большинство проблем при разграничении доступа к объектам, однако имеет существенный недостаток, заключающийся в применении статичных, предопределенных политик безопасности, которые не гарантируют безопасность объектов доступа в изменяющихся условиях окружающей обстановки. В различных ситуациях тра-

[1] ***Магомедов Шамиль Гасангусейнович,*** *кандидат технических наук, доцент, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» РТУ МИРЭА, г. Москва, Российская Федерация. ORCID: 0000-0001-8560-1937.*
E-mail: magomedov_sh@mirea.ru

[2] ***Козачок Александр Васильевич,*** *доктор технических наук, доцент, профессор кафедры КБ-4 «Интеллектуальные системы информационной безопасности» РТУ МИРЭА, г. Москва, Российская Федерация. ORCID: 0000-0002-6501-2008.*
E-mail: kozachok_a@mirea.ru

[3] ***Тарланов Арслан Тарланович,*** *доцент кафедры КБ-14 «Цифровые технологии обработки данных» РТУ МИРЭА, г. Москва, Российская Федерация. ORCID: 0000-0002-7508-9682.*
E-mail: tarlanov@mirea.ru

диционные модели формируют одно и то же решение по управлению доступом [1]. Подобное поведение не позволяет использовать их в качестве адаптивных методов в изменяющихся условиях.

В последние годы по всему миру часто фиксируют инциденты, связанные с утечкой конфиденциальной информации по вине внутренних нарушителей как в частных, так и в государственных учреждениях. Из-за недетерминированного поведения пользователей иногда достаточно трудно отличить легитимные запросы доступа на предоставление полномочий на основе традиционных статичных моделей управления доступом [2].

2. Исследования в области динамических моделей управления доступом

Динамические модели управления доступом используют не только политики доступа, но и параметры реального времени, которые рассчитываются во время запроса доступа и их значение определяет решение о предоставлении доступа. Доверие к источнику запросов, риск, контекст, история и операционные потребности — примеры параметров реального времени.

В работах [3, 4] предлагаются риск-ориентированные модели управления доступом к устройствам типа Internet of Things и Internet of Vehicles. Значение риска рассчитывается на основе параметров: контекст пользователя и агента, ценности ресурса, критичность действия, базы данных рисков (история рисков). На основе полученного значения риска принимается решение о предоставлении доступа к объекту.

Авторы исследования [5] отмечают недостатки дискреционных (DAC), мандатных (MAC) и ролевых моделей управления доступом (RBAC) при функционировании в экосистемах больших данных. В статье описана риск-ориентированная модель управления доступом на основе контента (RCBAC), позволяющая решить проблему утечки конфиденциальных данных по вине внутренних нарушителей за счет применения риск-ориентированной модели управления доступом авторизованных пользователей к ресурсам. Разработанная авторами модель оценивает риск на основе содержимого данных, поведения пользователя при доступе к объекту и истории доступа пользователя. Поведение пользователя, атрибуты пользователя сравниваются с атрибутами объекта доступа, учитывается также контент запрашиваемого объекта. История доступа пользователя учитывает предыдущие запросы пользователя к объектам.

В работе [6] отмечаются также недостатки существующих моделей управления доступом для облачной инфраструктуры, поскольку статические методы описания правил доступа ведут к значительным рискам нарушения информационной безопасности и не могут полностью реализовать потребности и функционал облачных сервисов. Для решения обозначенных проблем авторы предлагают динамическую риск-ориентированную модель управления доступом. Модель состоит из четырех основных блоков: обнаружение аномалий на основе правил, оценка риска на основе потока данных, комплексное принятие решений, динамическая подстройка порогового значения риска.

В работе [7] приводится описание оценки риска как комплексного свойства, состоящего из идентификации, анализа и оценки риска.

Цель идентификации риска заключается в определении событий, способных привести к потенциальной потере данных, и получении представления о причинах, способах и месте возникновения утечки данных. Идентификация риска включает риски независимо от того, находится ли их источник под контролем организации или нет, даже если источники или причины риска неочевидны.

Анализ риска определяет значения вероятности и последствия риска. Анализ рисков может быть выполнен с разной степенью детализации в зависимости от уязвимостей или инцидентов. Методология анализа риска включает в себя три подхода: качественный, количественный и их комбинацию. Обычно сначала выполняется качественный анализ: он позволяет получить первую информацию об уровне риска и оценить, действительно ли риск критичен. После этого может быть проведена более подробная количественная оценка. Качественный анализ рисков использует шкалу, которая описывает степень риска (например, информативный, низкий, средний, высокий и критический) для воздействия на бизнес и вероятности возникновения. Эта шкала может быть адаптирована к различным ситуациям и типам риска. Результат этого подхода представляется в виде строки данных (категории).

Количественный анализ риска использует числовое значение шкалы как для воздействия, так и для вероятности. Качество такого анализа зависит от качества входных данных (точности числовых значений) и достоверности используемых моделей (например, насколько они соответствуют поведению системы, корректируют данные измерений). Способ раскрытия воздействия и вероятности будет изменен в зависимости от типа риска и цели, для которой используется оценка риска. При анализе следует также учитывать неопределенность и изменчивость как влияния на бизнес, так и вероятности. Оценка риска — это процесс, используемый для сравнения результата оценки риска, достигнутого в ходе анализа, с заданными критериями риска, чтобы определить, является ли уровень риска приемлемым или нет.

Для определения риска в работе определяются 4 категории: место исходящего запроса (офис, дом, магазин, кинотеатр, аэропорт), время инициации запроса (8—16 ч., 16—22 ч., 22—6 ч., 6—8 ч.), сервис (банковский сектор, e-mail, серфинг сайтов, электронная коммерция), устройство (персональный компьютер, ноутбук, смартфон). Далее на основе веса контекста категории, веса безопасности контекста данных и фактора зависимости рассчитывается минимальный уровень безопасности объекта, который должен обеспечиваться.

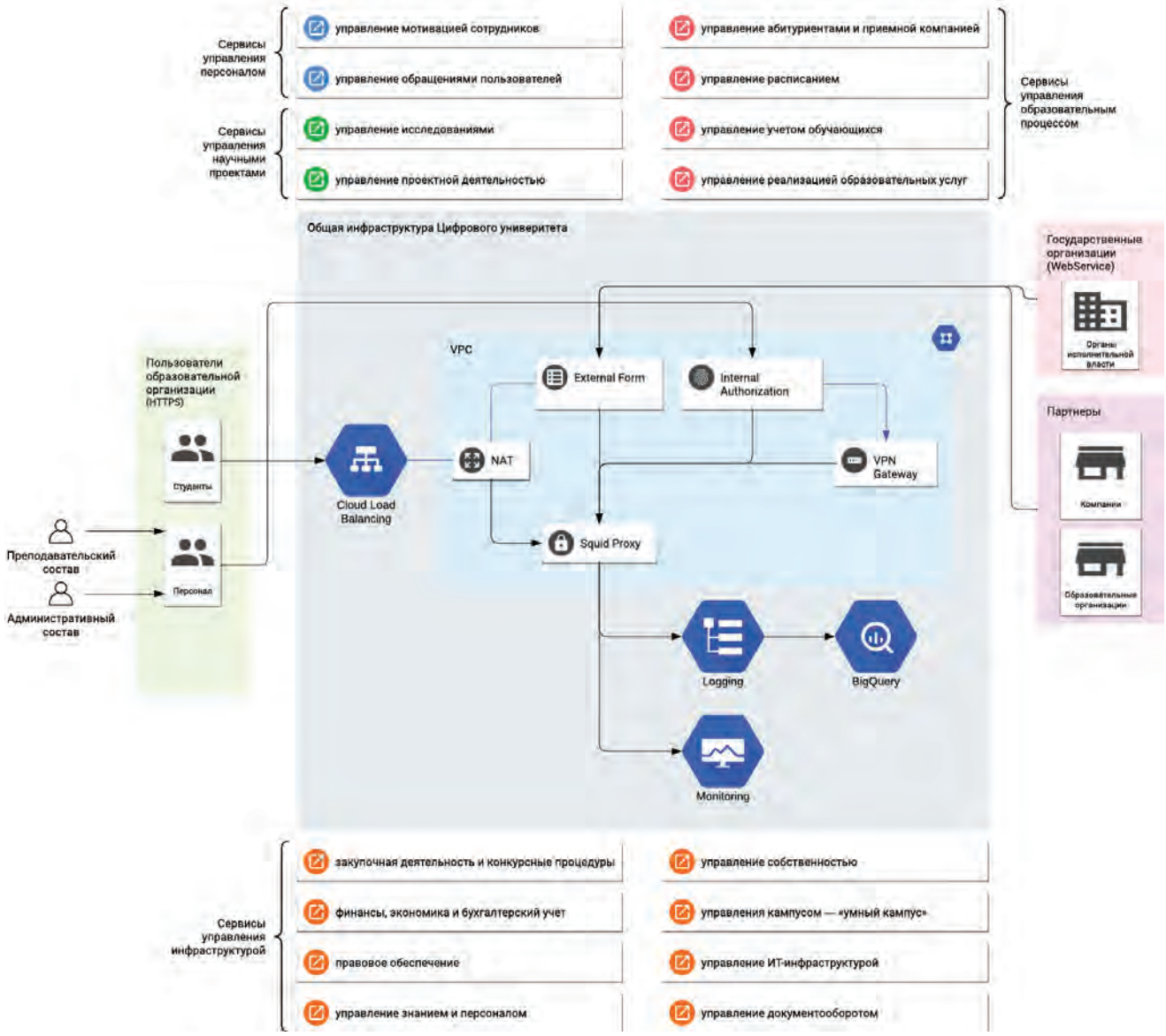

Рис. 1. Типовая структура ИТ-сервисов высшего образования

Авторы исследования [8] описывают риск-ориентированную систему управления доступом с учетом конфиденциальности для систем обнаружения угроз. Каждый запрос на доступ оценивается системой путем сравнения риска конфиденциальности и надежности запроса. Когда риск слишком велик по сравнению с уровнем доверия, фреймворк может применять стратегии адаптивной корректировки для снижения риска (например, путем выборочного запутывания данных) или для повышения уровня доверия для выполнения заданной задачи (например, наложения на пользователя обязательных к исполнению обязательств). Фреймворк может одновременно удовлетворять требованиям как конфиденциальности, так и полезности. Экспериментальные результаты, полученные авторами, показывают, что фреймворк приводит к значимым результатам и производительности в режиме реального времени в рамках решения для обнаружения промышленных угроз. Фреймворк состоит из 4 блоков: риск-ориентированный модуль контроля доступа, блок оценки риска, модуль оценки доверия запроса и модуль управления доверием и риском.

3. Управление доступом в организациях высшего образования

В современном цифровом обществе система обучения и доступа к образовательным ресурсам играет значительную роль, что было продемонстрировано с помощью анализа функционирования информационной образовательной среды в быстро меняющихся реалиях [9, 10].

Внедрение информационных технологий (ИТ) дает возможность учреждениям в сфере высшего образования усилить свои конкурентные преимущества с помощью перехода к более актуальной бизнес-стратегии, которая отвечает современным тенденциям и реализует задачи, стоящие перед образовательным учреж-

дением. С учетом последствий пандемии и различных ограничений по использованию, предлагаемых зарубежными разработчиками, образовательным учреждениям пришлось перейти на формат дистанционного обучения. Этот переход увеличил значение ИТ и, в частности, дистанционных образовательных технологий в сфере образования. Значительное число программ информатизации разработано с целью обновления ИТ-инфраструктуры учреждений образования, модернизации действующего лабораторного оснащения. Эти программы ориентированы на глобальную информатизацию, которая способствовала бы эффективному управлению организацией, предоставлению учащимся образовательных услуг, в т. ч. с использованием дистанционных технологий. Это определенным образом влияет на деятельность организаций: ИТ-инфраструктура образовательного учреждения должна быть безопасной, актуальной и масштабируемой. Именно эти требования служат основой для разработки, реализации и функционирования информационных систем в образовании.

ИТ-инфраструктурой образовательного учреждения называется совокупность программных, аппаратных, телекоммуникационных продуктов и ресурсов, необходимых для организации и реализации образовательного процесса (рис. 1).

К ИТ-инфраструктуре образовательного учреждения предъявляются следующие требования: обеспечение управления правами доступа всех пользователей, т. е. должен быть разграничен доступ пользователей к информационным ресурсам организации на основе правил, заданных в информационной системе, и должен выполняться контроль соблюдения этих правил.

В схему ИТ-инфраструктуры входят: 1) модели управления доступом (мандатные, дискреционные, ролевые); 2) виды доступа (просмотр, внесение изменений, создание, удаление, выполнение); 3) правила разграничения доступа, которые могут иметь привязку к ролям, спискам, значениям атрибутов, меткам безопасности и др.

Каждая из классических моделей управления доступом обладает своими преимуществами и недостатками, наиболее распространенной (по причине доступности и простоты реализации) является ролевая модель управления доступом (англ. role-based access control, RBAC). Суть подхода заключается в создании ролей, описывающих полномочия пользователей в соответствии с их должностными обязанностями. На основе ролей проводится проверка возможности выполнения того или иного действия пользователем.

Если иерархия ролей задана согласно штатному расписанию (преподаватель, администратор, студент и др.), то такой подход можно применять. Одной должности ставится в соответствие одна роль. Однако с увеличением сервисов, появлением новых кампусов, добавлением новых филиалов ролевая структура усложняется и становится многомерной, что влечет за собой создание новых ролей, которые будут соответствовать комбинациям всех атрибутов. Последствием этого является большое количество ролей, размытие регламента, а также сложности управления из-за отсутствия четкой иерархии.

Из этого следует, что как только для регламентов необходим контроль данных или они становятся многомерными, ролевая модель становится не только бесполезной для текущих проблем контроля доступа, но даже способствует появлению новых проблем.

Для решения проблем ролевого управления доступом был разработан другой подход, основанный на атрибутах (англ. attribute-based access control, ABAC) [11].

Главное отличие этого подхода — то, что отдельная ситуация оценивается не с позиции роли пользователя и действия, которые он планирует выполнить, а с точки зрения относящихся к ним атрибутов. Регламент — это набор условий, где разные атрибуты должны соответствовать требованиям, предъявляемым к ним для предоставления доступа.

4. Атрибутивная модель управления доступом в организациях высшего образования

Проанализировав ролевую модель управления доступом, можно сделать вывод, что данная модель подходит только для реализации простых регламентов. С ростом сложности снижается целесообразность применения ролевой модели управления доступом, потому что стоимость поддержки системы контроля доступа заметно увеличивается. При достаточно высоком уровне сложности правил применение данного подхода нецелесообразно.

Атрибутивная модель управления доступом не ограничивает сложность процессов. Из-за более простой реализации в рамках применения этого подхода стоимость поддержки при реализации более сложных правил не увеличивается. Кроме того, появляется возможность обеспечения контроля доступа и к действиям, и к данным. Данная модель является набором условий, в которых атрибуты должны соответствовать требованиям, предъявляемым к ним. Можно явно выделить несколько категорий атрибутов:

- атрибуты ресурса (тип, создатель, стоимость, название и др.);
- атрибуты субъекта (имя, отдел, должность, лимит утверждений и др.);
- атрибуты действия (название);
- атрибуты среды (IP-адрес, время, устройство).

Для того чтобы выполнить авторизацию, сравнивают значения всех атрибутов в момент проверки прав и ожидаемые значения. Доступ к ресурсу обеспечивается при выполнении всех условий.

Спроектируем ИТ-инфраструктуру образовательного учреждения с применением атрибутивной модели управления доступом.

Инфраструктура образовательного учреждения включает в себя значительное число связанных между

собой элементов, безопасность которых необходимо обеспечить:

- сервисы управления образовательным процессом;
- сервисы управления научными проектами;
- сервисы управления персоналом;
- сервисы контроля и управления доступом;
- сервисы бухгалтерского учета;
- сервисы управления инфраструктурой и др.

Среди угроз ИТ-инфраструктуре организации, работающей в сфере образования, можно назвать рассылку сообщений с вредоносными вложениями, попытки несанкционированного доступа к данным организации и многие другие. Злоумышленники разрабатывают все более совершенные механизмы атаки на информационные системы организаций, в том числе образовательных учреждений. Тогда в качестве атрибутов доступа ИТ-сервисов высшего образования можно выделить следующие атрибуты:

- роль: студент, преподаватель, административный персонал, внешние сущности, руководители подразделений;
- тип устройства доступа: рабочая ПЭВМ, ноутбук, мобильное устройство;
- тип сервиса: сервисы управления образовательным процессом, научными проектами, персоналом, инфраструктурой, сервисы контроля и управления доступом, сервисы бухгалтерского учета;
- местоположение: кампус 1, кампус 2, …, кампус N, филиал;
- тип подключения: VPN, внутренняя сеть, сеть Интернет;
- действие: запись, чтение, создание, удаление.

Необходимым требованием к ИТ-инфраструктуре организации является обеспечение защиты информационной образовательной среды организации и постоянного мониторинга и верификации пользователей. При этом пользователь должен иметь возможность оставаться в сеансе доступа к информационному ресурсу в течение времени, необходимого для работы. Работы в области адаптивной безопасности [12] показали, как применять этот вид проверок на основе различных техник.

Одна из них — это «контекстно-зависимая безопасность».

Этот подход опирается на контекстно-зависимую информацию, такую как геолокация, время доступа, репутация определенного IP-адреса или домена, тип используемого устройства и др., для принятия решений по предоставлению доступа. Вся эта информация, собранная и обработанная динамически, может обеспечить бóльшую защищенность и гранулярность относительно статических методов в различных областях применения. Эта концепция появляется в большинстве случаев в сценариях аутентификации и авторизации в распределенных системах, решение о предоставлении доступа может быть основано на различных процедурах или атрибутах в зависимости от контекста конкретного запроса.

Дополнительной техникой является инкрементная (интеллектуальная) безопасность.

Этот подход обычно сочетает в себе различные методы и инструменты, такие как большие данные, аналитика или управление информацией и событиями безопасности (SIEM), для обнаружения аномалий, выбросов или отклонений от стандартного поведения и принятия соответствующих мер. Инкрементальная (интеллектуальная) безопасность основана на сборе, стандартизации и анализе данных, генерируемых сетями, приложениями, базами данных, журналами и другой инфраструктурой в режиме реального времени. Эта информация оценивается и обрабатывается (с помощью машинного обучения, распознавания образов и др.) для перевода данных в удобочитаемый формат, который поддерживает принятие обоснованных решений.

5. Риск-ориентированная модель управления доступом для организаций высшего образования

Модель управления доступом на основе рисков является динамической моделью, которая функционирует в режиме реального времени и использует контекстную информацию для принятия решений о доступе к объекту. Эта модель выполняет расчет риска по каждому запросу на доступ к объекту и принимает решение динамически на основе полученного значения риска. Основная проблема, связанная с использованием этой модели, заключается в обеспечении оперативного, надежного и точного метода оценки риска, особенно в условиях отсутствия данных для количественного описания риска и оценки его воздействия.

Динамическая безопасность также включает в себя безопасность на основе рисков. Эта модель позволяет идентифицировать различные риски каждого из активов организации, расставляя приоритеты в отношении стоимости смягчения последствий, качества опыта и удобства использования, функциональности и др., что означает снижение этих рисков до приемлемого уровня. Этот подход позволяет организациям иметь дело с типичными компромиссами безопасности.

Необходимо постоянно отслеживать, измерять и оценивать риски, чтобы обеспечить адекватную безопасность, основанную на рисках. Необходимо также решить, как будут обрабатываться риски при их появлении. Эта методика может привести к эффективным и действенным результатам.

Большинство сценариев применения этого метода снова фокусируются на управлении доступом. Но есть и другие примеры в различных областях применения, таких как промышленные системы управлении или обработка данных.

Формирование ИТ-инфраструктуры вуза для продуктивной работы преподавателей, обучающихся и сотрудников невозможно без учета актуальных тенденций в сфере ИТ. На рис. 2 представлена риск-

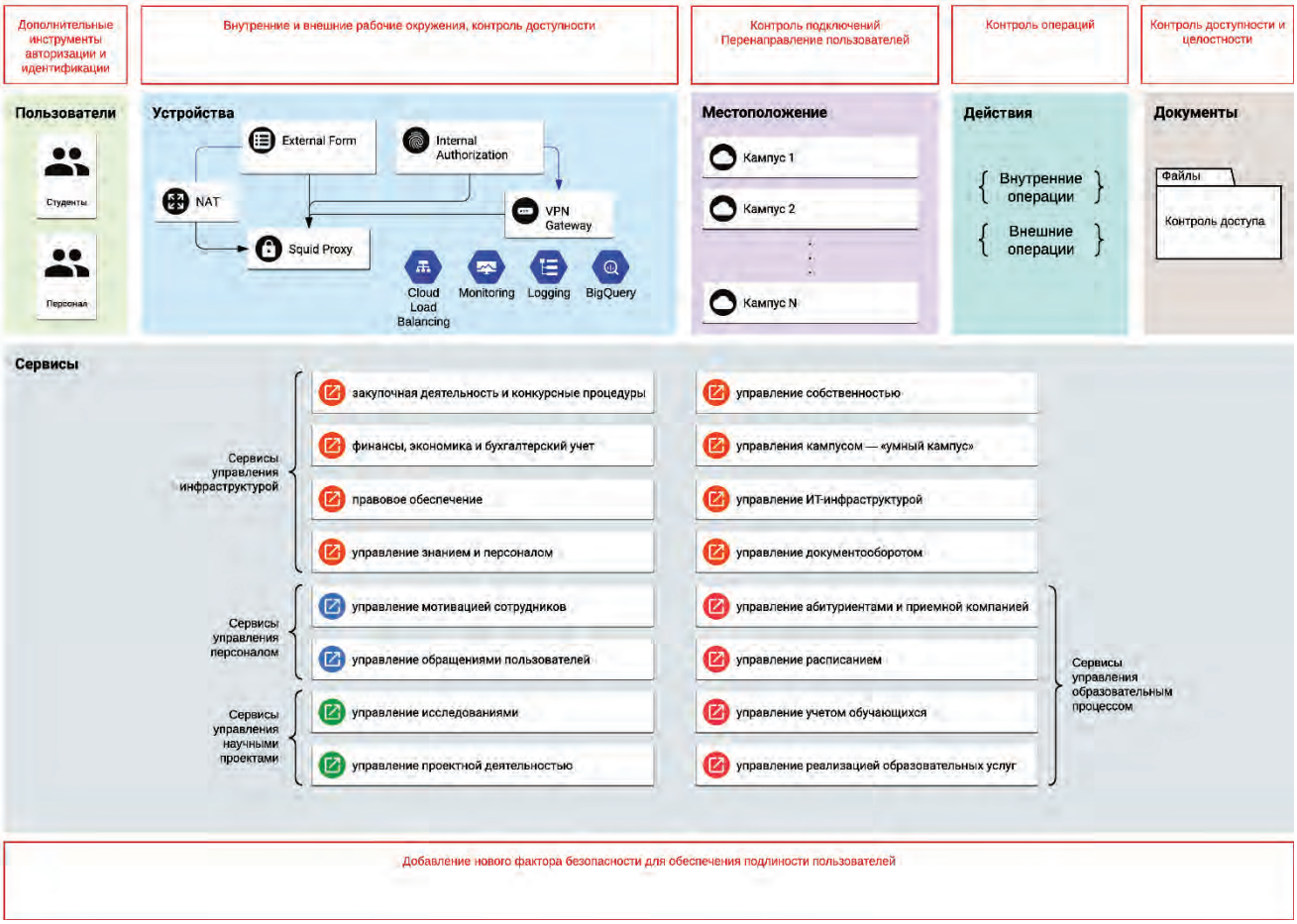

Рис. 2. Риск-ориентированная атрибутивная модель управления доступом для систем высшего образования

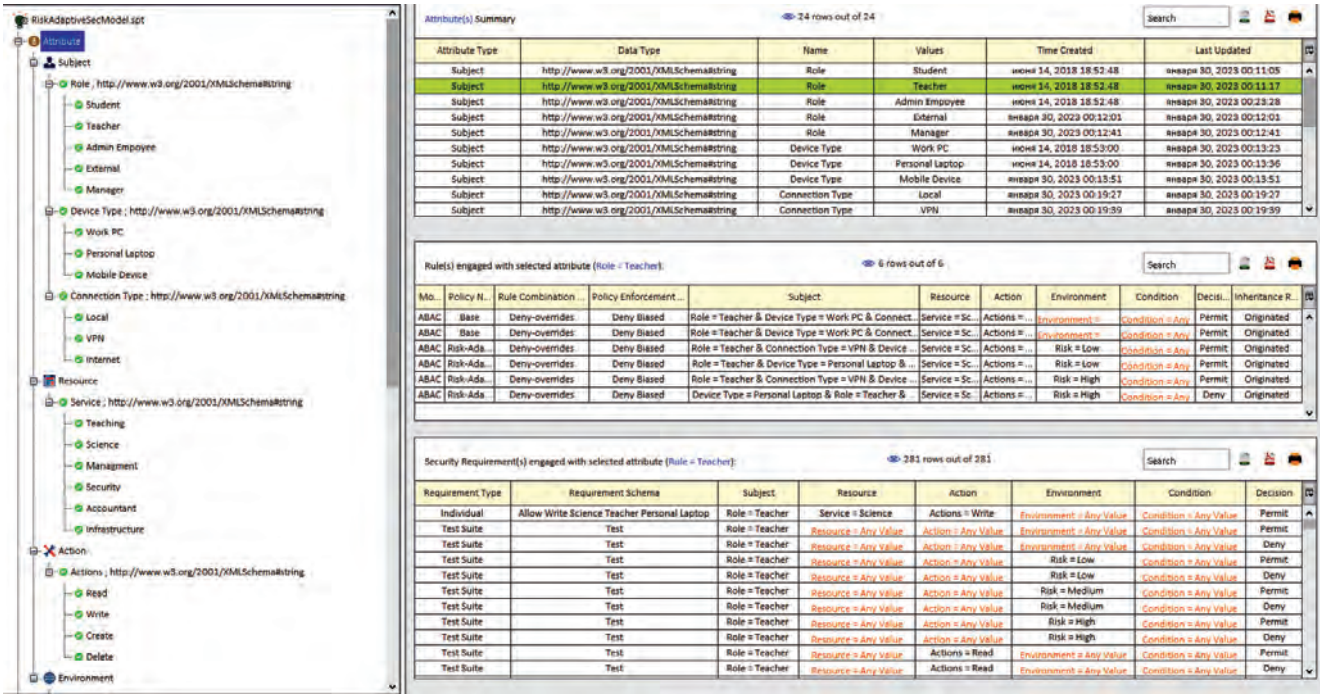

Рис. 3. Атрибуты объектов и субъектов модели

ABAC(s) Summary — 2 rows out of 2 — Search

Model	Policy Name	Rule Combination Algorithm	Policy Enforcement Algorithm	No. of Rule(s)	Time Created	L
ABAC	Base	Deny-overrides	Deny Biased	2	января 30, 2023 00:23:01	января
ABAC	Risk-Adaptive	Deny-overrides	Deny Biased	4	января 30, 2023 00:26:16	января

Rule (s) defined with selected policy (Risk-Adaptive): — 4 rows out of 4 — Search

Sequence No	Subject	Resource	Action	Environment	Condition	Decision
1	Role = Teacher & Connection Type = VPN & Device Type = Personal Laptop	Service = Science	Actions = Read	Risk = Low	Condition = Any Value	Permit
2	Role = Teacher & Device Type = Personal Laptop & Connection Type = VPN	Service = Science	Actions = Write	Risk = Low	Condition = Any Value	Permit
3	Role = Teacher & Connection Type = VPN & Device Type = Personal Laptop	Service = Science	Actions = Read	Risk = High	Condition = Any Value	Permit
4	Device Type = Personal Laptop & Role = Teacher & Connection Type = VPN	Service = Science	Actions = Write	Risk = High	Condition = Any Value	Deny

Рис. 4. Политики атрибутивного управления доступом

ориентированная модель управления доступом для организаций высшего образования. Оценка риска реализации угроз производится на основе анализа событий безопасности в SIEM-системе и анализа поведения пользователей с учетом выбранных ранее атрибутов.

Выбор подхода к количественной оценке рисков при этом может быть обусловлен следующими факторами:

– принятая модель угроз;
– модель нарушителя;
– атрибуты безопасности управления доступом.

За основу при этом предлагается взять подход к количественной оценке рисков на основе нечетких множеств [13].

Предлагаемая модель может позволить осуществить переход от статических правил управления [14, 15] к динамически изменяемым и при этом описываемым атрибутивной моделью управления доступом. Значение риска в этом случае является дополнительным атрибутом безопасности управления доступом.

Разработка модели и ее валидация производилась в среде Security Policy Tool (URL: https://securitypolicytool.com/). Для субъектов и объектов модели были заданы соответствующие атрибуты, описанные в разделе 4 статьи (рис. 3).

Были также заданы две политики атрибутивного управления доступом, в одной из которых производился учет значения рисков, а в другой — нет (рис. 4).

В риск-ориентированной модели управления доступом при доступе преподавателя к научным сервисам с личного ноутбука при подключении VPN и высоком значении риска доступ на запись запрещен.

Для валидации корректности модели был задан инвариант безопасности, разрешающий доступ препо-

Policy Verification (января 30, 2023 00:31:53)(s) Summary — 1 rows out of 1 — Search

Status	Name	Verification T...	Verification Tech...	Number of Poli...	Combination Algo...	Enforcement Algor...	Policy List
Outdat...	Policy Verification (января 30, 2023 ...	Standard	Merged Policy	2	Deny-overrides	Deny Biased	ABAC:Base, ABAC:Risk-A...

Warning : Changes to following input parameter(s) may render previous verification result inaccurate.

Requirement Schema(s) : Allow Write Science Teacher Personal Laptop

Please Refresh Policy Verification (января 30, 2023 00:31:53)(s) to ensure recent changes are updated in your results.

Result(s) with selected verification (Policy Verification (января 30, 2023 00:31:53)) — 2 rows out of 2 — Search

Requirement Schema	Subject	Resource	Action	Environment	Condition	Decision	Verification Result
Test	Role = Teacher	Service = Science	Actions = Write	Environment = Any Value	Condition = Any Value	Permit	FALSE
Test	Device Type = Personal Laptop	Service = Science	Actions = Write	Environment = Any Value	Condition = Any Value	Permit	FALSE

Рис. 5. Результаты тестирования инварианта безопасности для заданных политик

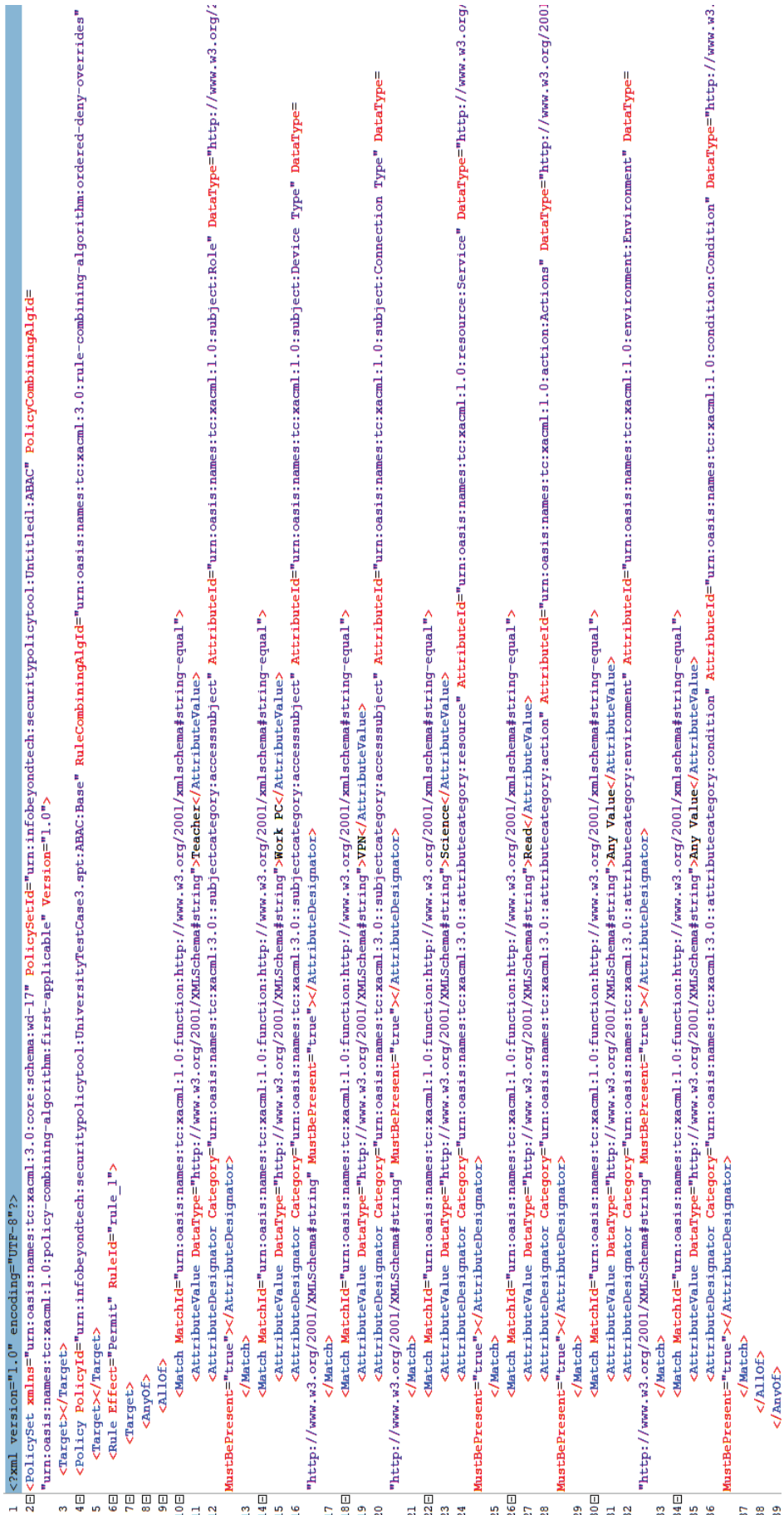

Рис. 6. Фрагмент риск-ориентированной политики управления доступом на языке XACML

давателя к научным сервисам с личного ноутбука при подключении VPN на запись. Тестирование моделей позволило выявить невыполнение данного инварианта для риск-ориентированной модели управления доступом (рис. 5).

Невыполнение указанного инварианта подтверждает корректную работу модели с учетом анализа рисков безопасности. Дополнительно была сгенерирована политика в формате XACML для обеспечения возможности использования ее в инфраструктуре образовательных организаций (рис. 6). XACML (расширяемый язык разметки управления доступом) — это открытый стандарт для авторизации и управления доступом, который обеспечивает детальный контроль над тем, кто из пользователей имеет доступ к каким ресурсам и какие действия может выполнять. Он используется для определения политик управления доступом в распределенных системах и приложениях.

6. Выводы

Предложенная риск-ориентированная модель управления доступом позволяет осуществить переход от статических правил управления доступом, используемых в классических моделях управления доступом, к динамическим, изменяющимся правилам с учетом оценки рисков реализации угроз. Оценку рисков предполагается осуществлять на основе подходов, связанных с нечеткими множествами, для определения количественной оценки рисков, что определяет область дальнейших исследований.

*Рецензент: **Алексеев Владимир Витальевич,** доктор технических наук, профессор, член-корреспондент РАЕН, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: vvalex1961@mail.ru

Литература

1. Atlam H.F., Walters R.J., Wills G.B., Daniel J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT // Mobile Networks and Applications. 2021, Vol. 26, No. 2, pp. 1—13. DOI: 10.1007/s11036-019-01214-w .
2. Ma K., Yang G., Xiang Y. RCBAC: A risk-aware content-based access control model for large-scale text data // Journal of Network and Computer Applications. 2020, Vol. 167. DOI: 10.1016/j.jnca.2020.102733 .
3. Priscila S.S. et al. Risk-Based Access Control Mechanism for Internet of Vehicles Using Artificial Intelligence // Security and Communication Networks. 2022, Vol. 2022. DOI: 10.1155/2022/3379843 .
4. Atlam H.F., Wills G.B. An efficient security risk estimation technique for risk-based access control model for IoT // Internet Things. 2019, Vol. 6, Article ID 100052. DOI: 10.1016/j.iot.2019.100052 .
5. Fan X., Li C., Dong X. A real-time network security visualization system based on incremental learning. // J. Visualization 22 (1), 2019, pp. 215—229.
6. Chen A., Lu G., Xing H., Xie Y., Yuan S. Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments // International Journal of Distributed Sensor Networks. 2020, Vol. 16. Iss. 5. DOI: 10.1177/1550147720921778 .
7. Sepczuk M., Kotulski Z. A new risk-based authentication management model oriented on user's experience // Computers & Security. 2018, Vol. 73, pp. 17—33. DOI: 10.1016/j.cose.2017.10.002 .
8. Armando A., Bezzi M., Metoui N., Sabetta A. Risk-Based Privacy-Aware Information Disclosure. In: Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications. 2019, pp. 567—586. DOI: 10.4018/978-1-5225-7113-1.ch030 .
9. Магомедов Ш.Г., Колясников П.В., Никульчев Е.В. Разработка технологии контроля доступа к цифровым порталам и платформам на основе встроенных в интерфейс оценок времени реакций пользователей // Russian Technological Journal. 2020. Т. 8. № 6 (38). С. 34—46. DOI: 10.32362/2500-316X-2020-8-6-34-46 .
10. Магомедов Ш.Г. Архитектура вычислительного комплекса с многоуровневым контролем доступа к веб-сервисам по общедоступным сетям // International Journal of Open Information Technologies. 2021. Т. 9. № 3. С. 36—43.
11. Xu Y. et al. An efficient privacy-enhanced attribute-based access control mechanism // Concurrency and Computation: Practice and Experience. 2020, Vol. 32, No. 5, p. e5556.
12. Calvo M., Beltrán M. A model for risk-based adaptive security controls // Computers & Security. 2022, Vol. 115. DOI: 10.1016/j.cose.2022.102612 .
13. Petrović Dejan V., Miloš Tanasijević, Saša Stojadinović, Jelena Ivaz, Pavle Stojković. Fuzzy Model for Risk Assessment of Machinery Failures // Symmetry. 2020. Vol. 12, No. 4, p. 525. DOI: 10.3390/sym12040525 .

14. Козачок А.В. Спецификация модели управления доступом к разнокатегорийным ресурсам компьютерных систем // Вопросы кибербезопасности. 2018. № 4 (28). С. 2—8. DOI: 10.21681/2311-3456-2018-4-2-8 .
15. Козачок А.В., Козачок В.И., Кочетков Е.В. Многоуровневая модель политики безопасности управления доступом операционных систем семейства Windows // Вопросы кибербезопасности. 2021. № 1 (41). С. 41—56. DOI: 10.21681/2311-3456-2021-1-41-56 .

A RISK-ORIENTED ATTRIBUTIVE ACCESS CONTROL MODEL FOR HIGHER EDUCATION ORGANISATIONS

Shamil' Magomedov, *Ph.D. (Technology), Associate Professor, Head of the Department KB-4 "Intelligent Information Security Systems" of the Russian Technological University MIREA, Moscow, Russian Federation. ORCID: 0000-0001-8560-1937.*
E-mail: magomedov_sh@mirea.ru

Aleksandr Kozachok, *Dr.Sc. (Technology), Associate Professor, Professor at the Department KB-4 "Intelligent Information Security Systems" of the Russian Technological University MIREA, Moscow, Russian Federation. ORCID: 0000-0002-6501-2008.*
E-mail: kozachok_a@mirea.ru

Arslan Tarlanov, *Associate Professor at the Department KB-14 "Digital Technologies for Data Processing" of the Russian Technological University MIREA, Moscow, Russian Federation. ORCID: 0000-0002-7508-9682.*
E-mail: tarlanov@mirea.ru

Keywords: *risk-based security, dynamic models, risk-oriented access control model, IT services infrastructure in the field of education, attributes, access control models.*

Abstract

Purpose of the paper: working out a risk-oriented access control model changing access rules in accordance with the current level of information security threat risk based on the analysis of key processes in the IT structure and information security events.

Methods of study: analysis of access control models, theoretical formalisation, simulation.

Study findings: the approach demonstrated its viability compared with traditional access control models, and the study findings made it possible to put forward proposals for further development of this research area.

Research novelty: a risk-oriented attributive access control model using the higher education system services as an example is proposed, and an access control policy based on the XACML industry standard is worked out which can change access rules according to risk assessment in real time.

References

1. Atlam H.F., Walters R.J., Wills G.B., Daniel J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT. Mobile Networks and Applications. 2021, Vol. 26, No. 2, pp. 1–13. DOI: 10.1007/s11036-019-01214-w .
2. Ma K., Yang G., Xiang Y. RCBAC: A risk-aware content-based access control model for large-scale text data. Journal of Network and Computer Applications. 2020, Vol. 167. DOI: 10.1016/j.jnca.2020.102733 .
3. Priscila S.S. et al. Risk-Based Access Control Mechanism for Internet of Vehicles Using Artificial Intelligence. Security and Communication Networks. 2022, Vol. 2022. DOI: 10.1155/2022/3379843 .
4. Atlam H.F., Wills G.B. An efficient security risk estimation technique for risk-based access control model for IoT. Internet Things. 2019, Vol. 6, Article ID 100052. DOI: 10.1016/j.iot.2019.100052 .
5. Fan X., Li C., Dong X. A real-time network security visualization system based on incremental learning. J. Visualization 22 (1), 2019, pp. 215–229.
6. Chen A., Lu G., Xing H., Xie Y., Yuan S. Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments. International Journal of Distributed Sensor Networks. 2020, Vol. 16. Iss. 5. DOI: 10.1177/1550147720921778 .

7. Sepczuk M., Kotulski Z. A new risk-based authentication management model oriented on user's experience. Computers & Security. 2018, Vol. 73, pp. 17–33. DOI: 10.1016/j.cose.2017.10.002 .
8. Armando A., Bezzi M., Metoui N., Sabetta A. Risk-Based Privacy-Aware Information Disclosure. In: Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications. 2019, pp. 567–586. DOI: 10.4018/978-1-5225-7113-1.ch030 .
9. Magomedov Sh.G., Koliasnikov P.V., Nikul'chev E.V. Razrabotka tekhnologii kontrolia dostupa k tsifrovym portalam i platformam na osnove vstroennykh v interfeis otsenok vremeni reaktsii pol'zovatelei. Russian Technological Journal, 2020, t. 8, No. 6 (38), pp. 34–46. DOI: 10.32362/2500-316X-2020-8-6-34-46 .
10. Magomedov Sh.G. Arkhitektura vychislitel'nogo kompleksa s mnogourovnevym kontrolem dostupa k veb-servisam po obshchedostupnym setiam. International Journal of Open Information Technologies, 2021, t. 9, No. 3, pp. 36–43.
11. Xu Y. et al. An efficient privacy-enhanced attribute-based access control mechanism. Concurrency and Computation: Practice and Experience. 2020, Vol. 32, No. 5, p. e5556.
12. Calvo M., Beltrán M. A model for risk-based adaptive security controls. Computers & Security. 2022, Vol. 115. DOI: 10.1016/j.cose.2022.102612 .
13. Petrović Dejan V., Miloš Tanasijević, Saša Stojadinović, Jelena Ivaz, Pavle Stojković. Fuzzy Model for Risk Assessment of Machinery Failures. Symmetry. 2020. Vol. 12, No. 4, p. 525. DOI: 10.3390/sym12040525 .
14. Kozachok A.V. Cpetsifikatsiia modeli upravleniia dostupom k raznokategoriinym resursam komp'iuternykh sistem. Voprosy kiberbezopasnosti, 2018, No. 4 (28), pp. 2–8. DOI: 10.21681/2311-3456-2018-4-2-8 .
15. Kozachok A.V., Kozachok V.I., Kochetkov E.V. Mnogourovnevaia model' politiki bezopasnosti upravleniia dostupom operatsionnykh sistem semeistva Windows. Voprosy kiberbezopasnosti, 2021, No. 1 (41), pp. 41–56. DOI: 10.21681/2311-3456-2021-1-41-56 .

ПРАВОВЫЕ АСПЕКТЫ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ

Карцхия А. А.[1]

Ключевые слова: *кибератаки, киберпреступность, кибербезопасность, информационно-коммуникационные технологии (ИКТ), цифровые технологии, программное обеспечение, мошенничество, способ, информационно-телекоммуникационные сети (ИТС), Интернет, трансграничность, персональные данные, сфера компьютерной информации.*

Аннотация

Цель работы: определение актуальных правовых аспектов и особенностей киберпреступности в сфере информационно-коммуникационных технологий (ИКТ) с учетом российского и зарубежного опыта и правоприменительной практики.

Методы: сравнительно-правовой анализ действующего российского и зарубежного законодательства и практики их применения, а также формально-логический анализ понятийного аппарата, содержания и структуры предмета исследования.

Результаты: предлагается совокупность формализованных представлений о правонарушениях и преступлениях с использованием компьютерной техники, информационно-коммуникационного оборудования и средств, включая компьютерные программные средства, для понимания правового содержания понятия киберпреступности; исследованы новые способы совершения преступлений в киберпространстве и выявлены новые объекты киберпреступлений; определено, что киберинциденты занимают лидирующую позицию среди группы рисков, связанных с развитием современной цифровой экономики, растущей угрозой со стороны программ-вымогателей и кибермошенничества, а также геополитическим соперничеством и конфликтами, которые все чаще разыгрываются в киберпространстве; обоснован вывод о формировании особого вида преступности — в сфере кибербезопасности и ИКТ, что ставит задачу разработки технологического и правового обеспечения эффективного регулирования отношений в данной сфере.

DOI: 10.21681/1994-1404-2023-1-83-92

Введение

Наряду с экономическими и политическими последствиями пандемии COVID-19, высокими ценами на энергоносители и инфляцией, геополитической и экономической неопределенностью и изменением климата, согласно проведенному в 2022 г. аналитическому исследованию международной страховой группы *Allianz*[2], *киберинциденты занимают лидирующую позицию среди группы рисков, связанных с развитием современной цифровой экономики, растущей угрозой со стороны программ-вымогателей и кибермошенничества, а также геополитическим соперничеством и конфликтами, которые все чаще разыгрываются в киберпространстве* [3, 16]. Киберриски, такие как перебои в работе *IT*-систем, атаки программ-вымогателей или утечка данных, второй год подряд считаются наиболее важным риском во всем мире, что произошло впервые за последнее десятилетие.

Кибератаки являются одной из самых постоянных и серьезных угроз, с которыми сегодня сталкиваются многие компании. Глобальные кибератаки, спонсируемые государством, могут привести к серьезному нарушению рынков и экономики. *Киберустойчивость* становится важнейшим экономическим и политическим фактором как противовес опасностям, связанным с *киберпреступностью* [3] в виде трех взаимосвязанных угроз: уязвимости «нулевого дня», уязвимости сторонних поставщиков услуг, уязвимости программ-вымогателей.

[2] Allianz Risk Barometer 2023, 12th Edition. URL: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html#download

[1] ***Карцхия Александр Амиранович,*** *доктор юридических наук, и. о. заведующего кафедрой правового обеспечения безопасности топливно-энергетического комплекса Российского государственного университета нефти и газа (НИУ) им. И. М. Губкина, г. Москва, Российская Федерация.*

E-mail: arhz50@mail.ru

Устойчивость подразумевает способность быстро восстанавливаться после неудач, приспосабливаться. Более 2/3 глобальных финансовых компаний в 2022 г. подверглись хотя бы одной атаке программ-вымогателей. Критическая рыночная инфраструктура (биржи, расчетные центры и др.) уже сталкивается с инцидентами *кибербезопасности* [1, 3] и продолжением угроз программ вымогателей, которые уже не ограничиваются участием изощренных разработчиков программ-вымогателей и простым пользовательским интерфейсом злоумышленников, а нанимают соучастников для развертывания программы-вымогателя в целях кибератаки на жертву за вознаграждение (процент от полученного выкупа). Киберустойчивость приобретает особое значение: многие кибератаки начинаются с общих уязвимостей, которые можно устранить с помощью надлежащей кибергигиены. Попытки фишинга, атаки на программное обеспечение и системы, которые не были обновлены, доступ через удаленные соединения и попытки инсайдеров получить данные продолжают использоваться киберпреступниками[3].

По оценкам Интерпола, преступники пользуются онлайн-трансформацией для выявления слабых мест в онлайн-системах, сетях и инфраструктуре. Фишинг, программы-вымогатели и утечка данных — это лишь несколько примеров современных киберугроз, в то время как новые виды киберпреступлений появляются постоянно. Киберпреступники становятся все более гибкими и организованными: они используют новые технологии, адаптируют свои атаки и сотрудничают по-новому. *Киберпреступность* (преступность в сфере высоких технологий) не знает национальных границ. Преступники, жертвы и техническая инфраструктура охватывают несколько юрисдикций, что создает множество проблем для расследований и судебного преследования. Поэтому необходимо тесное сотрудничество между государственными и частными партнерами[4].

Согласно статистике Банка России, в первом полугодии 2020 г. мошенники украли у банковских клиентов примерно 4 *млрд руб.*, совершив 360 тыс. несанкционированных операций. Из этой суммы банки смогли вернуть клиентам только 12,1% похищенных средств (около 485 *млн руб.*)[5].

Почти четверть криптовалютных токенов, выпущенных в 2021 г., продемонстрировали явные признаки мошеннической схемы. По оценкам аналитиков *Chainalysis*, схемы накачки и сброса распространены в традиционных финансах. Мошенники обычно продвигают активы, которыми они владеют, другим инвесторам, быстро повышая цену. Когда она достигает определенной точки, они продают переоцененные акции с прибылью, в результате чего цена резко падает (*Pump-and-Dump*). Криптовалюты, торгуемые цифровые активы, построенные на блокчейне другой криптовалюты, становятся все более популярными среди тех же мошенников, что часто связано с относительной легкостью, с которой злоумышленники могут запустить новый токен и установить для него искусственно высокую цену и рыночную капитализацию «на бумаге», задав первоначальный объем торговли и контролируя оборотное предложение[6]. Мошеннические объявления о продаже криптовалюты могут размещаться в социальных сетях и на законных веб-сайтах СМИ или появляться в списках онлайн-поиска.

Как только пользователи делятся своими личными данными, с ними можно связаться по телефону, электронной почте или в сообщении в социальных сетях и предложить высокую прибыль с минимальным риском или без него. На этом этапе мошенники обычно используют тактику продаж с высоким давлением. Но, как только деньги будут внесены, мошенники заморозят счет и украдут средства. Они получат доступ, обманом заставив жертву загрузить *троянскую* программу удаленного доступа (*Remote Access Trojan — RAT*), что позволит им захватить компьютер пользователя[7]. Согласно сообщениям, в 2021 г. жертвы мошенничества с криптовалютой уже потеряли более 146 *млн* фунтов стерлингов (200 *млн* долларов США), что на двузначное число больше, чем в 2020 г.[8]

Недавние кибератаки доказали, что киберпреступность представляет собой реальную и непосредственную опасность для большинства компаний в сегодняшнюю цифровую эпоху. Даже традиционные компании, не зависящие от *IT*, в том числе, например, в горнодобывающей и обрабатывающей промышленности, все чаще подключают свои компьютерные системы к своим *IT*-сетям и тем самым подвергают данные и системы рискам, связанным с киберугрозами.

Преступность в киберпространстве, как отмечалось в докладе ООН [6], является одной из самых сложных проблем, с которыми международное сообщество сталкивается в последние годы в связи с развитием информационных и коммуникационных технологий (ИКТ).

Киберпреступность носит трансграничный характер, а Интернет все чаще становится сферой террористических и экстремистских деяний, вовлечения и вербовки молодежи в преступную деятельность, областью целенаправленных кибератак на государственные и коммерческие структуры в преступных целях, включая посягательства на критически важную инфраструктуру, а также дестабилизацию международной информационной безопасности. Современная действительность показывает, что методы киберпреступности

[3] См.: CFTC Commissioner Christy Goldsmith Romero identified cybercrime and climate risk as severe threats to financial markets and called for collaborative action to strengthen resiliency in both areas. URL: https://www.cftc.gov/PressRoom/SpeechesTestimony/oparomero

[4] URL: https://www.interpol.int/Crimes/Cybercrime

[5] URL: https://www.cbr.ru/press/event/?id=8238

[6] URL: https://www.chainalysis.com/

[7] URL: https://www.infosecurity-magazine.com/news/santander-warns-of-87-surge-uk/

[8] URL: https://www.infosecurity-magazine.com/news-features/us-government-open-source-security/

могут эффективно использоваться в *информационной борьбе (войне)* [2, 8].

Стремительное распространение киберпреступности, появление новых форм организованной преступности, использующей глобальную сеть Интернет, спланированные и хорошо организованные кибератаки на критическую инфраструктуру государств и частных компаний свидетельствуют о формировании особого направления преступности — *преступность в сфере кибербезопасности и информационных технологий*, которая выходит за рамки традиционного понимания преступности в сфере информационных технологий и средств связи [6, 17].

Виды и особенности киберправонарушений

Киберпреступления совершаются с использованием компьютеров и компьютерных сетей и могут быть нацелены на отдельных физических лиц, компании и бизнес-структуры, государственные органы и управленческие структуры, а также объекты критической инфраструктуры. *Киберпреступником*, как правило, является лицо (группа лиц), использующее свои навыки в области компьютерных технологий для совершения злонамеренных действий и незаконной деятельности в противоправных целях. Киберпреступниками могут быть лица, торгующие незаконным онлайн-контентом или нарушающие права *интеллектуальной собственности* [9], кибермошенники, наркоторговцы, кибертеррористы. Чаще всего киберпреступления совершаются по мотивам личной мести, корыстным мотивам (мошенничество, вымогательство, кража цифровых активов или данных и др.), а также таким как шантаж, кибертерроризм и угрозы или идеологическая мотивация. К наиболее распространенным способам совершения киберпреступлений можно отнести следующие[9].

I. *Кибермошенничество* (*Internet fraud)* или кража личных данных как форма мошенничества в отношении потребителей (*identity theft*) — незаконное присвоение или использование киберпреступниками *персональных* или иных данных другого человека (номера кредитных карт, личные фотографии, имя, аккаунта в соцсети и др.) без разрешения владельца этих данных в целях совершения мошенничества или иного преступления.

К этой категории, в частности, относится фишинг (*fishing & scams*) — разновидность онлайн-мошенничества, которое нацелено на завладение персональными и иными данными потребителей путем отправки им электронного письма якобы от хорошо известного и доверенного источника (например, от интернет-провайдера, банка или ипотечной компании), и которым просят потребителя предоставить личную идентификационную информацию. Затем мошенник использует эту информацию в противоправных целях — для открытия новых учетных записей или вторжения в существующие учетные записи потребителя. Разновидностями такого рода афер (*scams*) в целях получения персональных данных являются, например:

(а) мошенничество с автогарантией или медицинским страхованием — мошенническое предложение о продлении гарантии на автомобиль, страховой или медицинский полис для завладения персональными данными;

(б) мошенничество с благотворительностью — мошеннические звонки с просьбой о благотворительных пожертвованиях в адрес выдуманных фальшивых благотворительных организаций или имитация настоящей благотворительности для выманивания денежных средств;

(в) мошенничество с оказанием помощи при несчастных случаях или стихийных бедствиях, когда преступник запрашивает деньги или персональные данные для якобы попавшего в беду родственника или члена семьи;

(г) мошенничество с предложением о трудоустройстве по онлайн-объявлениям, часто с незаконным использованием официальных названий известных компаний;

(д) мошенничество с подарочными картами или сертификатами;

(е) мошенничество с государственными грантами, с предложением перевести на расчетный счет потребителя денежные средства, как только он предоставит информацию о своей учетной записи, которую впоследствии мошенники продают или используют для кражи денег;

(ж) мошенничество с самозванцем (звонка, робозвонка, электронной почты или другого сообщения) от имени налоговой социальной или иной государственной службы с требованием немедленной оплаты задолженности, часто с помощью неотслеживаемых способов;

(з) мошенничество с технической поддержкой или бесплатной пробной версией компьютерной программы путем ложного заявления о том, что устройство пользователя заражено вирусом, иной вредоносной программой с последующим требованием оплаты за «исправление» несуществующего дефекта или удаление подключения к внешнему устройству для кражи личной информации.

В США, например, у физических лиц нет официального удостоверения личности, но номер социального страхования долгое время служил де-факто идентификационным номером. Налоги взимаются на основе номера социального страхования каждого гражданина, и многие частные учреждения используют этот номер для отслеживания своих сотрудников, студентов и пациентов. Доступ к номеру социального страхования человека дает возможность собрать все документы, относящиеся к гражданству этого человека, т. е. «украсть» его личность. Даже украденная информация кредитной карты может быть использована для восстановления личности[10].

[9] URL: https://www.ftc.gov/news-events/topics/identity-theft

[10] M. Aaron Dennis. Alternate titles: computer crime: Article History. URL: https://www.britannica.com/topic/cybercrime

По данным Банка России[11], за первое полугодие 2020 г. доля социальной инженерии в общем числе атак на банковских клиентов составила 83,8%. По оценкам Сбербанка, с начала 2020 г. мошенники позвонили клиентам около 15 *млн* раз. В сутки число мошеннических звонков в России достигает 100 *тыс*.

II. *Создание и применение шпионских и вредоносных компьютерных программ*, включая вирусы и «шпионские» программы в целях кражи персональных данных и иных личных данных (в том числе биометрические данные [11] и сведения о геноме [5] конкретного человека, сведения личного аккаунта в соцсетях или личного банковского и иного счета), рассылки спама и совершения мошеннических действий. Используя привлекательные веб-сайты, желаемые загрузки и убедительные истории, преступники заманивают потребителей по ссылкам, по которым загружается вредоносное программное обеспечение (ПО), особенно на компьютерах, где не используются ПО безопасности. «Шпионское» ПО как вид вредоносного ПО способно отслеживать использование чужого компьютера или контролировать его, а также позволяет отправлять потребителям всплывающие окна, перенаправлять их компьютеры на нежелательные веб-сайты, отслеживать их интернет-серфинг или записи нажатий клавиш в целях кражи личных данных.

III. *Кражи персональных данных или иных данных военнослужащих* и членов их семей составляют особую категорию, направленную на подрыв боеспособности Вооруженных сил.

IV. *Навязанные платежи* *(mobile cramming)* — взимание несанкционированных платежей третьими лицами со счетов мобильных телефонов за сторонние услуги без ведома или согласия потребителей (например, предложение бесплатных призов, а затем взимания с телефонных счетов потребителей периодических платежей в пользу третьих лиц за услуги, не связанные с предложением).

V. *Кибератаки программ-вымогателей* *(ransomware attack)* — кибератаки с использованием программ-вымогателей, вредоносного ПО, которое способно препятствовать доступу пользователей к их личным данным (аккаунтам) в системе, шифруя эти данные, а затем запрашивая выкуп за открытие доступа к зашифрованным данным.

VI. *Взлом/блокировка доступа в компьютерных сетях* *(hacking/misusing computer networks)*, т. е. несанкционированный доступ к частным компьютерам или иным *IT-сетям* и последующем их неправомерном использовании либо путем их отключения, либо путем изменения хранимых данных, либо другими противоправными способами.

VII. *Киберзапугивание* *(cyber bullying)* — онлайн- или интернет-издевательства, включающие отправку или совместное использование вредоносного и унизительного контента о каком-либо лице, направленное на то, чтобы вызвать его смущение, что может быть причиной возникновения психологических проблем — это в последнее время стало распространенным явлением, особенно среди подростков.

VIII. *Киберпреследование* *(cyber stalking)* — использование лицом нежелательного и постоянно нацеленного на других людей онлайн-контента с целью контроля и/или запугивания (например, нежелательные и систематически продолжающиеся звонки и сообщения).

IX. *Киберпиратство,* пиратское программное обеспечение (*software piracy*), нарушения прав интеллектуальной собственности (*intellectual property infringements*) — незаконное использование или копирование платного ПО с нарушением авторских прав или лицензионных ограничений. Например, загрузка нелицензированной копии *Windows* и ее взлом; неправомерное использование в сети музыки, фильмов, фотографий и иных объектов авторских или смежных прав, патентных прав и прав на товарные знаки и др. [12].

X. *Мошенничество в социальных сетях* *(social media frauds)* — использование поддельных аккаунтов в социальных сетях для совершения любого рода неправомерных и вредоносных действий (выдача себя за других пользователей или отправка устрашающих сообщений, распространение спама по электронной почте).

XI. *Онлайн-торговля наркотиками* *(online drug trafficking)*. Существенный рост сбыта наркотиков в Интернете, особенно в «теневом Интернете» (*Darknet*) связан с развитием технологий криптовалют, облегчающих перевод денег и заключение сделок с наркотиками, не привлекая внимания правоохранительных органов.

XII. *Отмывание электронных денег* *(electronic money laundering)* — наиболее распространенный онлайн-бизнес, использующий противоправные способы оплаты и транзакции по кредитным картам или криптовалютам с предоставлением неполной или противоречивой платежной информации для приобретения запрещенных к обороту объектов или сокрытия источников финансирования, денежных средств.

XIII. *Кибервымогательство* (*cyber extortion*) — требование выкупа киберпреступниками за возврат неправомерно полученных ими важных документов или личных данных либо за прекращение совершения вредоносных действий (кибератаки типа «отказ в обслуживании»).

XIV. *Мошенничество с наймом на работу, подбором персонала онлайн* *(online recruitment fraud)* — получающее распространение киберпреступление, заключающееся в предложении онлайн поддельных трудовых вакансий, предоставляемых поддельными компаниями с целью получения финансовой выгоды от соискателей или даже использования их личных данных, по типу операции «программа-вымогатель как услуга»[12].

[11] URL: https://www.rbc.ru/society/12/12/2020/5fd446c49a7947746aba6e19

[12] L. Fair. Taking the "ploy" out of employment scams. January 25, 2023. URL: https://www.ftc.gov/business-guidance/blog/2023/01/taking-ploy-out-employment-scams

XV. *Мошенничество с банкоматами*, через которые многие люди получают наличные. Для доступа к учетной записи пользователь предъявляет карту и персональный идентификационный номер (ПИН — *PIN*). Преступники разработали средства для перехвата как данных на магнитной полосе карты, так и *PIN*-кода пользователя. В свою очередь, информация используется для создания поддельных карт, которые затем используются для снятия средств со счета ничего не подозревающего человека.

XVI. *Мошенническая романтическая афера (romance scam)*[13] — использование онлайн-приложений в соцсетях, мессенджерах или Интернете для романтического знакомства в мошеннических целях, где мошенники-любовники под различными предлогами выманивают деньги у лица за мнимое оказание услуги или для преодоления выдуманной сложной жизненной ситуации и др., либо личные фото и/или иную личную информацию для последующего шантажа.

XVII. *Мошеннические рекламные акции в Интернете*[14] **—** использование сомнительных заявлений для рекламы мошенниками столь же сомнительных продуктов: таблетки для похудения или лекарства от всех болезней, рекламные акции быстрого обогащения и др. Отличие таких рекламных акций в якобы одобрении рекламируемых продуктов знаменитостями или известными лицами в деловом мире. Например, Федеральная комиссия по торговле США в 2019 г. возбудила административное производство в защиту прав потребителей по факту ложной рекламы новостных сайтов «умных» таблеток *Geniux*, якобы повышающих деятельность мозга, с неправомерным использованием имен и фото Билла Гейтса и покойного профессора Стивена Хокинга[15] — обман, который стоил большого штрафа.

XVIII. *Нарушение сохранности данных несовершеннолетних* *в сети Интернет*[16]. *В* частности, в соответствии с Законом США о защите частной жизни детей в Интернете (Children's Online Privacy Protection Act of 1998, COPPA) операторы сайтов и онлайн-сервисов, ориентированных на детей (определение делается путем оценки предмета, визуального контента, использования анимированных персонажей или ориентированных на детей действий и стимулов, а также других факторов), которые собирают или хранят личную информацию детей младше 13 лет, обязаны среди прочего получить поддающееся проверке согласие родителей, прежде чем собирать, использовать или раскрывать личную информацию детей (включая полные имена, адреса электронной почты и имена пользователей). Нарушение этих требований закона владельцем популярной игры *Fortnite* (*Epic Games*) стало предметом расследования в 2019 г. Федеральной комиссией по торговле США, на которую возложен контроль за обеспечением защиты конфиденциальности детей в цифровом мире. Этот контроль распространяется не только на онлайн-игры, но и на защиту конфиденциальности детей в сфере онлайн-образования, оказание онлайн медицинских услуг и иных потребительских услуг. Следует заметить, что точная геолокация (данные о точном местоположении) детей при онлайн-играх, телереклама также подпадают под определение персональных данных, защищаемых *COPPA*[17].

XIX. *Кибертерроризм и экстремизм*. Интернет широко используется для пропаганды различных экстремистских идей и движений, кибермошенничества, информационных блокад, компьютерного шпионажа и иных противоправных действий [14, 15].

Особая сфера противоправных действий в сфере ИКТ — *кибервойна*, использование ложной, фейковой информации, обработка сознания человека и общества, целью которого может быть конкретное лицо (государственный или общественный деятель, популярный политик и др.), а также в целях получения глобального результата (массовые беспорядки или гражданское неповиновение, формирование негативного образа публичной власти и др.).

Однако следует заметить, что сфера кибервойны постоянно расширяется. Например, ряд исследований исходит из того, что культура как таковая определяется как коллективное программирование разума, которое отличает членов одной группы или категории людей от другой[18] [18], что оказывает огромное влияние на жизнь людей и в результате влияет на события, в которых участвуют представители разных культур. Распространение новостей представляет один из наиболее эффективных механизмов трансграничного распространения информации.

В связи с постоянно растущим числом событий, имеющих значительный международный резонанс, все бóльшее значение для профессионалов и исследователей во многих дисциплинах, включая цифровые гуманитарные науки, медиа-исследования и журналистику, приобретает *кросс-культурная аналитика*. Самые последние примеры таких событий включают COVID-19 и Brexit. Существует несколько детерминант, которые оказывают существенное влияние на процесс отбора,

---

[13] E. Fletcher. Romance scammers' favorite lies exposed. February 9, 2023. URL: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

[14] L. Fair. A warning to marketers about testi-phony-als, including ads falsely claiming a "Shark Tank" connection. February 17, 2023. URL: https://www.ftc.gov/business-guidance/blog/2023/02/warning-marketers-about-testi-phony-als-including-ads-falsely-claiming-shark-tank-connection

[15] URL: https://www.ftc.gov/business-guidance/blog/2019/04/bogus-celebrity-testimonials-and-phony-formats-donts-advertisers-and-affiliates

[16] L. Fair. Record-setting FTC settlements with Fortnite owner Epic Games are the latest "Battle Royale" against violations of kids' privacy and use of digital dark patterns. December 19, 2022. URL: https://www.ftc.gov/business-guidance/blog/2022/12/record-setting-ftc-settlements-fortnite-owner-epic-games-are-latest-battle-royale-against-violations

[17] L. Fair. Updating you on FTC privacy and data security initiatives. 25 May, 2021. URL: https://www.ftc.gov/business-guidance/blog/2021/05/updating-you-ftc-privacy-data-security-initiatives

[18] Abdul Sittar, Dunja Mladenic. Classification of Cross-cultural News Events. January 2023. URL: https://arxiv. org/abs/2301.05543

анализа и распространения информации. К ним относятся культурные ценности и различия, экономические условия и связи между странами. Например, если две страны более схожи в культурном отношении, больше шансов, что между ними будет более интенсивный поток новостей. Анализ новостных событий может применяться с использованием реестра событий, т. е. системы, которая анализирует новостные статьи, идентифицирует группы статей, описывающих одно и то же событие, и представляет их как единое событие.

Рассматривая позицию Международного валютного фонда, как отмечается в исследованиях [7], следует поддержать призыв международного сообщества к решению вопроса регулирования цифровых валют как стратегически важного этапа развития мировой экономики, поскольку цифровая валюта может использоваться для легализации денежных средств, полученных преступным путем и кибермошенничеством.

Российское законодательство и правоприменение в сфере противодействия киберпреступности

В настоящее время киберпреступность является одной из наиболее серьезных угроз национальной безопасности Российской Федерации в информационной сфере. Эксперты отмечают [3, 4, 13] особые характеристики киберпреступности: высокая латентность, специальная подготовка преступников, трансграничность, автоматизированность преступлений, нетрадиционность средств противодействия киберпреступности.

Российское законодательство и судебная практика определили группы преступлений, связанных с использованием современных компьютерных технологий, которые формируют особую группу преступлений — *преступления в сфере компьютерной информации* (по состоянию на июль 2022 г.): неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ИТС) (ст. 274); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1), а также нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации ИТС Интернет и сети связи общего пользования (ст. 274.2).

Важной вехой формирования *единой судебной практики* стало Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или ИТС, включая сеть Интернет» (далее — Постановление), принятое для обеспечения единообразного применения законодательства об уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные статьями 272, 273, 274 и 274.1 УК РФ, а также за иные преступления, совершенные с использованием электронных или ИТС.

Постановление разъяснило понятие «компьютерной информации» в ст. 272 УК РФ, которая включает любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Эти сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах (далее — компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе жестких дисках-накопителях, флеш-картах и др.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электросвязи. Кроме того, в качестве *охраняемой законом компьютерной информации* (п. 1 ст. 272 УК РФ) рассматривается как *информация*, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и *информация*, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности.

Постановление содержит ряд ключевых для применения гл. 28 УК РФ определений, включая следующие:

- *компьютерной программой* с учетом положений ст. 1261 ГК РФ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения;
- *уничтожением* компьютерной информации является приведение такой информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена;
- *блокированием* компьютерной информации является воздействие на саму информацию, средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме (искусственное затруднение или ограничение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением);

– *модификация* компьютерной информации представляет собой внесение в нее любых изменений, включая изменение ее свойств, например, целостности или достоверности;
– *копированием* компьютерной информации является перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме (в том числе отправка по электронной почте, распечатывание на принтере, фотографирование, переписывание от руки и др.);
– *нейтрализацией средств защиты* компьютерной информации является воздействие, в частности, на технические, криптографические и другие средства, предназначенные для защиты компьютерной информации от несанкционированного доступа к ней, а также воздействие на средства контроля эффективности защиты информации (технические средства и программы, предназначенные для проверки средств защиты компьютерной информации, например, осуществляющие мониторинг работы антивирусных программ) с целью утраты ими функций по защите компьютерной информации или контролю эффективности такой защиты.

В соответствии с п. 7 Постановления, к иной компьютерной информации (ст. 273 УК РФ), заведомо предназначенной для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, могут быть отнесены любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить достижение целей, перечисленных в ч. 1 ст. 273 УК РФ, например, *ключи доступа,* позволяющие нейтрализовать защиту компьютерной информации, элементы кодов компьютерных программ, способных скрытно уничтожать и копировать информацию.

Уголовную ответственность по ст. 273 УК РФ влекут действия по созданию, распространению или использованию только вредоносных компьютерных программ либо иной компьютерной информации, т. е. заведомо для лица, совершающего указанные действия, предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Создание вредоносных компьютерных программ или иной вредоносной компьютерной информации представляет собой деятельность, направленную на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютерной информации, предназначенных для *несанкционированного доступа*[19] [10], т. е. совершаемого без согласия обладателя информации, лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты (п. 9 Постановления).

Особая ответственность установлена за незаконное воздействие на критическую информационную инфраструктуру (ст. 274.1 УК РФ), что представляет собой нарушение установленных законом и подзаконными актами правил, если установлено, что компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, определение понятия которой содержится в ст. 2 Федерального закона от 26 июля 2017 г. № 187- ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В ином случае действия лица при наличии на то оснований могут быть квалифицированы по ст. 273 УК РФ.

В сфере противодействия киберпреступности особое значение имеют: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также международные акты по вопросам борьбы с преступлениями в сфере компьютерных технологий, в частности, Соглашение стран СНГ от 2001 г. о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации, которое рекомендовало странам-участницам признавать уголовно наказуемыми следующие деяния, если они совершены умышленно:

1) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

2) создание, использование или распространение вредоносных программ;

3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;

4) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского пра-

[19] Начиная с 70-х гг. прошлого века несанкционированный доступ к особо 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.

ва, а равно присвоение авторства, если это деяние причинило существенный ущерб[20].

Самостоятельным составом преступления является мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), определяемое как хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или ИТС. При этом Пленум Верховного Суда РФ от 30 ноября 2017 г. № 48[21] (в ред. от 29.06.2021) указал, что под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или ИТС признается *целенаправленное воздействие* программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) — ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим ПО, или на ИТС, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Вместе с тем, если хищение совершается путем использования учетных данных собственника или иного владельца имущества, то, независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и др.), оно подлежит квалификации как кража, если виновным не было оказано незаконного воздействия на ПО серверов, компьютеров или на сами ИТС. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, произошедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием. Если же хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в ИТС, включая сеть Интернет (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159, а не по ст. 159.6 УК РФ.

В соответствии с Кодексом об административных правонарушениях (КоАП) РФ установлена ответственность за административные правонарушения в области связи и информации (гл. 13 КоАП РФ), которые предусматривают административную ответственность, в том числе за нарушение правил защиты информации (ст. 13.12), нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (ст. 13.12.1), злоупотребление свободой массовой информации (ст. 13.15), нарушение порядка ограничения доступа к информации, информационным ресурсам, доступ к которым подлежит ограничению в соответствии с информационным законодательством Российской Федерации, и (или) порядка удаления указанной информации (ст. 13.41), нарушение требований законодательства к установке технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации ИТС Интернет и сети связи общего пользования либо технических средств контроля за соблюдением операторами связи, собственниками или иными владельцами технологических сетей связи требований законодательства, предусматривающих ограничение доступа к информации (ст. 13.42), и др.

Особое регулирование осуществляется в сфере оборота персональных данных: принят Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 14.07.2022) «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Заключение

Особенности современной киберпреступности проявляются в следующем:

- мотивы и цели совершения преступления — использование цифровых технологий и компьютерных устройств для достижения противоправных целей;
- место совершения преступления — определяется глобальным, трансграничным характером преступности в силу трансграничности Интернета, *IT* и цифровых технологий;
- способы (средство) совершения преступлений — использование технологически нейтральных *IT* и цифровых технологий для достижения самых различных противоправных целей от кражи или мошенничества до преступлений против государственного строя и военных преступлений;
- субъекты совершения преступлений — преступления могут совершаться как отдельными физическими лицами или группой лиц, так и специалистами (хакерами) или хакерскими организованными сообществами в Интернете, а в отдельных случаях — с использованием средств (технологий или объектов), принадлежащих другим лицам без их ведома и согласия.

[20] URL: http://www.cis.minsk.by/page.php?id=866

[21] См.: Пункт 20 Постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2018. № 2. Фев.

*Рецензент: Т**ерентьева Людмила Вячеславовна,** доктор юридических наук, доцент, доцент кафедры международного частного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА).*
E-mail: terentevamila@mail.ru

Литература

1. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5. С. 39—42.
2. Глазов Б.И., Ловцов Д.А. Информационная борьба как система отношений в информационной среде // Военная мысль. 1997. № 5. С. 36—41.
3. Государство и право в новой цифровой реальности : монография / Под общ. ред. И.А. Конюховой-Умновой, Д.А. Ловцова. М. : ИНИОН РАН, 2020. 259 с. ISBN 978-5-248-00959-6.
4. Далгалы Т.А. Киберкриминология: вызовы XXI века // Российская юстиция. 2020. № 10. С. 19—21.
5. Запольский С.В., Пестрикова А.А., Сморчкова Л.Н. Информационно-правовой режим получения, хранения и использования биологического материала человека // Правовая информатика. 2022. № 4. С. 4—14. DOI: 10.21681/1994-1404-2022-4-4-14 .
6. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1. С. 28—44.
7. Кузнецова А.Д., Калмакова Н.А. Становление законодательной базы Российской Федерации в сфере оборота криптовалюты: цифровизация рубля // Финансовое право. 2022. № 3. С. 21—24.
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., Галахова А.Е. Защита интеллектуальной собственности в сети Интернет // Информационное право. 2011. № 4 (27). С. 13—20.
10. Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 2. Информ. процессы и системы. 2006. № 9. С. 1—9.
11. Ловцов Д.А., Князев К.В. Защищённая биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100—103.
12. Мельников В.С. Защита авторских и смежных прав в сети Интернет: проблемы теории и правоприменительной практики // Российское правосудие. 2013. № 5 (85). С. 46—56.
13. Мордвинов К.В., Удавихина У.А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1 (11). С. 83—88.
14. Савенкова Д.Д. Правовое обеспечение информационной безопасности Российской Федерации и развитие института ответственности за правонарушения в информационной сфере // Динамика институтов информационной безопасности. Правовые проблемы : сб. науч. трудов / Отв. ред. Т.А. Полякова, В.Б. Наумов, Э.В. Талапина. М. : Канон Плюс, РООИ «Реабилитация», 2018. С. 118—124.
15. Смирных С.Е. Международная информационная безопасность как гарантия осуществления права народов на самоопределение // Международное право и международные организации. 2022. № 2. С. 20—30.
16. 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 .
17. Терентьева Л.В. Управление киберпространством в условиях противостояния России и стран североатлантического альянса // Правовая информатика. 2022. № 3. С. 51—60. DOI: 10.21681/1994-1404-2018-3-51-60 .
18. Rampersad G., Althiyabi T. Fake news: acceptance by demographics and culture on social media. Journal of Information Technology & Politics, 2020, 17.1, pp. 1–11.

LEGAL ASPECTS OF MODERN CYBERCRIME

***Aleksandr Kartskhiia,** Ph.D. (Law), Acting Head of the Department of Legal Support for Fuel and Energy Industry Security of Gubkin Russian State University of Oil and Gas, Moscow, Russian Federation.*
E-mail: arhz50@mail.ru

***Keywords:** cyberattacks, cybercrime, cyber security, information and communication technologies (ICT), digital technologies, software, fraud, information and telecommunication networks (ITN), Internet, crossborderness, personal data, sphere of computer information.*

Abstract

Purpose of the paper: identifying topical legal aspects and specific features of cybercrime in the sphere of information and communication technologies (ICT) considering Russian and foreign experience and law enforcement practice.

Methods used: comparative legal analysis of current Russian and foreign laws and the practice of applying them as well as formal logical analysis of the conceptual framework, content and structure of the subject under study.

Study findings: a system of formalised views on offences and crimes committed using computers, information and communication equipment and means including software is proposed, to the end of understanding the legal content of the concept of cybercrime. New ways to commit crimes in cyberspace are studied and new objects of cybercrime are identified. It is found that cyber incidents hold a leading position within the group of risks related to the development of modern digital economy, a growing threat from ransomware and cyber fraud as well as geopolitical rivalry and conflicts happening ever more often in cyberspace. A conclusion is justified that a new, special type of crime is emerging, that is, crime in the field of cyber security and ICT, which poses a problem of developing technological and legal support for efficient regulation of relations in this sphere.

References

1. Alpeev A.S. Terminologiia bezopasnosti: kiberbezopasnost', informatsionnaia bezopasnost'. Voprosy kiberbezopasnosti, 2014, No. 5, pp. 39–42.
2. Glazov B.I., Lovtsov D.A. Informatsionnaia bor'ba kak sistema otnoshenii v informatsionnoi srede. Voennaia mysl', 1997, No. 5, pp. 36–41.
3. Gosudarstvo i pravo v novoi tsifrovoi real'nosti : monografiia. Pod obshch. red. I.A. Koniukhovoi-Umnovoi, D.A. Lovtsova. M. : INION RAN, 2020. 259 pp. ISBN 978-5-248-00959-6.
4. Dalgaly T.A. Kiberkriminologiia: vyzovy XXI veka. Rossiiskaia iustitsiia, 2020, No. 10, pp. 19–21.
5. Zapol'skii S.V., Pestrikova A.A., Smorchkova L.N. Informatsionno-pravovoi rezhim polucheniia, khraneniia i ispol'zovaniia biologicheskogo materiala cheloveka. Pravovaia informatika, 2022, No. 4, pp. 4–14. DOI: 10.21681/1994-1404-2022-4-4-14 .
6. Kartskhiia A.A., Makarenko G.I. Pravovye aspekty sovremennoi kiberbezopasnosti i protivodeistviia kiberprestupnosti. Voprosy kiberbezopasnosti, 2023, No. 1, pp. 28–44.
7. Kuznetsova A.D., Kalmakova N.A. Stanovlenie zakonodatel'noi bazy Rossiiskoi Federatsii v sfere oborota kriptovaliuty: tsifrovizatsiia rublia. Finansovoe pravo, 2022, No. 3, pp. 21–24.
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., Galakhova A.E. Zashchita intellektual'noi sobstvennosti v seti Internet. Informatsionnoe pravo, 2011, No. 4 (27), pp. 13–20.
10. Lovtsov D.A., Ermakov I.V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. NTI, ser. 2. Inform. protsessy i sistemy, 2006, No. 9, pp. 1–9.
11. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2013, No. 1, pp. 100–103.
12. Mel'nikov V.S. Zashchita avtorskikh i smezhnykh prav v seti Internet: problemy teorii i pravoprimenitel'noi praktiki. Rossiiskoe pravosudie, 2013, No. 5 (85), pp. 46–56.
13. Mordvinov K.V., Udavikhina U.A. Kiberprestupnost' v Rossii: aktual'nye vyzovy i uspeshnye praktiki bor'by s kiberprestupnost'iu. Teoreticheskaia i prikladnaia iurisprudentsiia, 2022, No. 1 (11), pp. 83–88.
14. Savenkova D.D. Pravovoe obespechenie informatsionnoi bezopasnosti Rossiiskoi Federatsii i razvitie instituta otvetstvennosti za pravonarusheniia v informatsionnoi sfere. Dinamika institutov informatsionnoi bezopasnosti. Pravovye problemy : sb. nauch. trudov. Otv. red. T.A. Poliakova, V.B. Naumov, E.V. Talapina. M. : Kanon Plius, ROOI "Reabilitatsiia", 2018, pp. 118–124.
15. Smirnykh S.E. Mezhdunarodnaia informatsionnaia bezopasnost' kak garantiia osushchestvleniia prava narodov na samoopredelenie. Mezhdunarodnoe pravo i mezhdunarodnye organizatsii, 2022, No. 2, pp. 20–30.
16. 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 .
17. Terent'eva L.V. Upravlenie kiberprostranstvom v usloviiakh protivostoianiia Rossii i stran severoatlanticheskogo al'iansa. Pravovaia informatika, 2022, No. 3, pp. 51–60. DOI: 10.21681/1994-1404-2018-3-51-60 .
18. Rampersad G., Althiyabi T. Fake news: acceptance by demographics and culture on social media. Journal of Information Technology & Politics, 2020, 17.1, pp. 1–11.

ЦИКЛИЧНОСТЬ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Омельченко В.В.[1]

Ключевые слова*: аттестация, базовый цикл, государственное управление, качество, классификация, научная деятельность, научная специальность, регулирование, цикл, этап.*

Аннотация

Цель работы: повышение качества государственного управления на основе учета цикличности процессов управления национальными ресурсами на примере циклического управления научной деятельностью — организации научной аттестации.

Методы: комплексные методы систематизации и общей теории классификации объектов, процессов и явлений реальности.

Результаты: рассмотрены методологические вопросы государственного управления научной деятельностью и управления в целом, в том числе анализ существующего нормативно-правового обеспечения, свойства и основные подэтапы и этапы циклов управления; предложена универсальная модель базового цикла управления; введены новые определения цикличности государственного управления; обобщены итоги проведенных ранее исследований вопросов качества государственного управления научной аттестацией на примере анализа утвержденных на каждом этапном цикле научных специальностей, по которым присуждаются ученые степени; сделаны выводы.

DOI: 10.21681/1994-1404-2023-1-93-104

Введение

Настоящая статья посвящена рассмотрению методологических вопросов *цикличности* государственного управления. Предлагаемый в статье подход является продолжением работ по повышению качества и эффективности государственного управления национальными ресурсами. Так, предложенный в [13—20] подход к анализу и систематизации [12] задач и функций государственного управления национальными ресурсами был использован при рассмотрении:

1) частных задач и функциональных элементов государственного управления, в их числе: *прогнозирование* [13], *надзор* и *контроль* [14];

2) особенностей государственного управления в разных предметно-ориентированных сферах, в том числе при управлении:

- развитием малого и среднего предпринимательства в Российской Федерации [15];
- научной деятельностью в Российской Федерации на примере организации научной аттестации [16—20].

Полученные в [13—20] результаты оценки качества государственного управления по разным направлениям позволяют сделать *вывод* о необходимости и целесообразности использования свойств *цикличности* управления. Понимание и применение логики цикличности управления позволяет *системно* [4] проводить оценку её качества и эффективности.

Классификация основных свойств управления

В современной научной литературе *управление* рассматривается с самых разных его сторон, и, соответственно, в его понятие вкладывается разное содержание. Следствием этого являются самые разные определения (дефиниции) понятия *«управление»,* при этом за основу берутся те или иные свойства этого понятия. С целью различения (анализа) основных свойств понятия «управление» для его определения проведем их классификацию (рис. 1).

По основанию «направленность целеполагания» исходное множество свойств понятия управления подразделяется на следующие классы (см. рис. 1):

1) целенаправленный процесс изменения объекта управления или его состояния (№ 1);

[1] ***Омельченко Виктор Валентинович,*** *доктор технических наук, профессор, заслуженный деятель науки и техники Российской Федерации, государственный советник Российской Федерации 1 класса, советник секретариата научно-технического совета АО «ВПК «НПО машиностроения», г. Реутово, Московская область, Российская Федерация.*

E-mail: omvv@yandex.ru

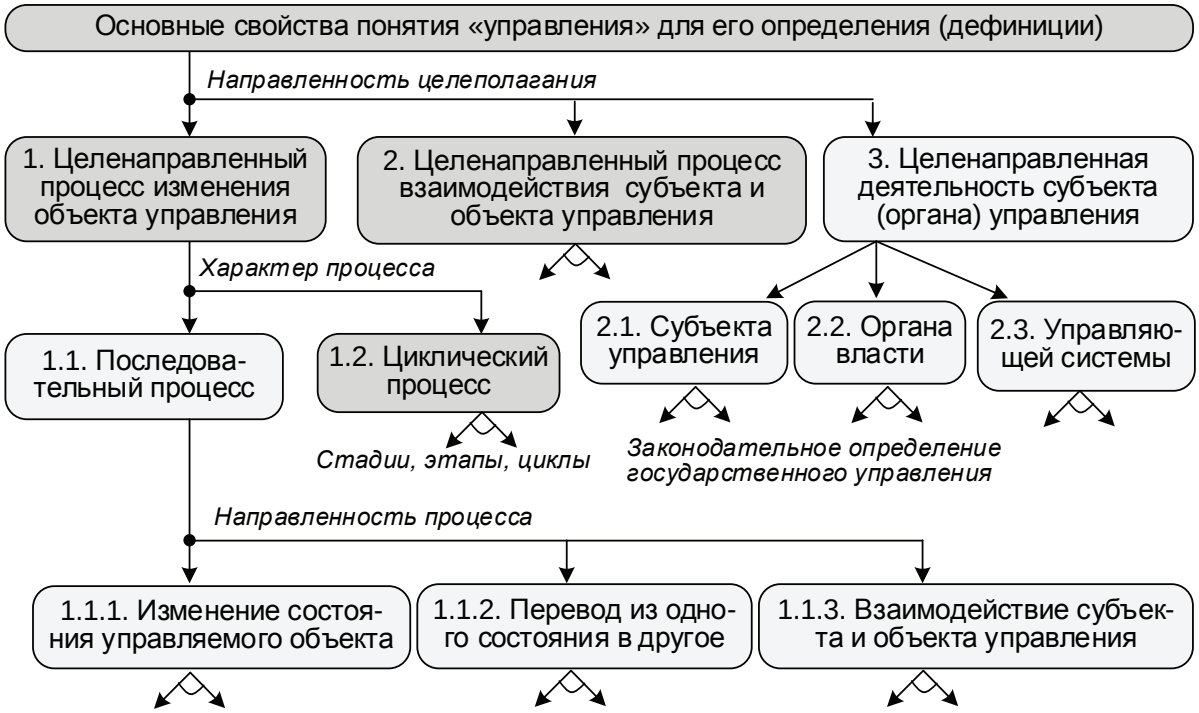

Рис. 1. Классификация основных свойств понятия «управление» для его определения

2) целенаправленный процесс взаимодействия субъекта (органа власти) и объекта управления (№ 2);

3) целенаправленная деятельность субъекта управления (№ 3).

Результат любого управления — это прежде всего целенаправленное изменение состояния объекта управления, поэтому первый класс свойств — это управление, ориентированное на результат, или *результативное управление*. Управление как целенаправленный процесс взаимодействия субъекта и объекта управления характерен для организационных систем управления, в которых объект управления является также субъектом[2] [9].

Для третьего класса, для которого управление — деятельность управляющего органа: результат не очевиден, по сути, он вторичен по отношению к деятельности.

Управление как *деятельность* традиционно рассматривается в государственной и юридической практике[3] [1—3, 7]. К этому же классу управления, не ориентированного на результат, относится и существующее нормативно-правовое определение понятия «государственное управление». Так, согласно Федеральному закону от 28 июня 2014 г. № 172-ФЗ, «*государственное управление*» — это ***деятельность органов государственной власти по реализации своих полномочий*** в сфере социально-экономического развития Российской Федерации и обеспечения национальной безопасности Российской Федерации. Такое определение государственного управления — по сути, не ориентированное на результат — создает определенные трудности при оценке его эффективности. Действительно, государственный орган власти как бы и выполняет свои полномочия, а вот оценить качество или эффективность такой деятельности весьма затруднительно.

Вместе с тем существуют и другие определения понятия управления. Так, в кибернетике принят другой подход к пониманию управления — как целенаправленного процесса изменения объекта управления или его состояния. Например, под управлением понимается любое изменение состояния рассматриваемого объекта, системы или процесса, ведущее к достижению поставленной цели [4, 7][4].

Этот класс свойств понятия управления по основанию «характер изменения» подразделяется на два подкласса:

- последовательный (поступательный, линейный) процесс (№ 1.1);
- циклический (повторяющийся, вращательный) процесс (№ 1.2).

Первый подкласс последовательных процессов по основанию «направленность процессов» подразделяется на подклассы:

[2] Козбаненко В.А. Государственное управление: основы теории и организации. В 2-х томах. Учебник. М. : «Статус», 2002. 366 с.

[3] Антонова Н.Б., Захарова Л.М., Вечер Л.С. Теория и методология государственного управления : курс лекций. Мн. : Акад. упр. при Президенте Респ. Беларусь, 2005. 231 с.; Атаманчук Г.В. Теория государственного управления : учебник. М. : Омега-Л, 2011. 525 с.; Охотский Е.В. Теория и современные механизмы государственного управления : учебно-метод. комплекс. М. : Юрайт, 2013. 701 с.; Правовое обеспечение государственного управления и исполнительная власть : учебник / Под ред. С.А. Старостина. 2023. М. : КонсультантПлюс. 21 с.; Радченко А.И. Основы государственного и муниципального управления: системный подход : учебник. М., Ростов н/Д : Март, 2007. 605 с.

[4] Словарь по кибернетике / Под ред. В.М. Глушкова. К. : Глав. ред. Укр. сов. энциклопедии, 1979. 624 с.

1) с изменением состояния управляемого объекта (№ 1.1.1);

2) с переводом из одного состояния управляемого объекта в другое (№ 1.1.2). Например, как перевод управляемой системы из одного состояния в другое, обусловленное закономерностями окружающей среды, посредством целенаправленного управляющего воздействия на эту систему[5] [5, 8].

3) с взаимодействием субъекта (органа) управления и управляемого объекта (№ 1.1.3).

Из всех представленных основных свойств понятия «управление» практически нераскрытым и неисследованным является класс свойств № 1.2, являющийся, на наш взгляд, наиболее важным и ключевым. Именно на этом направлении исследований мы в дальнейшем и сосредоточим свое внимание.

В современной научной литературе цикличность государственного управления либо вообще не рассматривается[6], либо освещается весьма ограниченно[7]. Например, в учебной литературе[8] упоминается о *«колебательной и цикличной природе управленческого воздействия»*, при этом контроль рассматривается как *«стадия управленческого цикла»*, однако на этом рассмотрение вопроса и заканчивается.

В научной литературе рассматриваются либо функции управления, либо стадии (этапы) управленческой деятельности, при этом состав и количество стадий или функций управленческой деятельности весьма различны и по количеству, и по содержанию. В первом случае в числе наиболее значимых функций управления выделяются следующие:

- организация, планирование, прогнозирование, мотивация, регулирование, контроль[9];
- сбор данных, формирование сообщения, передача данных по каналам связи, учет, контроль, анализ, прогнозирование, планирование, оперативное управление, организация и координация, доведение решений[10].

Во втором случае предлагаются следующие стадии управленческого процесса[11]:

1) анализ и оценка управленческой ситуации;

2) прогнозирование и моделирование необходимых (и возможных) действий по сохранению и преобразованию состояния управленческой ситуации (в субъекте и объектах государственного управления);

3) разработка предполагаемых правовых актов или организационных мероприятий;

4) обсуждение и принятие правовых актов и осуществление организационных мероприятий;

5) организация исполнения принятых решений (правовых и организационных);

6) контроль выполнения и оперативное информирование;

7) обобщение [10] проведенной управленческой деятельности, оценка новой (результирующей) управленческой ситуации.

Указанные стадии и функции управленческого процесса ориентированы, собственно, на деятельность органа или субъекта управления. А где сам объект управления? Где самые первые необходимые этапы (стадии) управления, такие как *измерение* состояния объекта управления, сбор и представление информации (*мониторинг*)? Ведь, как учил Д.И. Менделеев, любая наука, в том и числе наука управления, начинается там, где начинаются измерения.

Таким образом, можно сделать следующий вывод. В научной литературе нет общепризнанного однозначного понимания категорий «*государственное управление*» и «*управление*». В существующих разнообразных определениях рассматриваемых понятий не рассмотрено важное системное свойство — *цикличность* управления.

Цикличность управления

Изменение реальности и её важной составляющей — объектов управления является непрерывным и практически бесконечным процессом. Таких непрерывных и бесконечных процессов в реальности бесчисленное множество, что видно из приведенной на рис. 2 классификации циклического изменения объектов, процессов или явлений. Из этой же классификации видны роль и место циклов управления (на рисунке выделено цветом), которые представлены соответствующими классами управленческих циклов: базовые, этапные, государственные, муниципальные и др.

Рассматриваемое фундаментальное свойство непрерывного и бесконечного изменения объекта (процесса) управления с позиций теории управления является исключительно важным, так как оно требует определиться, в рамках какой системы реализуется процесс управления: открытой или закрытой.

Если процесс изменения состояния объекта управления непрерывный и бесконечный (открытая систе-

---

[5] Правовое обеспечение государственного управления и исполнительная власть : учебник / Под ред. С.А. Старостина. 2023. М. : КонсультантПлюс. 213 с.

[6] Антонова Н.Б., Захарова Л.М., Вечер Л.С. Теория и методология государственного управления : курс лекций. Мн. : Акад. упр. при Президенте Респ. Беларусь, 2005. 231 с.

[7] Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении : учеб. пособие / Под ред. А.А. Емельянова. М. : Финансы и статистика, 2002. 368 с.; Атаманчук Г.В. Теория государственного управления : учебник. М. : Омега-Л, 2011. 525 с.; Радченко А.И. Основы государственного и муниципального управления: системный подход : учебник. М., Ростов н/Д : Март, 2007. 605 с.

[8] Правовое обеспечение государственного управления и исполнительная власть : учебник / Под ред. С.А. Старостина. 2023. М. : КонсультантПлюс. 213 с. (с. 6).

[9] Козбаненко В.А. Государственное управление: основы теории и организации : учебник. В 2-х тт. М. : «Статус», 2002. 366 с.

[10] Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении : учеб. пособие / Под ред. А.А. Емельянова. М. : Финансы и статистика, 2002. 368 с. (с. 211).

[11] Там же.

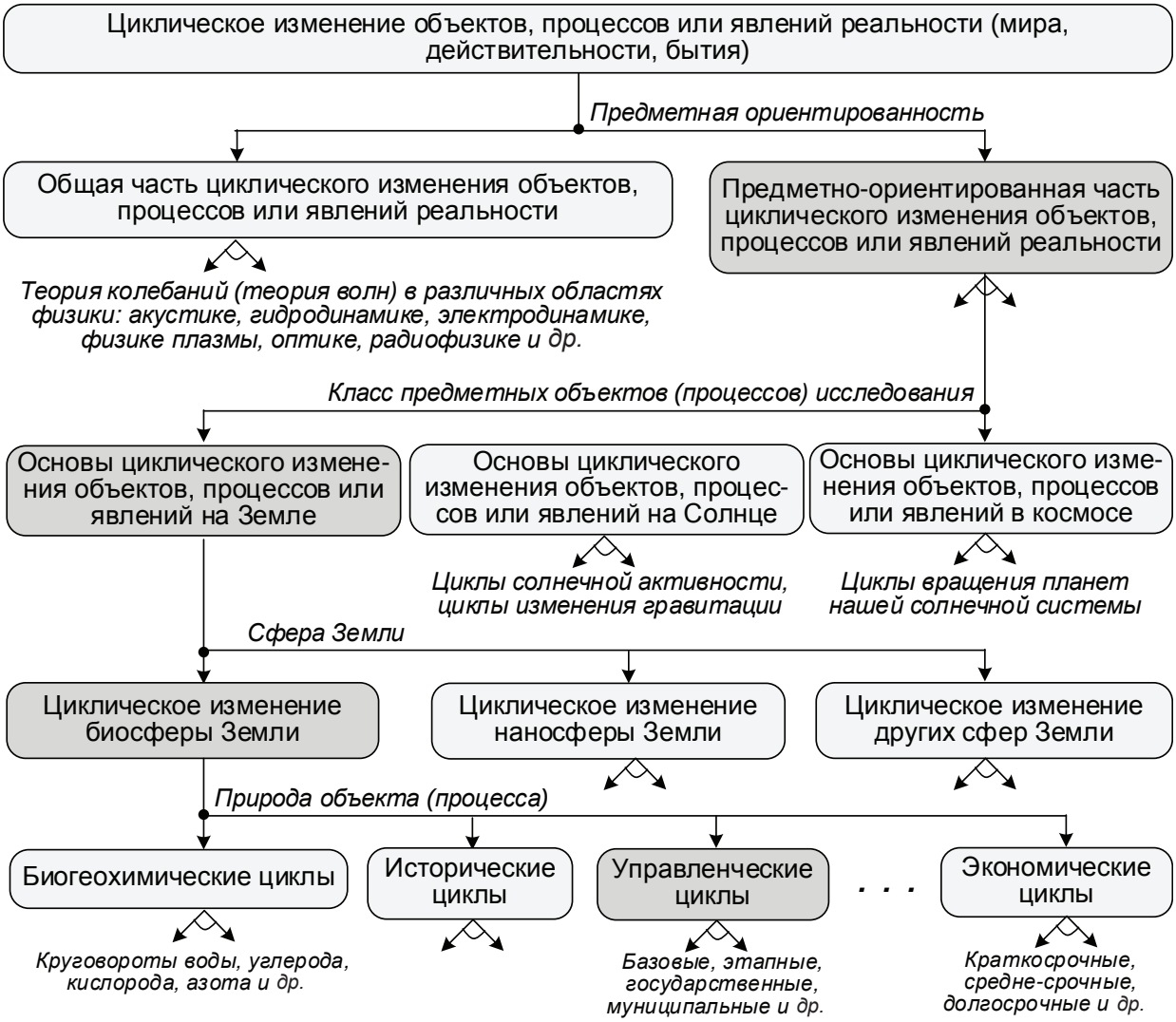

Рис. 2. Структурная схема классификации циклического изменения объектов, процессов или явлений реальности

ма), то возникает масса неразрешимых вопросов, в том числе:

- каковы цели и целеполагание для таких бесконечных процессов?
- как понимать и оценивать качество или эффективность таких процессов?

Системный подход [4] к решению проблем эффективного управления, также как и к познанию многообразной и разнообразной реальности в целом позволяет решать сложные задачи, только введя ограничения на бесконечность. Так, например, исходное (неструктурированное, неупорядоченное, необусловленное) бесконечное множество объектов, процессов и явлений реальности мы представляем структурированным и конечным множеством: классом (теория классификации) или системой (системный подход, системология, теория систем).

Применение системного подхода к непрерывному и бесконечному процессу управления реальностью также предполагает введение *системного ограничения*, в роли которого используется фундаментальное понятие *«цикл»*. Только тогда все вопросы целеполагания и эффективности управления приобретают конкретные смыслы, когда процесс управления рассматривается в границах конечного, фиксированного интервала времени или цикла управления. Продолжительность *цикла управления* реальностью в рассматриваемом контексте не имеет принципиального значения и связана главным образом с целями, планами, задачами управления, а также с состоянием объекта управления.

Такой подход позволяет для любого процесса управления в соответствии с поставленной целью определить циклы управления, имеющие замкнутый (циклический) характер. Каждый цикл управления реализуется с выполнением соответствующих управленческих функций и завершается достижением поставленной цели и выполнением соответствующих целевых задач. Получаемый при завершении цикла *результат* — это целенаправленно изменённое состояние объекта управления. При этом с появлением и постановкой новой цели (целей) управления начинается новый или очередной цикл управления. Такой подход представляется необходимым для сложных, непрерыв-

но изменяющихся, ответственных и дорогостоящих государственных объектов управления. Например, это такие сферы государственного управления, как освоение космоса, развитие науки и техники, развитие вооружения, социально-экономические программы и др.

Таким образом, использование понятия «цикличность» для управления реальностью позволяет организовать:

– переход от рассмотрения сложных *открытых* систем (объектов и процессов реальности) к познанию таких же сложных, но *закрытых* систем, что значительно упрощает решение проблемы управления;
– непрерывное циклическое управление для сложных, непрерывно изменяющихся, ответственных и дорогостоящих объектов управления.

Новые определения понятий «управление» и «государственное управление»

На основе результатов проведенного ИКС-анализа («информационно-кибернетически-синергетического») [6], соответствующего физической природе систем управления, обоснованы следующие определения основных понятий:

***Определение* 1.** *Управление* — это целенаправленный *циклический* процесс воздействия органа управления на объект управления.

Частным случаем понятия *управление* является государственное управление.

***Определение* 2.** *Государственное управление* — это целенаправленный *циклический* процесс воздействия государственного органа власти на объект управления.

Здесь ключевым является понятие «циклический». В общем случае, понятие *«цикл (период)»* любого изменения объекта, процесса или явления реальности отражает:

– *завершенность* или *законченность* циклического процесса через некоторый промежуток времени;
– *повторяемость* определенных циклических процессов управления изменением объекта управления;
– *системность* циклического процесса, предполагающая объединение в нечто единое, целое или систему его составных частей.

Совокупность функций управления, выполняемых в рассматриваемой системе управления, принято называть *циклом управления*. Выполняя цикл за циклом, система управления приближается к достижению сформулированной цели.

Цикличность управления предполагает наличие множества повторяющихся циклов управления, каждый из которых включает логическую последовательность разных подэтапов и/или этапов управления, повторяющихся в каждом цикле. Такое многообразие циклов можно представить в виде многоуровневой классификационной системы циклов, в которой выделено два класса циклов (рис. 3):

– *базовые* (первичные) циклы, включающие совокупность функций управления, но не содержащие в себе какие-либо другие циклы;

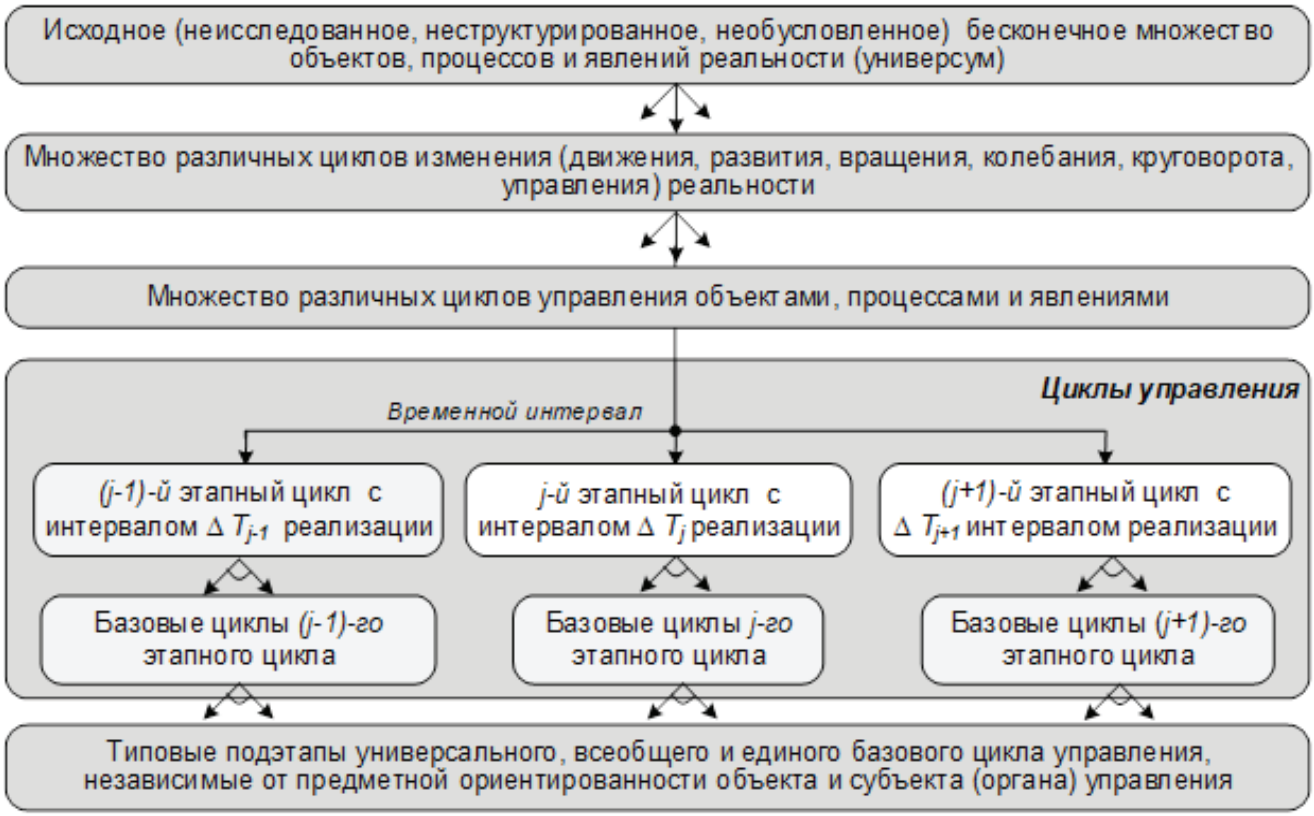

Рис. 3. Классификация циклов управления

– *этапные* (вторичные) циклы, которые содержат в себе другие циклы.

***Определение* 3.** *Базовый цикл управления* — это целенаправленный завершенный *циклический* процесс, который содержит последовательно реализуемые типовые подэтапы, независимые от предмета управления.

***Определение* 4.** *Типовой подэтап управления* — часть базового циклического процесса, на котором реализуется одна из функций управления.

Базовый цикл управления является первичной основой любого другого этапного цикла управления. Поэтому его место в многоуровневой системе управления всегда находится на нижних уровнях такой системы. Соответственно, место этапного цикла управления в многоуровневой системе управления — это верхние уровни такой системы.

***Определение* 5.** *Этапный цикл управления* — это целенаправленный завершенный *циклический* процесс, который содержит типовые базовые циклы управления, реализуемые на заданном временном интервале.

Типовые подэтапы базового цикла управления

В нормативно-правовой базе России отсутствует какая-либо *систематизация* [12] или *классификация* [11] типовых подэтапов и этапов государственного управления. Вместе с тем в полномочиях органов власти в неструктурированном виде представлены функции, последовательно реализуемые на типовых подэтапах государственного управления.

Для выделения типовых подэтапов, образующих единый и целостный базовый цикл, важна их природа и взаимные отношения между собой, что отражает соответствующую природу и отношения основных частных функций управления, реализуемых на этих подэтапах. Основные функции управляющего органа (субъекта управления), реализующие *обратную связь* на управляемый объект (объект управления), выполняемые последовательно в составе единого базового цикла, представляются следующим образом [13—20].

1. *Наблюдение* (мониторинг) за состоянием объекта управления — функция, реализуемая на 1-м типовом подэтапе базового цикла управления. Согласно теории управления, для реализации управления должно соблюдаться первое фундаментальное свойство управления — необходимое *условие наблюдаемости* объекта управления[12]. Для безусловного выполнения этого условия первый типовой подэтап управления включает следующие функции: измерение, сбор, представление данных о состоянии объекта управления.

2. *Оценивание* состояния объекта управления — функция, реализуемая на 2-м типовом подэтапе базового цикла управления. Осуществляется по полученным результатам наблюдения текущего состояния объекта управления. На этом типовом подэтапе оцениваются: степень достижения поставленных целей и решения задач управления; выполнение требований нормативных правовых документов; выполнение планов, проектов, программ; влияние выявленных недостатков, нарушений, противоречий, аномалий, рисков на качество управления, а также оценка причин их возникновения и влияния.

Например, результатами оценивания могут быть полученные оценки:

– *соответствует / не соответствует* текущее состояние объекта управления требованиям законодательства и других документов (технических заданий);
– *выполнено / не выполнено* — требования принятой системы целеполагания, государственных планов, проектов и программ и др.

3. *Классификация* текущего состояния объекта управления (или частные её проявления: распознавание, диагностика, идентификация) — функция, реализуемая на 3-м типовом подэтапе базового цикла управления. На этом подэтапе с использованием фундаментальных классификационных отношений *различия* и *тождества* проводится установка принадлежности оцененного текущего состояния объекта управления к тому или иному ранее установленному классу состояний. Реализация типового подэтапа осуществляется путем *различения* (распознавания, диагностики, идентификации, анализа, дедукции, декомпозиции и др.) текущего состояния и *отождествления* (обобщения, синтеза, индукции, композиции и др.) в соответствующий класс состояний объекта управления.

4. *Предвидение* (прогнозирование) будущего состояния объекта управления — функция, реализуемая на 4-м типовом подэтапе базового цикла управления. Период предвидения выбирается из условий целеполагания и планирования.

5. *Планирование* деятельности по достижению целей — функция, реализуемая на 5-м типовом подэтапе базового цикла управления. С учетом текущего состояния объекта управления и результатов предвидения формируется или корректируется соответствующий план с обязательным отражением предпринимаемых мер, установлением сроков и ответственных за конечные результаты управления.

6. *Регулирование* (выдача управляющих воздействий) объекта управления — функция, реализуемая на 6-м типовом подэтапе базового цикла управления. Согласно теории управления, для реализации управления должно соблюдаться второе необходимое и достаточное *условие управляемости* объекта управления[13]. Осуществляется путем реализации мер, поручений и решений по управлению, в том числе по устранению выявленных недостатков, нарушений, аномалий, рисков.

[12] Воронов А.А. Устойчивость, управляемость, наблюдаемость. М. : Наука. Гл. ред. ФМЛ. 1979. 336 с.; Словарь по кибернетике / Под ред. В.М. Глушкова. К. : Глав. ред. Укр. сов. энциклопедии, 1979. 624 с.

[13] Там же.

Рис. 4. Полный базовый цикл государственного управления

Последним в базовом цикле 6-м подэтапом, по сути, завершается рассматриваемый процесс управления, реализуемый для достижения поставленной конкретной цели (целей). Если цели управления на этом цикле не достигнуты или возникают новые цели и задачи, то начинается следующий базовый цикл управления с реализацией всех его типовых подэтапов. При этом повторение циклического процесса должно осуществляться для решения новых задач и достижения целей, что обеспечивает целевое изменение состояния управляемого объекта по некоторой спирали изменения, вектор изменения которой может быть как *восходящего* (развития, возрождения, подъема и др.), так и *нисходящего* (деградации, вырождения, падения) характера.

Системная организация успешного завершения каждого цикла управления обеспечивается путем *координации* последовательности и согласованности выполнения всех типовых подэтапов базового цикла. Такая координация является системообразующей функцией управления. Для государственного управления эта функция реализуется в соответствии с принятой государственной политикой.

Состав рассмотренных выше функций, реализуемых последовательно на типовых подэтапах базового цикла управления, является единообразным и универсальным по содержанию и различным по форме проявления. При этом разнообразие форм проявления определяется предметной ориентированностью и соответствующей спецификой объектов (процессов) управления.

Анализ нормативной правовой базы полномочий органов государственной власти, включая все ветви власти, показывает [13—20]:

наличие практически всех рассмотренных выше функций, реализуемых последовательно на типовых подэтапах базового цикла управления;

отсутствие какой-либо систематизации (классификации, упорядоченности, структуризации) функций, реализуемых на типовых подэтапах базового цикла управления.

Таким образом, можно сделать следующие *выводы*:

1) каждый типовой подэтап базового цикла управления осуществляется последовательно с использованием полученных результатов предыдущих типовых подэтапов. С окончанием последнего в цикле 6-го подэтапа завершается базовый цикл управления и с соответствующим целеполаганием начинается новый;

2) в научной литературе отсутствует какая-либо классификация или систематизация цикличности управления объектами, процессами или явлениями реальности. Аналогичная ситуация характерна и для государственного управления.

Полный базовый цикл управления как универсальная модель управления

С учетом проведенного выше анализа типовых этапов базового цикла государственного управления и структуры известного инвариантного контура рационального управления (регулирования) [4, 5], представим универсальную и целостную структуру типового

Рис. 5. Нормативно-правовое обеспечение государственного управления научной деятельностью в России

базового цикла государственного управления и управления в целом (рис. 4).

Необходимые прямые и обратные связи, показанные на рис. 4, определяются особенностями реализации отдельных подэтапов цикла государственного управления. Внешние связи — как надсистемное (концептуальное) управление двух видов:

- цели государственного управления, реализуемые вышестоящей системой (надсистемой);
- угрозы, риски, ограничения (обстоятельства непреодолимой силы).

Под *надсистемой* понимаем систему верхнего уровня, которая формирует государственные цели и политику для системы государственного управления.

Угрозы (внешние и внутренние), появление которых требует коррекции принятого для рассматриваемой системы государственного управления целеполагания: например, возникновение новой внешней угрозы для государства требует изменения (коррекции) целеполагания и политики системы государственного управления.

Целеполагание и государственная политика являются системообразующими функциями по отношению ко всем частным функциям и задачам, реализуемым на каждом подэтапе базового цикла управления.

То есть представленный базовый цикл государственного управления, как и управления в целом, является полным (целостным, завершенным), универсальным (по всем видам управления от человека до государства) и независимым от природы или предметно-ориентированной сферы применения.

Подход к оценке качества циклического государственного управления

Традиционно совершенствование систем с управлением сводится к сокращению длительности цикла управления и повышению качества управляющих воздействий (решений)[14] [8]. Эти *требования*, с одной стороны, носят противоречивый характер, с другой стороны — характеризуют внутреннюю (внутрисистемную) оценку качества управления.

Можно применить другой подход, связанный с внешней (надсистемной) оценкой качества управления, известный как *внешний контроль* (аудит). Такой подход рассмотрим на примере государственного управления научной деятельностью в части регулирования системы научной аттестации. Основные документы, в которых отражены вопросы государственного управления научной и научно-технической деятельностью в Российской Федерации, представлены на рис. 5.

Объектом государственного управления является состояние научной и научно-технической деятельности в Российской Федерации. Органом государственного управления является Минобрнауки России и Высшая аттестационная комиссия.

Существующее государственное управление научной деятельностью (научной аттестации) согласно Федеральному закону № 127-ФЗ представляет собой

[14] Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении : учеб. пособие / Под ред. А.А. Емельянова. М. : Финансы и статистика, 2002. 368 с. (с. 14).

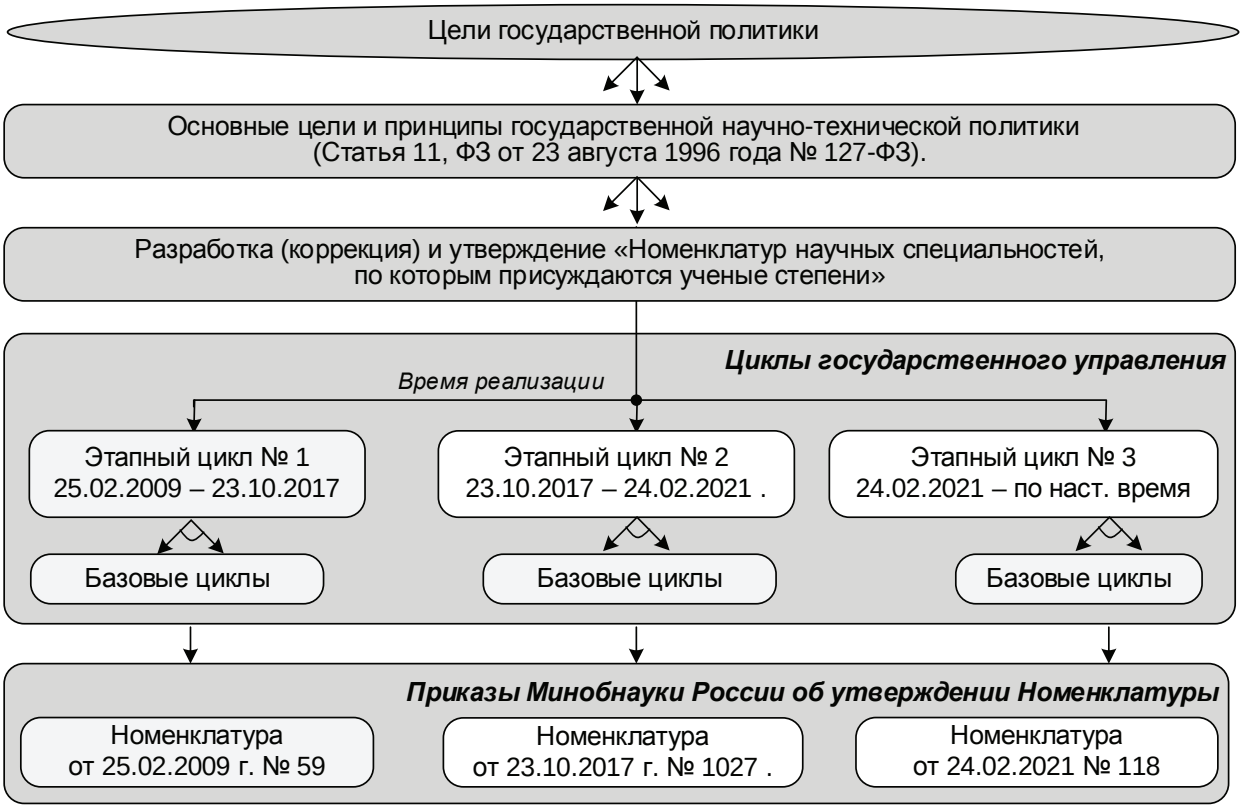

Рис. 6. Основные циклы государственного управления научной деятельностью в части регулирования системы научной аттестации

многоэтапный циклический процесс подготовки, разработки, согласования и утверждения приказом Минобрнауки России «Номенклатуры научных специальностей, по которым присуждаются ученые степени» (далее — Номенклатура). Оценка качества или эффективности этого процесса должна проводиться по полученным результатам, коим является сама Номенклатура и ее содержание, соответствующее реальному положению дел.

Логика рассмотрения вопроса оценки полученного результата (Номенклатуры) государственного управления научной деятельностью в части регулирования системы научной аттестации сводится к следующему.

1. Учет цикличности государственного управления при оценивании его результатов осуществляется (рис. 6):

– по каждой текущей реализации базового цикла государственного управления (текущая оценка с выявлением недостатков, ошибок, противоречий, угроз);
– по каждому этапному циклу государственного управления, включающего совокупность базовых циклов управления (обобщенная этапная оценка с выявлением недостатков, ошибок, противоречий, угроз). На рис. 6 показаны три этапных цикла: 1-й цикл: 25.02.09 — 23.10.17; 2-й цикл: 23.10.17 — 24.02.21; 3-й цикл: 24.02.21 — по настоящее время;
– по совокупности этапных циклов государственного управления (стратегическая оценка с выявление трендов, закономерностей).

2. Утвержденная и принятая к исполнению Номенклатура — это результат реализации этапного цикла государственного управления системой научной аттестации. На трех последних этапных циклах осуществлена подготовка, утверждение и принятие к исполнению Номенклатур от 25.02.09, 23.10.17 и 24.02.21.

3. Качество разрабатываемой, корректируемой и утверждаемой Номенклатуры напрямую зависит от эффективности государственного управления на каждом цикле и на всех предыдущих циклах.

4. Проведенный анализ качества утвержденных и принятых к исполнению Номенклатур на трех последних этапных циклах государственного управления (с 2009 г. по настоящее время) позволил вскрыть ряд её *системных недостатков* и даже противоречий, которые рассмотрены в [13—20]. Так, анализ государственного управления (регулирования) научной деятельностью (качеством государственной системы научной аттестации) на примере рассмотрения базового и трех этапных циклов разработки и внедрения «Номенклатур научных специальностей, по которым присуждаются ученые степени» показывает [20], что:

– выявленные системные недостатки утвержденных и принятых к исполнению Номенклатур значительно ухудшают их качество;
– неправильное определение места и роли научной специальности «Системный анализ», а также других универсальных и общесистемных наук и специальностей в утвержденных Номенклатурах значительно снижает достоверность её клас-

сификационной системы, что ведет к ухудшению качества государственной системы научной аттестации в целом.

В соответствии с этим государственное управление (регулирование) научной деятельностью по ряду показателей (*достоверность, полнота, целостность, наблюдаемость* и др.) на рассматриваемых этапных циклах можно оценить как неэффективное [20].

Таким образом, в связи с изложенным можно сделать следующие прагматические *выводы*.

1. Государственное управление, как и управление в целом, осуществляется циклически, где каждый типовой подэтап в базовом цикле управления реализуется последовательно с использованием полученных результатов предыдущих этапов этого цикла. Представленный базовый цикл управления, включающий совокупность типовых подэтапов управления, является:

– *независимым* (инвариантным) от природно-ориентированных сфер деятельности человека, общества и государства;
– *универсальным*, так как является всеобщим для любого вида управления в любой сфере деятельности человека, общества, государства;
– *целостным (полным, завершенным, единым)*, так как реализацией только всех последовательно выполняемых типовых этапов в конечном плане завершается единый базовый цикл управления;
– *динамическим* (изменяющимся) в результате воздействия на него как внутренних, так и внешних воздействий, что требует, как в кибернетической системе (с обратной связью), непрерывного и циклического воздействия управляющего органа на объект управления.

2. Невыполнение или некачественное выполнение задач любого типового подэтапа базового цикла управления приводит к невыполнению фундаментальных условий *наблюдаемости* и *управляемости*, что неизбежно снижает качество и эффективность как государственного управления, так и управления в целом.

3. Предложенный подход к определению понятия «*управление*» как целенаправленного циклического процесса позволяет с системных позиций подойти к рассмотрению вопросов качества и эффективности управления объектами и процессами реальности (мира, действительности, бытия).

Рецензент: ***Бетанов Владимир Вадимович,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, член-корреспондент РАРАН, начальник центра АО «Российские космические системы», г. Москва, Российская Федерация.*
E-mail: vlavab@mail.ru

Литература

1. Бондарева В.О., Новикова И.В. Понятие государственного управления // Наука. Образование. Инновации : сб. трудов. 2020. С. 27—30.
2. Журавлев А.В. Теория управления развитием вооружения. Часть I. Основы общей теории развития вооружения. М. : ВА им. Петра Великого, 2002. 223 с.
3. Ершов В.В. Правовое и индивидуальное регулирование общественных отношений : монография. М. : РГУП, 2018. 628 с. ISBN: 978-5-93916-631-7.
4. Ловцов Д.А. Системный анализ. Часть. 1. Теоретические основы. М. : РГУП, 2018. 224 с. ISBN 978-5-93916-701-7.
5. Ловцов Д.А. Информационная теория эргасистем: Тезаурус. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
6. Ловцов Д.А. Современная концепция комплексного «ИКС»-подхода к анализу и оптимизации правовых эргасистем // Правосудие/Justice. 2020. Т. 2. № 1. С. 59—81. DOI: 10.37399/issn2686-9241.2020.1.59-81 .
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 : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
9. Новиков Д.А. Теория управления организационными системами. М. : МПСИ, 2005. 584 с.
10. Омельченко В.В. Структурно-логический метод обобщения и анализа данных и знаний // Изв. РАН. Теория и системы управления. № 5. 1998. С. 96—105.
11. Омельченко В.В. Общая теория классификации. В 2 ч. Часть I. Основы системологии познания действительности // Предисл. Д.А. Ловцова. М. : ИПЦ «Маска», 2008. 466 с. ISBN 978-5-91146-297-0; Часть II. Теоретико-множественные основания. М. : Либроком, 2010. 296 с. ISBN 978-5-397-01327-7.
12. Омельченко В.В. Основы систематизации. В 2 ч. М. : Кн. дом «Либроком», 2012. 480 с. ISBN 978-5-397-02383-2.
13. Омельченко В.В. Прогнозирование как важнейшая функция управления: Историко-логический анализ древних писаний и древнерусского языка // Вестник РУДН. Сер. Гос. и муницип. управление. 2014. № 2. С. 85—102.
14. Омельченко В.В. Систематизация и анализ истоков происхождения ключевых понятий государственного управления «надзор» и «контроль» // Вестник РУДН. Сер. Гос. и муницип. управление. 2016. № 1. С. 7—19.

15. Омельченко В.В. Подход к оценке эффективности государственного управления национальными ресурсами на примере развития малого и среднего предпринимательства Российской Федерации // Вестник РУДН. Сер. Гос. и муницип. управление. 2017. Т. 4. № 1. С. 7—24.
16. Омельченко В.В. Государственное управление научной и научно-технической деятельностью в Российской Федерации на примере подготовки и принятия системы специальностей // Вестник РУДН. Сер. Гос. и муницип. управление. 2018. Т. 5. № 4. С. 397—410.
17. Омельченко В.В. Информационное обеспечение государственного регулирования подготовки и принятия системы научных специальностей // Правовая информатика. 2019. № 2. С. 4—14. DOI: 10.21681/1994-1404-2019-2-4-14 .
18. Омельченко В.В. Сравнительный анализ Российской и международной систем классификации научных направлений (специальностей) // Правовая информатика. 2020. № 1. С. 55—63. DOI: 10.21681/1994-1404-2020-1-55-6320 .
19. Омельченко В.В. Качество систематизации научных специальностей в Российской номенклатуре 2021 года // Правовая информатика. 2021. № 3. С. 4—14. DOI: 10.21681/1994-1404-2019-3-04-14 .
20. Омельченко В.В. Качество государственного управления научной деятельностью на примере организации научной аттестации // Тр. XXII Нац. науч. конф. с межд. уч-м «Модернизация России: приоритеты, проблемы, решения» (14—16 февраля 2023 г.) / ИНИОН РАН. М. : ИНИОН, 2023.

PUBLIC ADMINISTRATION CYCLICITY

Viktor Omel'chenko, *Dr.Sc. (Technology), Professor, Honoured Figure of Science and Technology of the Russian Federation, State Councillor of the 1st Class of the Russian Federation, Advisor to the Secretariat of the Board for Science and Technology of the AO (JSC) "VPK "NPO Mashinostroeniia", Reutovo, Moscow Oblast, Russian Federation.*
E-mail: omvv@yandex.ru

Keywords: *academic audit, basic cycle, public administration, quality, classification, research activity, research specialty, regulation, cycle, stage.*

Abstract

Purpose of the paper: raising the quality of public administration based on allowing for the cyclicity of the processes of management of national resources using the example of cyclic administration of research activities, that is, the organisation of academic audit.

Methods used: multi-faceted methods of systematisation and of the general theory of classification of objects, processes and phenomena of reality.

Study findings: methodological questions of public administration of research activities and management at large are considered, including an analysis of the current legal regulatory support, properties and the main substages and stages of management cycles. A universal model of the basic management cycle is put forward. New definitions for public administration cyclicity are introduced. A generalisation of the overall results of previous studies concerning questions of quality of public administration of academic audit is carried out using the example of analysis of research specialties in which academic degrees are awarded, approved at each stage cycle, and appropriate conclusions are made.

References

1. Bondareva V.O., Novikova I.V. Poniatie gosudarstvennogo upravleniia. Nauka. Obrazovanie. Innovatsii : sb. trudov. 2020, pp. 27–30.
2. Zhuravlev A.V. Teoriia upravleniia razvitiem vooruzheniia. Chast' I. Osnovy obshchei teorii razvitiia vooruzheniia. M. : VA im. Petra Velikogo, 2002. 223 pp.
3. Ershov V.V. Pravovoe i individual'noe regulirovanie obshchestvennykh otnoshenii : monografiia. M. : RGUP, 2018. 628 pp. ISBN: 978-5-93916-631-7.
4. Lovtsov D.A. Sistemnyi analiz. Chast'. 1. Teoreticheskie osnovy. M. : RGUP, 2018. 224 pp. ISBN 978-5-93916-701-7.
5. Lovtsov D.A. Informatsionnaia teoriia ergasistem: Tezaurus. M. : Nauka, 2005. 248 c. ISBN 5-02-033779-X.
6. Lovtsov D.A. Sovremennaia kontseptsiia kompleksnogo "IKS"-podkhoda k analizu i optimizatsii pravovykh ergasistem. Pravosudie/Justice, 2020, t. 2, No. 1, pp. 59–81. DOI: 10.37399/issn2686-9241.2020.1.59-81 .

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. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
9. Novikov D.A. Teoriia upravleniia organizatsionnymi sistemami. M. : MPSI, 2005. 584 pp.
10. Omel'chenko V.V. Strukturno-logicheskii metod obobshcheniia i analiza dannykh i znanii. Izv. RAN. Teoriia i sistemy upravleniia, No. 5, 1998, pp. 96–105.
11. Omel'chenko V.V. Obshchaia teoriia klassifikatsii. V 2 ch. Chast' I. Osnovy sistemologii poznaniia deistvitel'nosti. Predisl. D.A. Lovtsova. M. : IPTs "Maska", 2008. 466 pp. ISBN 978-5-91146-297-0; Chast' II. Teoretiko-mnozhestvennye osnovaniia. M. : Librokom, 2010. 296 pp. ISBN 978-5-397-01327-7.
12. Omel'chenko V.V. Osnovy sistematizatsii. V 2 ch. M. : Kn. dom "Librokom", 2012. 480 pp. ISBN 978-5-397-02383-2.
13. Omel'chenko V.V. Prognozirovanie kak vazhneishaia funktsiia upravleniia: Istoriko-logicheskii analiz drevnikh pisanii i drevnerusskogo iazyka. Vestnik RUDN, ser. Gos. i munitsip. upravlenie, 2014, No. 2, pp. 85–102.
14. Omel'chenko V.V. Sistematizatsiia i analiz istokov proiskhozhdeniia kliuchevykh poniatii gosudarstvennogo upravleniia "nadzor" i "kontrol'". Vestnik RUDN, ser. Gos. i munitsip. upravlenie, 2016, No. 1, pp. 7–19.
15. Omel'chenko V.V. Podkhod k otsenke effektivnosti gosudarstvennogo upravleniia natsional'nymi resursami na primere razvitiia malogo i srednego predprinimatel'stva Rossiiskoi Federatsii. Vestnik RUDN, ser. Gos. i munitsip. upravlenie, 2017, t. 4, No. 1, pp. 7–24.
16. Omel'chenko V.V. Gosudarstvennoe upravlenie nauchnoi i nauchno-tekhnicheskoi deiatel'nost'iu v Rossiiskoi Federatsii na primere podgotovki i priniatiia sistemy spetsial'nostei. Vestnik RUDN, ser. Gos. i munitsip. upravlenie, 2018, t. 5, No. 4, pp. 397–410.
17. Omel'chenko V.V. Informatsionnoe obespechenie gosudarstvennogo regulirovaniia podgotovki i priniatiia sistemy nauchnykh spetsial'nostei. Pravovaia informatika, 2019, No. 2, pp. 4–14. DOI: 10.21681/1994-1404-2019-2-4-14 .
18. Omel'chenko V.V. Sravnitel'nyi analiz Rossiiskoi i mezhdunarodnoi sistem klassifikatsii nauchnykh napravlenii (spetsial'nostei). Pravovaia informatika, 2020, No. 1, pp. 55–63. DOI: 10.21681/1994-1404-2020-1-55-6320 .
19. Omel'chenko V.V. Kachestvo sistematizatsii nauchnykh spetsial'nostei v Rossiiskoi nomenklature 2021 goda. Pravovaia informatika, 2021, No. 3, pp. 4–14. DOI: 10.21681/1994-1404-2019-3-04-14 .
20. Omel'chenko V.V. Kachestvo gosudarstvennogo upravleniia nauchnoi deiatel'nost'iu na primere organizatsii nauchnoi attestatsii. Tr. XXII Nats. nauch. konf. s mezhd. uch-m "Modernizatsiia Rossii: prioritety, problemy, resheniia" (14–16 fevralia 2023 g.). INION RAN. M. : INION, 2023.