Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт права, социального управления и безопасности
Кафедра информационной безопасности в управлении

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Сборник статей
III Всероссийской научно-практической конференции
с международным участием
27 марта 2026 г.

Ижевск
2026

ISBN 978-5-4312-1367-0
DOI 10.35634/978-5-4312-1367-0-2026-1-110

УДК 34.03:004.056.5(063)
ББК 67.401.114я431
О-136

Рекомендовано к изданию Редакционно-издательским советом УдГУ

Рецензенты: д-р юрид. наук, профессор, и. о. зав. сектором информационного права и международной информационной безопасности ИГП РАН, главный научный сотрудник, Заслуженный юрист Российской Федерации **Т. А. Полякова**;
канд. юрид. наук, доцент, зав. каф. экологического, трудового, административного права, основ права и российской государственности ФГБОУ ВО «УдГУ» **Е. А. Белокрылова**.

Научный редактор: Г. Г. Камалова, д-р юрид. наук, доцент, зав. каф. информационной безопасности в управлении ФГБОУ ВО «Удмуртский государственный университет».

О-136 Обеспечение информационной безопасности: вопросы теории и практики : сб. ст. III Всерос. науч.-практ. конф. с международным участием / науч. ред. Г. Г. Камалова. – Ижевск : Удмуртский университет, 2026. – 1 DVD-R (2,9 Мб). – Текст : электронный.

В издание вошли статьи участников III Всероссийской научно-практической конференции, проведённой 27 марта 2026 г. Институтом права, социального управления и безопасности Удмуртского государственного университета. В статьях рассматриваются актуальные вопросы теории и практики обеспечения информационной безопасности различной научной и отраслевой направленности. Сборник представляет интерес для ученых, специалистов, аспирантов, магистрантов и иных лиц, заинтересованных в решении актуальных проблем организационно-правового и технологического обеспечения информационной безопасности в условиях формирования многополярного мира, развития экономики данных и цифровой трансформации государства.

Минимальные системные требования:
Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше, 8x DVD-ROM
разрешение экрана 1024×768 или выше; программа для просмотра pdf.

ISBN 978-5-4312-1367-0
DOI 10.35634/978-5-4312-1367-0-2026-1-110

Обеспечение информационной безопасности: вопросы теории и практики
Сборник статей III Всероссийской научно-практической конференции
с международным участием, 27 марта 2026 г.

Подписано к использованию 12.08.2026
Объем электронного издания 2,9 Мб, тираж 10 экз.
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел.: +7(3412)263-751 E-mail: editorial@udsu.ru

Г. Г. Камалова,
д-р юрид. наук, доцент, зав. кафедрой информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Современные векторы развития обеспечения информационной безопасности прорывных цифровых технологий

Современный этап цифровой трансформации государства характеризуется беспрецедентной интеграцией цифровых технологий в процессы публичного управления, бизнеса и повседневную жизнь граждан, включая технологии искусственного интеллекта, больших данных и распределённого реестра, квантов. Эти цифровые инновации и построенные на их базе программные и аппаратно-программные решения и продукты, обеспечивая рост эффективности деятельности в экономической сфере и публичном управлении, масштабируемость успешных решений, одновременно формируют принципиально новые вызовы и риски, информационные угрозы, в том числе киберугрозы нового поколения, требуя адекватного реагирования со стороны профессионального сообщества. В связи с этим ранее выработанные правовые механизмы обеспечения информационной безопасности оказываются недостаточными в условиях динамичных технологических изменений современного мира, и возникает необходимость в определенном переосмыслении существующих правовых подходов.

Динамика цифровых технологий как ключевой фактор развития современных общества и государства констатируется множеством ученых[1]. Вместе с тем общепризнанно, что цифровизация имеет разнонаправленные проявления, в том числи риски и угрозы в связи с ростом проблем в области обеспечения информационной безопасности личности, общества и государства. Указанное сегодня наиболее актуально в отношении такого направления информационной безопасности, как кибербезопасность, что определяется трендами развития цифровых технологий и цифровой трансформацией широкого спектра общественных отношений. При этом проблемные вопросы, связанные с информационной безопасностью, весьма разнообразны и требуют глубоких научных исследований, охватывающих широкий спектр наук и научных направлений, включая права, в отношении дальнейших перспектив совершенствования организационных, технических и правовых средств защиты информации в цифровой форме[2]. При этом следует отметить, что в условиях максимального расширения поля функционирования цифровых технологий, которые оказывают влияние фактически на все сферы жизни общества и государства, особое значение приобретают вопросы кибербезопасности и доверия при использовании цифровых устройств.

Использование технологии искусственного интеллекта, внедрение алгоритмов машинного обучения, хранения критически важных данных на облачных платформах, распределённый характер современных цифровых сервисов в совокупности создают сложный и многоуровневый характер регулируемых общественных отношений, правовые коллизии и снижают уровень доверия в обществе к ходу и результатам цифровизации. При этом, безусловно, особую озабоченность вызывают правовые проблемы, порождаемые цифровой трансформацией государственного управления, а также состояние защищенности критической информационной инфраструктуры (далее – КИИ) и персональных данных граждан.

Нарастающее несоответствие между динамикой технологического развития и современным состоянием правового регулирования отношений в связи с цифровыми технологиями проявляется в устойчивом росте киберугроз. Статистика последних нескольких лет, начиная с 2022 года, показывает тревожную тенденцию. Государственные информационные системы, объекты критической информационной инфраструктуры всё чаще становятся мишенью для сложных целевых кибератак, зачастую носящих многоуровневый характер. Особые проблемы представляют недостаточная правовая защищённость КИИ, чьи компоненты интегрированы в цифровые экосистемы различных уровней; защита промышленных систем интернета вещей; интеллектуальных транспортных, медицинских и иных комплексов, содержащих особо чувствительную для граждан информацию.

---

[1] См., напр.: Механизмы и модели регулирования цифровых технологий / А. В. Минбалеев, А. В. Мартынов, Г. Г. Камалова, С. Г. Чубукова, О. В. Сушкова, М. В. Бундин, В. М. Жернова, И. С. Бойченко, К. Ю. Никольская. М., 2023; и др.

[2] Камалова Г. Г. Перспективы развития регулирования сферы обеспечения информационной безопасности в условиях формирования экономики данных и цифровой трансформации государства // Обеспечение информационной безопасности: вопросы теории и практики : сб. ст. Всерос. науч.-практ. конф. с междунар. участием. Ижевск, 2025. С. 6–15.

Однако положения действующих нормативных правовых актов зачастую не учитывают современную специфику защиты цифровых данных в условиях непрерывного технологического прогресса, а также существующих тенденций в области практики информационной безопасности[3]. Это свидетельствует о необходимости постоянного совершенствования законодательства в области информационно-коммуникационных технологий и информационной безопасности, а также внедрения опережающего регулирования на основе формирования адаптивных регуляторных моделей.

Указ Президента РФ «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»[4] в качестве национальных целей развития нашего государства определяет формирование безопасной среды для жизни, технологическое лидерство, цифровую трансформацию системы публичного управления, экономики и социальной сферы[5]. Очевидно, что безопасная среда включает и безопасность в цифровом пространстве на основе высокого уровня технологического суверенитета России в сфере цифровых технологий. Кроме того, активное развитие национальных программ цифровизации, включая национальный проект «Экономика данных и цифровая трансформация государства»[6], также требует совершенствования правовых механизмов обеспечения информационной безопасности. В связи с этим представляется закономерным, что национальный проект «Экономика данных и цифровая трансформация государства» в состав подлежащих реализации федеральных проектов включает разнообразные проекты в связи с информационно-коммуникационными технологиями, в том числе направленные на совершенствование инфраструктуры доступа к информации через информационно-телекоммуникационную сеть «Интернет» и формирование социальных цифровых платформ, развитие отечественных решений на основе технологии искусственного интеллекта, дальнейшую цифровизацию государственного управления и подготовку кадров для цифровой трансформации.

Необходимость своевременного правового сопровождения цифровой трансформации государства дополнительно обусловлена экономическими и социальными рисками технологического отставания и требованиями обеспечения технологического суверенитета в цифровой сфере[7]. Международный опыт показывает, что государства, обеспечивающие гармоничное развитие технологий и их регулирования, показывают большую устойчивость национальной информационной инфраструктуры к актуальным киберугрозам и более высокую защищенность национальных информационных ресурсов. В этом контексте научное исследование проблем правового обеспечения информационной безопасности в условиях цифровой трансформации государства приобретает стратегическое значение для национальной безопасности и технологического суверенитета. В связи с этим настоящее исследование направлено на поиск баланса между необходимостью защиты национальных интересов в цифровой сфере, поддержанием темпов научно-технологического развития в области цифровых технологий и правовым обеспечением прав и свобод человека и гражданина в информационной сфере.

Как известно, формирование законодательной базы РФ в области информационной безопасности началось в 1990-х годах в условиях становления новой российской государственности и первоначально фокусировалось на защите государственной тайны и базовых аспектах информационного обмена. Этот период развития информационного законодательства характеризовался фрагментарным подходом к регулированию цифровых отношений, отсутствием системного видения угроз киберпространства и недостаточной развитостью информационно-правовых институтов. Законодательные инициативы того времени заложили лишь минимальные основы для последующего развития отраслевого регулирования. В связи с этим можно утверждать, что информационное законодательство России прошло с девяностых годов двадцатого века по настоящее время достаточно большой путь формирования и становления в качестве комплексной правовой отрасли в составе публичного права и в настоящее время включает в себя правовое обеспечение информационной безопасности как одну из наиболее разработанных подотраслей.

---

[3] Камалова Г. Г. Перспективы развития регулирования сферы обеспечения информационной безопасности в условиях формирования экономики данных и цифровой трансформации государства… С. 6–15.

[4] О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента РФ от 07.05.2024 № 309 [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru, 07.05.2024 (дата обращения: 06.01.2026).

[5] Камалова Г. Г. Национальный технологический суверенитет в сфере цифровых технологий: вопросы правового обеспечения // Вестник Университета имени О. Е. Кутафина (МГЮА). 2024. № 10 (122). С. 52–60.

[6] Национальный проект «Экономика данных и цифровая трансформация государства» [Электронный ресурс] // Официальный сайт Правительства России. URL: http://government.ru/rugovclassifier/923/about/ (дата обращения: 06.01.2026).

[7] Полякова Т. А., Камалова Г. Г. Правовое обеспечение технологической политики развития экономики данных и трансформации государственного управления: вызовы и перспективы // Правовое государство: теория и практика. 2025. № 4 (82). С. 59–65; Камалова Г. Г. Национальный технологический суверенитет в сфере цифровых технологий: вопросы правового обеспечения // Вестник Университета имени О. Е. Кутафина (МГЮА). 2024. № 10 (122). С. 52–60.

Современный этап развития информационного законодательства связан с принятием специализированных нормативных актов, учитывающих технологические вызовы цифровой эпохи. При этом содержательные ограничения ранних нормативных актов продолжают проявляться в условиях цифровой трансформации государства и формирования экономики данных. Так, ранее не учитывались особенности облачных технологий, интернета вещей и больших данных, технологий искусственного интеллекта и иных цифровых инноваций, что создаёт в настоящее время определенные правовые лакуны. Не в полной мере были разработаны правовые режимы цифровых данных и цифровых сервисов. При этом отсутствие достаточных механизмов регулирования трансграничной передачи цифровых данных и противодействия киберугрозам снижает эффективность правоприменения, в том числе в транспортной, медицинской и иных профессиональных сферах[8]. Сохраняется недостаточная разработанность категориально-понятийного аппарата в информационном законодательстве, на что справедливо обращается внимание в большинстве научных исследований в информационно-правовой сфере. Особенно следует отметить научное исследование представителя екатеринбургской научной школы информационного права М. И. Паршукова[9].

Эти и иные проблемы для своего решения требуют системной модернизации законодательства для соответствия современным технологическим реалиям. При этом цифровая трансформация обусловила необходимость совершенствования российского законодательства в нескольких ключевых направлениях:

– формирование правовых механизмов противодействия новым видам киберугроз, включая целенаправленные атаки на критическую информационную инфраструктуру;

– регулирование обработки больших данных, требующее уточнения правовых режимов таких данных и информационно-аналитических систем, а также разграничения больших данных с персональными данными, представленными в цифровой форме;

– защита устройств интернета вещей (IoT), чьи уязвимости создают риски для информационной безопасности личности, общества и государства;

– определение правовых основ разработки, создания, внедрения и обеспечения безопасности систем искусственного интеллекта;

– правовое регулирование цифровых платформ и цифровых сервисов;

– и иные.

Так, обработка больших данных и внедрение технологий искусственного интеллекта стимулировали разработку норм об обезличивании информации и ограничении её вторичного использования. Вместе с тем в контексте расширения использования больших данных остаются и иные проблемы, формирующие основные векторы развития законодательства в контексте правового регулирования цифровых технологий.

Следует также отметить, что дальнейшее совершенствование правового обеспечения вопросов информационной безопасности порой не учитывает специфику практики деятельности по защите информации, углубления теории и методологии в данной области, динамику общественных отношений. По аналитическим исследованиям специалистов трендами в области информационной безопасности в настоящее время являются:

– переход от модели обеспечения безопасности функционирующей информационной инфраструктуры и цифровых сервисов посредством дополнительного внедрения разнообразных средств защиты информации к модели безопасности на всех этапах жизненного цикла продукта и сервиса, в том числе обеспечения безопасной разработки;

– перенос приоритета с защиты системы на защиту управленческих и бизнес-процессов путем формирования приоритетов на основе определения критичности цифровых данных и информационных систем для обеспечения устойчивости;

– развитие инструментария обеспечения кибербезопасности, включая развитие системы киберполигонов и SOC-центров;

– активизация использования функциональных технологий искусственного интеллекта, а также квантовых технологий;

– расширение требований к компетенциям специалистов информационной безопасности в условиях сохранения дефицита кадров;

[8] Быстрякова С. А. Формирование государственной политики в системе транспортной безопасности: публично-правовые вопросы цифрового оборота персональных данных // Правовая политика и правовая жизнь. 2024. № 3. С. 347–351.

[9] Паршуков М. И. Теоретические основании формирования понятийного аппарата информационного права в Российской Федерации. Екатеринбург : Университетская типография «Альфа Принт», 2025.

– усиление национального технологического суверенитета;

– расширение применения средств идентификации и аутентификации, верификации, а также развитие вопросов обеспечения доверия в цифровой среде;

– и другие[10].

В этой связи в настоящее время важное значение для совершенствования правового регулирования цифровой среды приобретают идеи «регуляторной гибкости», позволяющие адаптировать правовые и технические нормы под быстроразвивающиеся технологии, что направлено на поиск баланса между стимулированием инноваций в цифровой сфере и обеспечением информационной безопасности.

Исследование показало, что оценка действенности законодательства в области информационной безопасности сегодня должна осуществляться через призму его способности обеспечить противостояние современным киберугрозам, а также, как было отмечено выше, соответствия современным практикам защиты информации. В связи с этим, полагаем, ключевыми критериями должны выступать своевременность реагирования права на происходящие технологические изменения, полнота охвата правовых рисков информационной сферы и практическая реализуемость информационно-правовых норм. Поэтому исследователи отмечают дальнейшее усиление значимости развития правового прогнозирования, а также механизмов обеспечения адаптивности и прогностичности правового регулирования, позволяющих своевременно реагировать на динамику цифровизации бизнеса и государственного управления, демонстрируя высокие показатели роста и внедрения цифровых инноваций[11]. Эти идеи приобретают ключевое значение в условиях динамичной цифровой трансформации, требующей постоянной актуализации существующих правовых механизмов.

Результаты анализа текущего состояния правового регулирования информационной сферы показывают определенные тенденции его развития, обусловленные стоящими на современном этапе задачами обеспечения национальной безопасности в информационной сфере. Так, в последнее время наблюдается последовательное усиление ответственности за правонарушения в области информационной безопасности, сопровождающееся расширением перечня составов правонарушений и уточнением санкций за уголовные преступления и административные правонарушения в информационной сфере.

Вместе с тем современное информационное законодательство Российской Федерации по-прежнему не содержит необходимых специализированных норм, регулирующих общественные отношения в связи с целым рядом цифровых технологий, в том числе, например, в отношении обработки цифровых данных в распределённых облачных средах. Всё это создаёт правовые пробелы в определении требований к защите информации при использовании инфраструктуры третьих сторон, что широко распространено в связи тенденциями перехода организаций на сервисную модель обеспечения информационной безопасности, при которой многие процессы передаются на аутсорсинг. Однако отсутствие чётких критериев безопасности, установленных в нормативных правовых актах или документах по техническому регулированию, нередко осложняет построение системы защиты информации в организации и последующее проведение аудита безопасности, включая безопасности цифровых данных, обеспечиваемых облачными провайдерами и владельцами цифровых сервисов. В связи с этим можно делать вывод, что сохраняющаяся правовая неопределённость в отношении критериев защищенности определенных видов цифровых данных, обрабатываемых с использованием технологий, относящихся к сквозным, приводит к рискам несанкционированного доступа и утечек конфиденциальной информации.

При этом многие облачные сервисы используют географически распределённые дата-центры, что, безусловно, противоречит требованиям локализации персональных данных по российскому законодательству. Кроме того, трансграничный характер облачных технологий порождает коллизии юрисдикций при обработке цифровых данных, требуя проведения сложного комплаенса. Различия в национальных законодательствах затрудняют определение применимого права при возникновении споров, правонарушений и в случае инцидентов информационной безопасности. Например, требования GDPR[12] в ЕС и Федерального закона № 152-ФЗ[13] в России по-разному трактуют условия правомерной обработки персональных данных.

---

[10] Тенденции в ИБ на 2025 год [Электронный ресурс] // Securitylab.ru by Positive Technologies. URL: https://www.securitylab.ru/blog/company/Rubikon/355166.php?ysclid=mal2t5z66m83313170 (дата обращения: 12.03.2026); Что ждёт сферу кибербезопасности в 2025 году: тренды, технологии и ключевые скиллы [Электронный ресурс] // Хабр. URL: https://habr.com/ru/companies/netologyru/articles/900718/ (дата обращения: 12.03.2026).

[11] Полякова Т. А. Развитие информационных технологий и права на информацию в современном цифровом пространстве: риски и юридическое прогнозирование // Вестник Академии права и управления. 2019. № 1 (54). С. 97–103.

[12] О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) : Регламент № 2016/679 Европейского

Это создаёт правовые риски для организаций, использующих международные облачные платформы для обработки персональных данных в цифровой форме, а также сложности при расследовании инцидентов информационной безопасности в связи с возникающими проблемами доступа к логам и данным, что снижает эффективность предпринимаемых мер по установлению лиц, виновных в нарушении требований безопасности информации. Полагаем, решение этих и многих иных вопросов возможно лишь на основе гармонизации законодательств государств на межгосударственном уровне. Перспективным инструментом является также заключение двухсторонних и многосторонних межгосударственных соглашений, поскольку в современных условиях глубокого проникновения цифровизации во все сферы возможностей простого комплаенса уже недостаточно. При этом следует также отметить разрозненность национальных законодательств в определении киберпреступлений, что создаёт существенные препятствия для эффективного международного сотрудничества в области преследования киберпреступников. Кроме того, в настоящее время пока не выработаны единые или хотя бы широко признанные на международном уровне унифицированные критерии определения компьютерных инцидентов.

В связи с этим следует признать соответствующими требованиям времени инициативы по гармонизации законодательства на основе принятой в 2025 году Ханойской конвенции о киберпреступности[14]. Полагаем, такая динамика послужит значительному прогрессу в вопросах борьбы с киберпреступностью. Вместе с тем участие государств в таких соглашениях остаётся добровольным. В связи с этим по-прежнему сохраняется актуальность заключения двухсторонних и многосторонних межгосударственных механизмов противодействия киберпреступности.

Следует также отметить сложный и многоэтапный характер современных кибератак, что создает определенные трудности в выявлении источника, цифровых следов и в последующем определении достаточности действий операторов информационных систем и цифровых платформ по внедрению средств защиты информации. Эта ситуация еще более сложная при аутсорсинге и использовании цифровых сервисов третьей стороны. При этом оценка эффективности совокупности предпринятых оператором организационно-правовых и технических мер в условиях отсутствия установленных критериев в этой области требует учета комбинированного характера кибератак с использованием уязвимостей в сторонних сервисах.

Вместе с тем нормы Федерального закона «Об информации, информационных технологиях и о защите информации» носят в части обязанности операторов по обеспечению информационной безопасности рамочный характер и не конкретизируют критерии достаточности мер защиты. Однако проведенное исследование свидетельствует, что в условиях распределённых информационных систем, роста цифровых платформ и сервисов, применения технологий больших данных и искусственного интеллекта установление причинно-следственной связи между действиями оператора и наступившими последствиями кибератак является в практике защиты информации одной из сложнейших задач. Это может повлечь значительный ущерб национальной безопасности при каскадном отказе нескольких взаимосвязанных информационных систем и платформ, управляемых разными операторами. В связи с этим актуализируется вопрос распределения ответственности в цепочке взаимодействия операторов, провайдеров услуг и субподрядчиков.

Следует отметить, что сложность современных киберугроз и превращение деятельности злоумышленников в преступный бизнес актуализируют целесообразность постоянного совершенствования нормативной правовой базы, включая область технического регулирования, включая вопросы лицензирования, сертификации, аттестации и стандартизации. Динамичное развитие цифровых технологий формирует новые риски, что требует адаптации правовых и технических регуляторных требований к быстро меняющимся технологиям и методам кибератак, периодического пересмотра критериев оценки безопасности информации, оперативной разработки и внедрения требований к новым классам информационных систем, цифровым платформам и сервисам. Указанное должно явиться одним из главных векторов развития правового обеспечения безопасности российской информационной инфраструктуры.

парламента и Совета Европейского Союза (принят в г. Брюсселе 27.04.2016) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 20.04.2026).

[13] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

[14] О церемонии подписания конвенции ООН против киберпреступности и конференции высокого уровня в Ханое (Вьетнам), 25–26 октября 2025 года [Электронный ресурс] // Официальный сайт Министерства иностранных дел Российской Федерации. URL: https://www.mid.ru/ru/foreign_policy/un/2055978/ (дата обращения: 20.04.2026).

В последнее время важное место в теории и практике обеспечения информационной безопасности этическими, организационно-правовыми и техническими средствами занимает риск-ориентированный подход, позволяющий дифференцировать требования к информационным системам в зависимости от потенциального ущерба от реализации информационных угроз и их вероятности последствий, чем объясняется внимание исследователей к данному методологическому решению[15]. Применение риск-ориентированного подхода при построении системы защиты информации в организации позволяет обеспечить оптимальное распределение имеющихся ресурсов и повысить гибкость защитных механизмов, что целесообразно учитывать при совершенствовании правового обеспечения информационной безопасности. Вместе с этим для практической реализации риск-ориентированного подхода в правоприменительной практике положительную роль сыграет установление единых критериев и методик оценки уровня информационных угроз в подзаконных актах. В настоящее время ориентиром для практиков могут служить только положения документов по стандартизации. Положительное влияние, полагаем, также будет иметь создание типовых профилей защищённости для различных категорий информационных систем с конкретизацией минимального уровня защитных мер. В настоящее время такие требования установлены в отношении государственных информационных систем и информационных систем персональных данных, что представляется недостаточным. Кроме того, указанные нормы определены на уровне правовых актов и методических документов федеральных органов исполнительной власти[16].

Таким образом, в связи с экспоненциальным ростом использования цифровых технологий и их трансформационным влиянием на общественные отношения возникают определенные вопросы в связи с регулированием цифровых данных. Это актуализирует внедрение гибких регуляторных механизмов, в том числе так называемых цифровых песочниц, которые представляют собой применение перспективного механизма тестирования инновационных правовых решений в области информационной безопасности[17]. Экспериментальные правовые режимы в сфере цифровых инноваций позволяют создавать контролируемые правовые среды для апробации новых технологий без применения обычно действующих нормативных требований, а также формировать потенциальные правила регулирования в отношении продуктов на базе прорывных цифровых технологий.

Особую актуальность такие гибкие механизмы приобретают в условиях динамичного развития цифровых платформ, технологий искусственного интеллекта, квантовых технологий и интернета вещей, для которых традиционные правовые средства не всегда применимы при регулировании взаимосвязанных общественных отношений. Обращает на себя внимание тот факт, что сложившаяся практика применения регуляторных песочниц уже показывает их эффективность. Однако, безусловно, целесообразно их дальнейшее развитие для обеспечения безопасности при одновременном сохранении достаточной свободы для тестирования инновационных решений и продуктов. Кроме того, целесообразно развивать способы интеграции успешных правовых решений в сфере цифровых инноваций в правовое поле.

В завершение следует отметить, что дифференциация требований в области информационной безопасности также должна учитывать специфику различных отраслей экономики и управления в условиях цифровой трансформации государства и формирования экономики данных, поскольку универсальные подходы не всегда адекватно отражают уровень рисков в таких сферах, как здравоохранение, транспорт, образование, наука, промышленность или энергетика, для которых последствия киберинцидентов могут быть порой критическими. В связи с этим формирование отраслевых профилей защиты информационных систем, с учетом особенностей их функционирования и использовании, безусловно, позволит установить требования, соответствующие технологическим особенностям конкретных секторов экономики и управления.

Таким образом, проведенное научное исследование позволило выявить ряд направлений совершенствования правового обеспечения информационной безопасности, обусловленных стремительной

---

[15] Букалерова Л. А., Лапшин В. Ф., Остроушко А. В. Риск-ориентированный подход в области правового регулирования обеспечения информационной безопасности несовершеннолетних // Вестник Сургутского государственного университета. 2021. № 1 (31). С. 76–83.

[16] Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования : приказ Минкомсвязи РФ от 25.08.2009 № 104 // Российская газета. 2009; Методический документ «Методика анализа защищенности информационных систем» (утв. ФСТЭК России 25.11.2025) [Электронный ресурс] // Официальный сайт ФСТЭК России. URL: https://fstec.ru, 15.12.2025; Методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах» (утв. ФСТЭК России 12.04.2026) [Электронный ресурс] // Официальный сайт ФСТЭК России. URL: https://fstec.ru, 28.04.2026; и др.

[17] Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации : Федеральный закон от 31.07.2020 № 258-ФЗ (ред. от 31.07.2025) // СЗ РФ. 2020. № 31 (часть I). Ст. 5017.

динамикой цифровой трансформации государства и формированием экономики данных, а также определить основные векторы дальнейшего совершенствования законодательства. При этом ключевым принципом в этой области должен быть баланс интересов различных субъектов, позволяющий, с одной стороны, конкретизировать и усиливать требования, а с другой – стимулировать инновационное развитие цифровых технологий. Вместе с тем в настоящее время целесообразно развивать адаптивные правовые механизмы, учитывающие специфику технологий, информационных систем и сферы их применения.

А. И. Химченко,

канд. юрид. наук, доцент кафедры информационных технологий и цифрового права ФГАОУ ВО «Московский государственный юридический университет имени О. Е. Кутафина», г. Москва

Отдельные вопросы правового обеспечения оборота данных в условиях развития экономики данных и цифровой трансформации

В условиях интенсивной цифровой трансформации происходит видоизменение форм и механизмов реализации правоотношений, формирование новых инструментов взаимодействий и экономических моделей. Происходящие процессы меняют подходы к использованию, обработке и обороту данных между участниками и субъектами взаимодействия, их взаимодействия с информационной инфраструктурой.

Одновременно меняется сама природа и сущность данных. От статичной модели (и соответствующим ей традиционным механизмам учета, обработки, хранения, защиты) трансформируется в динамическую – в технологических процессах с данными возникают производные данные на данные, которые также ложатся в основу новых процессов (и могут использоваться для поведенческой аналитики, профилирования, прогнозирования, парсинга открытых данных, обогащения, алгоритмической обработки и других решений).

Указанная ситуация предопределяет необходимость осмысления, систематизации и поиска новых правовых решений в части использования и обеспечения оборота таких данных, а также конструкций по их защите.

Новые решения экономики данных требуют правовые конструкции своего функционирования. Основа для этих конструкций – данные.

Вместе с тем на текущий момент не сформированы концептуальные регуляторные подходы в отношении новой категории данных, будь то пользовательские, большие, производные или другие категории данных в контексте экономики данных, применительно к которым нет легального определения их сущности, закрепления их роли в правоотношениях, взаимосвязи с персональными данными, механизмов оборота, режима права собственности.

Несмотря на то, что дефиниции традиционно являются одной из фундаментальных проблем информационного права[18], на данном этапе проблема легальной дефиниции такой сущности – понятия пользовательских (либо же разновидности наблюдаемых, прогнозных и пр.) данных рассматривается преимущественно для понимания проблематики (и для этого обозначим их просто «пользовательскими»).

В то же время в качестве примера необходимости поиска подходящей дефиниции можно отметить ситуацию с определением больших данных, которой были характерны попытки механистического переноса в правовую понятийную систему технологических характеристик больших данных, использования логически близкого понятия «обработка больших объемов данных» и др.[19].

Разработка дефиниции представляет довольно нетривиальную задачу, поскольку, решая ее, необходимо заранее определиться с соотнесением понятий «данные» и «информация», а также концептуально определиться с тем, что такое пользовательские данные, их взаимосвязь и отличия от персональных и их производных.

[18] Терещенко Л. К. Трансформация понятийного аппарата информационного права в условиях цифровизации // Журнал российского права. 2022. № 12. С. 98–110.

[19] Химченко А. И. Информационно-правовые вопросы регулирования больших данных: поиск доверенных решений. Вестник Московского университета. Серия 26: Государственный аудит. 2023. № 4. С. 106–118.

При этом уже на данном этапе необходимо определиться, становятся ли такие данные новой информацией, остаются ли разновидностью персональных либо приобретают какую-то иную форму и наименование, поскольку на следующем этапе неизбежно возникает новый вопрос. В случае если это уже информация, то действующее законодательство подразумевает ее свободный оборот, но это может противоречить интересам субъектов данных. А если такие данные это разновидность персональных, то законодательство о персональных данных не допускает их свободного оборота и это ограничивает реализацию самого принципа экономики данных.

Другим концептуальным вопросом регулирования пользовательских данных является определение степени применимости результатов их автоматизированной обработки. Поскольку, с одной стороны, действующее регулирование, в частности ст. 16 Федерального закона от 27.07.2006 № 152-ФЗ[20], исключает принятие на основании автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении их субъекта. В то же время в основе непосредственно технологической реализации лежит принятие алгоритмических решений на основе поступающих массивов данных.

Таким образом, на текущем этапе задача сводится в том числе и к поиску точек пересечения действующего законодательства о данных и новых технологических сущностей.

Цель. После дефиниции представляется необходимым определить цель, преследуемую в процессе сбора и обработки пользовательских данных, поскольку в технологическом цикле появляются и используются новые массивы данных.

Оборот данных. После определения первоочередных понятийных и организационных задач следует обратиться к проблематике организации гражданского оборота данных.

На данный момент такой оборот данных в принципе запрещен действующим законодательством – нормы о банковской тайне, тайне связи, персональных данных, режим коммерческих тайн защищают частные данные потребителей. Одновременным обязательным условием является наличие согласия клиентов на обработку их данных.

Важный момент в вопросе оборота данных и их возможных источников отчасти отражен в судебной практике (спор «ВКонтакте» и ООО «Дабл»[21]), где был сформирован подход, не предполагающий возможности отнесения данных в социальных сетях к общедоступным и не допускающий их последующей обработки без согласия субъекта[22].

Права на данные. Одним из приоритетных для решения в данном направлении вопросов является установление и распределение прав на данные. Как отмечается в исследованиях, правовой режим персональных данных тесно связан с конституционным правом человека на неприкосновенность частной жизни и, будучи проявлением нематериального блага, является неотчуждаемым и непередаваемым иным способом, что, в свою очередь, затрудняет коммерциализацию данных и создание цивилизованного рынка их обмена[23].

Ключевым вопросом является распределение прав на данные. В условиях повышенной экономической ценности данных принципиальное значение приобретает то, кто обладает правом на них. В то же время, обратившись к закону о персональных данных, как наиболее близкому к тематике регулирования оборота данных, можно отметить, что за много лет своего действия в нем не нашел ответа вопрос о том, кем создаются данные и кому они принадлежат. При этом течение необратимых процессов, в которых определенные данные (например ФИО) создают родители, а не субъект данных, в то время как другие присваивают государственные органы (СНИЛС, ИНН), лишь актуализируют вопрос их принадлежности.

Вопрос определения прав на данные имеет высокую практическую значимость, поскольку ценность в процессе реализации технологии возникает не только в результате их обработки, но в отношении самих данных как актива.

Указанный вопрос актуален и в контексте исключительных прав, поскольку в определенных случаях данные подпадают под понятие охраняемых объектов авторского права, и возникает вопрос несовместимости свободного движения данных и абсолютного права на данные[24].

---

[20] СЗ РФ, 31.07.2006, № 31 (1 ч.), ст. 3451.

[21] См.: решение АС г. Москвы от 12.10.2017, постановление Девятого ААС от 06.02.2018 по делу № А40-18827/17; постановление СИП от 24.07.2018 № С01-201/2018.

[22] Определение Верховного Суда РФ от 29 января 2018 г. № 305-КГ17-21291 по делу № А40-5250/2017.

[23] Савельев А. И. На пути к концепции регулирования данных в условиях цифровой экономики // Закон. 2019. № 4. С. 174–195.

[24] Войниканис Е. А. Регулирование больших данных и право интеллектуальной собственности: общие подходы, проблемы и перспективы развития // Закон. 2020. № 7. С. 135–156.

Специфика современных технологий обработки данных предполагает различные варианты их использования (как товара) и результатов такой обработки. В ситуации, когда наборы данных способны создавать различную ценность в зависимости от целей обработки, обогащения другими массивами данных либо обновления задачи использования, актуальной становится и задача создания правовых условий для их многократного использования.

Таким образом, невозможность распространения на пользовательские данные существующих правовых режимов ставит вопрос поиска новых. А также ответа на фундаментальный вопрос – целесообразно ли признание таких данных новым объектом информационных правоотношений.

Доверенный оборот данных. В качестве завершения следует отметить, что это лишь малый и далеко не исчерпывающий набор вопросов. Но в то же время регуляторные вопросы оборота данных становятся фундаментальными в условиях развития экономики данных.

Вместе с тем важным принципом реализации взаимодействия в любой среде является доверие, что также крайне актуально как для экономики в целом, так и для развития технологической основы экономики данных.

Фундаментально доверие в экономике состоит из множества факторов, среди которых отношение экономических агентов друг к другу, доверие общества к действиям государства и доверие государства к действиям экономических агентов. А принимая во внимание технологические особенности экономики данных, актуальным вопросом становится и обеспечение механизмов доверенного оборота данных.

Закономерно, что проблематика формирования доверия нашла отражение и ранее при разработке программы «Цифровая экономика»[25], где среди вызовов цифровой трансформации была выделена проблема обеспечения доверия граждан к цифровой среде,

Несмотря на то, что подходы к обеспечению цифровой среды доверия не являются предметом настоящего исследования, следует отметить, что механизмы, реализующие доверенное взаимодействие, имеют ключевое значение для развития экономики данных и подразумевают широкий спектр задач в части конфиденциальности, сохранности, целостности, безопасности и достоверности данных и других[26].

Е. В. Некрасова,

канд. экон. наук, доцент, доцент кафедры информационной безопасности в управлении ФГБОУ ВО «Удмуртский государственный университет»,
доцент кафедры менеджмента и права ФГБОУ ВО Удмуртский ГАУ,
г. Ижевск

Управление процессами обеспечения информационной безопасности экономических субъектов в условиях цифровой трансформации государства

В целях обеспечения технологической и экономической независимости нашей страны в условиях цифровой трансформации экономики и развития искусственного интеллекта построение эффективной системы управления процессами обеспечения информационной безопасности на разных уровнях становится особенно актуальными.

Современные требования к формированию системы управления процессами обеспечения информационной безопасности различных экономических субъектов предполагают четкое регламентирование деятельности основных структурных подразделений и ответственных лиц в соответствии с установленными нормативно-правовыми требованиями и с учетом быстрых изменений факторов внешней и внутренней среды.

В первую очередь при построении эффективной системы управления процессами обеспечения информационной безопасности экономических субъектов необходимо руководствоваться базовыми нормативно-правовыми документами: Конституцией РФ, основными федеральными законами (ФЗ № 149 «Об информации... », ФЗ № 152 «О персональных данных»), указами Президента РФ (Указ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации

[25] Программа «Цифровая экономика Российской Федерации», утв. распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р // СЗ РФ. 2017. № 32, ст. 5138. Прим.: документ утратил силу с 12 февраля 2019 года в связи с изданием распоряжения Правительства РФ от 12.02.2019 № 195-р.

[26] Химченко А. И. Актуальные информационно-правовые вопросы формирования цифровой среды доверия // Правовое государство: теория и практика. 2023. № 4. С.78–86.

на 2017–2030 годы», Указ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Указ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации»), которые регулируют современное состояние и перспективы развития IT-отрасли, обеспечение защиты больших баз данных и использование искусственного интеллекта в системах принятия управленческих решений на разных уровнях.

Региональное управление процессами цифровой трансформации и обеспечения информационной безопасности фокусируется на интеграции мер управления данными процессами для различных отраслей с использованием федеральных, региональных и отраслевых мер государственного регулирования.

Так, на уровне Удмуртской Республики при принятии решений в данной сфере, помимо вышеуказанных нормативно-правовых актов, необходимо руководствоваться Указом Главы УР от 31.03.2020 № 74, который представляет собой ключевой документ, утвердивший Стратегию цифровой трансформации Удмуртии до 2030 года. В последних редакциях данного документа область информационной безопасности выделена как направление, необходимое для достижения «цифровой зрелости» экономики.

Кроме того, необходимо использовать распоряжение Главы УР от 20.11.2020 № 262-РГ (с учетом актуализации распоряжением от 04.03.2025 № 52-РГ), которое регулирует организационные вопросы цифровой трансформации для госструктур и экономических субъектов для соответствия новым вызовам в сфере информационной безопасности.

Однако в условиях быстрой цифровой трансформации экономики и систем государственного управления необходимо учитывать важные требования к современной системе информационной безопасности объектов. С нашей точки зрения, к их числу следует отнести следующее:

1. Стратегическая направленность в области технологической независимости, в т. ч.:

– акцент на импортозамещение (переход на отечественные средства защиты информации (СЗИ) и операционные системы, использование сертифицированных ФСТЭК/ФСБ решений);

– развитие организационно-технических систем повышения киберустойчивости объектов защиты, внедрение механизмов непрерывного мониторинга для выявления и реагирования на инциденты.

2. Совершенствование организационных форм и методов обеспечения информационной безопасности объектов, в т. ч.:

– развитие систем защиты критической информационной инфраструктуры объекта с обязательной категоризацией объектов и принятием комплекса решений по их защите;

– развитие систем управления цифровыми рисками, интеграция требований ИБ на ранних этапах разработки цифровых продуктов и систем.

Внедрение данных требований к развитию систем управления разного уровня является обязательным для обеспечения непрерывности бизнеса и защиты государственных информационных систем в рамках реализации национального проекта «Цифровая экономика».

Управление системой информационной безопасности сегодня – это в первую очередь стратегический вопрос, а не только организационно-технические мероприятия, обеспечивающий непрерывность экономических и административно-управленческих процессов. Неоспоримым является факт, что качество управленческих решений зависит от своевременности, полноты, структурированности и достоверности информации о характеристиках объекта, степени влияния факторов внешней и внутренней среды. В условиях цифровой трансформации экономики важными факторами является время принятия решений и обеспечения информационной безопасности, защиты персональных данных, государственной тайны и коммерческой информации.

В качестве основных рисков влияния цифровой трансформации на процессы управления экономическими объектами и систем государственного управления можно выделить:

– необходимость постоянной перестройки бизнес и управленческих моделей, что повышает эффективность, но увеличивает уязвимость к кибератакам, внутренним и внешним угрозам;

– развитие цифровых государственных услуг, что требует усиления взаимодействия общества и бизнеса с государственными цифровыми платформами, повышая значимость кибергигиены на всех уровнях;

– недостаточно разработанные цифровые технологии могут увеличивать ошибки обработки данных, неэффективные процедуры мониторинга и информационного контроля, устаревшие или некорректные данные для обучения систем искусственного интеллекта, могут искажать результаты;

– высокий риск неправильной реализации информационных технологий отдельных экономических субъектов может привести к финансовым и репутационным потерям и росту затрат на внедрение и поддержание управленческих решений;

– неготовность персонала к работе с новыми технологиями, сопротивление изменениям со стороны сотрудников, дефицит квалифицированных специалистов, способных управлять цифровыми процессами.

Для минимизации этих рисков необходим комплексный подход, включающий развитие нормативно-правовой базы на разных уровнях, инвестиции в обеспечение кибербезопасности, обучение кадров основам ИБ, обеспечение доступности цифровых технологий для всех слоёв населения и мониторинг качества данных.

Сегодня управление информационной безопасностью экономических субъектов в условиях цифровой трансформации требует перехода от реактивной защиты к проактивной модели. Ключевые процессы проактивной модели системы управления информационной безопасностью объектов должны включать систему стратегического планирования, развитие систем комплексной защиты данных для принятия и реализации решений, внедрение современных цифровых технологий и адаптацию к новым вызовам и возможностям, обеспечивая устойчивость к угрозам разного уровня.

Каждая организация может сформировать комплекс управленческих решений в зависимости от потребностей в информационной защите обеспечения информационной безопасности. В число таких решений может входить:

– формирование и реализация стратегии развития информационной безопасности организации с учетом основных социально-экономических и технологических тенденций;

– развитие передовых технологий обнаружения, устранения и предотвращения угроз в области информационной безопасности;

– совершенствование адаптивной и многоуровневой системы информационной безопасности в организации;

– обеспечение своевременного реагирования на изменение нормативно-правовых требований и регуляторов уровня соответствия необходимым параметрам критической инфраструктуры объектов;

– постоянное ведение аналитики вероятных и актуальных киберугроз для разных уровней управления и объектов в организации;

– повышение качества обучения сотрудников организации основам информационной безопасности, формирование внутренней корпоративной культуры в данной сфере.

С нашей точки зрения, любые решения в области развития цифровых технологий должны быть сконцентрированы на реализации стратегического потенциала объекта на основе обеспечения информационной безопасности систем управления разного уровня, что позволит добиться необходимого уровня конкурентоспособности и социально-экономической стабильности организационного развития в долгосрочной перспективе с учетом динамики развития внешней и внутренней среды.

Т. В. Пашнина,

канд. юрид. наук, доцент, доцент кафедры общетеоретических правовых дисциплин Уральского филиала ФГБОУ ВО «Российский государственный университет правосудия им. В. М. Лебедева»,
г. Челябинск

Влияние нейротехнологий на обеспечение информационной безопасности личности

Конец XX – начало XXI вв. ознаменовали собой появление прорывных технологий, которые не только привели к качественной трансформации различных сфер жизнедеятельности: промышленности, экономики, военного дела, медицины, образования и т. д., но и оказались способны изменить природу человека, что, в свою очередь, поставило новые вопросы перед обеспечением информационной безопасности личности.

К числу таких технологий относятся *нейротехнологии* – «технологии, которые используют или помогают понять работу мозга, мыслительные процессы, высшую нервную деятельность, в том числе технологии по усилению, улучшению работы мозга и психической деятельности» (п. 3.34 ГОСТа Р 59277-2020 «Системы искусственного интеллекта. Классификация систем искусственного интеллекта»[27]; Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект»[28], др.).

[27] ГОСТ Р 59277-2020. Системы искусственного интеллекта. Классификация систем искусственного интеллекта [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200177292/ (дата обращения: 30.03.2026).

[28] Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект» [Электронный ресурс]. URL: https://digital.gov.ru/uploaded/files/07102019ii.pdf (дата обращения: 30.03.2026).

Анализируя правовую природу нейротехнологий, необходимо отметить, что они могут быть отнесены к категориям стратегически значимых технологий, в том числе:

- ✓ *Прорывных технологий*, относящихся к группе НБИКС-технологий, находящихся на «стыке» био- (соматических) и инфо- (цифровых)[29].
- ✓ *Сквозных технологий*, способных применяться совместно с технологиями искусственного интеллекта – ИИ (Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект»[30]); виртуальной и дополненной реальности (проекты Центра Национальной технологической инициативы[31]).
- ✓ *Критических технологий* («биомедицинские и *когнитивные* технологии здорового и активного долголетия» – Указ Президента РФ № 529 от 18.06.2024 «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоемких технологий»[32]).

Применяемые в настоящее время нейротехнологии классифицируются по различным основаниям. В том числе нормативные акты, документы по стандартизации, а также представители экспертного сообщества называют следующие *виды нейротехнологий*:

- ✓ Технологии (устройства), отслеживающие нейронную активность; технологии (устройства), изменяющие (модулирующие) нейронную активность; бимодальные технологии (устройства), объединяющие обе функции.
- ✓ Технологии (устройства) нейровизуализации; технологии (устройства) нейростимуляции.
- ✓ Инвазивные нейротехнологии; неинвазивные нейротехнологии.
- ✓ Нейропротезирование; нейроинтерфейсы, нейростимуляция и нейросенсинг[33].

Все вышеперечисленные технологии (устройства) собирают *нейроданные* – особый вид информации об активности головного мозга.

Говоря о сфере применения нейротехнологий, Д. А. Белова в монографическом исследовании «Нейроправо. Правовой аспект исследования применения нейротехнологий» (2025) отмечает: сфера применения нейротехнологий весьма широка – от медицинских целей, например лечения болезней Альцгеймера и Паркинсона; использования в военных целях, связанных с повышением когнитивных способностей участников боевых действий, – до использования с целью общения, развлечения и получения образования[34].

В данном контексте особого внимания заслуживает тот факт, что цели применения нейротехнологий могут быть как медицинские, так и немедицинские, а способы – как инвазивные, так и неинвазивные. При этом неинвазивные нейротехнологии, применяемые в немедицинских целях, вызывают особое беспокойство у исследователей с точки зрения правовых и этических аспектов.

Аналитики отмечают, что «юристов и защитников данных больше беспокоят нейроданные, собираемые не специфически медицинскими компаниями – ведь в отношении медицинских разработок и так действуют довольно строгие нормы регулирования. А вот в случае потребительских гаджетов такого регулирования пока практически не существует. <…> На рынке действуют десятки производителей различных гаджетов, улавливающих импульсы головного мозга. Эти гаджеты разработаны так, чтобы с помощью небольших электродов считывать активность головного мозга и собирать нейронные данные, а в некоторых случаях и воздействовать на мозговую активность электрическими импульсами. По сути, это упрощенная версия электроэнцефалографии, электромиографии и других технологий, используемых в медицинских устройствах.

Среди подобных устройств – маски для сна, предназначенные для оптимизации глубокого сна или способствующие осознанным сновидениям, повязки на голову для улучшения концентрации, гарнитуры для медитаций и т. д.»[35].

---

[29] См., напр.: Корнехо Я. Нейроправа, нейротехнологии и персональные данные: обзор проблем психологической автономии // Journal of Digital Technologies and Law. 2024. № 2 (3). P. 711–728.

[30] [Электронный ресурс]. URL: https://digital.gov.ru/uploaded/files/07102019ii.pdf (дата обращения: 30.03.2026).

[31] Центр компетенций НТИ по направлению «Нейротехнологии, технологии виртуальной и дополненной реальности» [Электронный ресурс]. URL: https://nti2035.ru/technology/competence_centers/fefu.php (дата обращения: 30.03.2026).

[32] СЗ РФ. 2024. № 26. Ст. 3640.

[33] См.: Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект». URL: https://digital.gov.ru/uploaded/files/07102019ii.pdf (дата обращения: 30.03.2026); Предварительный национальный стандарт РФ ПНСТ 981-2024. Нейротехнологии и нейроинтерфейсы. Термины и определения. URL: https://docs.cntd.ru/document/1310381187/ (дата обращения: 30.03.2026); Белова Д. А. Нейроправо. Правовой аспект исследования применения нейротехнологий : моногр. М. : Проспект, 2025. С. 14–26; Филипова И. А. Нейротехнологии: развитие, применение на практике и правовое регулирование // Вестник Санкт-Петербургского университета. Право. 2021. Т. 12, вып. 3. С. 504; и др.

[34] Белова Д. А. Нейроправо. Правовой аспект исследования применения нейротехнологий : моногр. М. : Проспект, 2025. С. 20–23.

[35] Рождественская Я. Приватность пришла в биологию [Электронный ресурс] // Коммерсантъ : [сайт газеты]. 2024. URL: https://www.kom-mersant.ru/doc/6917393 (дата обращения: 20.03.2026).

В свете этого справедливым представляется утверждение о том, что «современные достижения в области исследований мозга и ИИ позволяют собирать большой объем личной информации, которая раньше казалась недоступной для получения... Такая информация обладает высокой ценностью для коммерческих и государственных структур, поэтому вполне вероятно, что в ближайшем будущем как инвазивные, так и неинвазивные методы сбора этих данных станут повсеместной практикой»[36].

Очевидно, что недостаточное правовое регулирование использования нейротехнологий и полученных в результате их применения нейроданных порождает ряд рисков и вызовов как для информационной безопасности личности, так и для института прав человека, в целом.

В научных исследованиях выделяют следующие *риски*, связанные с нейротехнологиями:

- ✓ *медико-биологические риски*, связанные с возможным повреждением головного мозга и побочными эффектами, касательно которых отсутствуют достаточные эмпирические данные;
- ✓ *технологические риски*: уязвимости нейроинтерфейсов и нейроимплантов к кибератакам (риски хакерства), технические сбои;
- ✓ *правовые и этические риски*: утрата автономии личности (манипуляции сознанием, навязанные эмоции и мысли); угроза для частной жизни (вопрос конфиденциальности психической деятельности); цифровое неравенство (доступ к технологиям только при наличии финансовых возможностей); принудительное применение (армия, места лишения свободы и др.)[37].

Последняя группа рисков привлекла внимание мирового сообщества, на уровне ЮНЕСКО, обозначившего *четыре главных вызова нейротехнологий* для человеческой личности:

- ✓ *Церебральная и психическая неприкосновенность и человеческое достоинство.* Нейротехнологии открывают возможности для инвазивного и всепроникающего изменения мозга, следовательно, и сознания.
- ✓ *Целостность человеческой личности.* Человек имеет право думать и чувствовать самостоятельно, но, когда мозг будет подключаться к компьютеру, личность может размываться, в том числе потому, что алгоритмы будут помогать ей принимать решения.
- ✓ *Свобода мысли, когнитивная свобода и свобода воли.* Нейротехнологии могут повлиять на работу нашего мозга, а значит, и на свободу мышления, принятия решений и действий. Это может оказать серьезное влияние на системы правосудия и социальные организации.
- ✓ *Психическая неприкосновенность и конфиденциальность данных о мозге.* Нейротехнологии могут получать множество данных из нашего мозга, и эти «частные» данные необходимо защищать[38].

Решение проблемы правового обеспечения информационной безопасности личности при применении нейротехнологий и обработке нейроданных, на наш взгляд, включает ответы на четыре ключевых вопроса.

- ✓ *Что должно защищаться с позиции института прав человека?* На данный вопрос отвечает категория *нейроправ*, которая в нашей стране на сегодняшний день не получила достаточного теоретического осмысления и закрепления на национальном, конституционного либо отраслевого законодательства, уровне.

При этом, несмотря на несомненную важность нейроправ, полагаем, что их закрепление по модели Чили на конституционном уровне[39] является избыточным. Более целесообразной представляется трактовка существующих конституционных прав (на свободу мысли, личную и семейную тайну и т. д.) с точки зрения возможностей и рисков нейротехнологий, которую может, при необходимости, дать высший судебный орган конституционного контроля – Конституционный Суд РФ.

- ✓ *Что является основным объектом правоотношений, возникающих при применении нейротехнологий?*

Таковым, на наш взгляд, являются – *нейроданные*, в качестве которых экспертами предлагается рассматривать «данные о нейронной активности нервной системы человека, включая нейронную активность головного мозга, периферической нервной системы, а также сведения, полученные на основе этих данных»[40].

Нейроданные по своей правовой природе представляют собой особый вид информации, требующий закрепления на уровне информационного законодательства (федеральных законов: от 27.07.2006

---

[36] Лихачев Г. Нейроправа и когнитивная свобода [Электронный ресурс] // Insolarance : [сайт]. URL: https://insolarance.com/neurorights-and-cognitive-liberty/ (дата обращения: 20.03.2026).

[37] См.: Посадкова М. В., Брежнева Е. А. Правовое регулирование нейротехнологий: игра без правил или жесткий контроль? // Lex Genetica. 2025. № 4 (2). С. 49; и др.

[38] Этика нейротехнологий [Электронный ресурс] // UNESCO. URL: https://www.unesco.org/ru/ethics-neurotech?hub=83294 (дата обращения: 20.03.2026).

[39] См.: Посадкова М. В., Брежнева Е. А. Указ. соч. С. 55; и др.

[40] Белова Д. А. Указ. соч. С. 98.

№ 149-ФЗ «Об информации, информационных технологиях и о защите информации»[41], от 27.07.2006 № 152-ФЗ «О персональных данных»[42], от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации»[43], и др.) с установлением особенностей режима доступа к нему.

✓ *Какие действия являются недопустимыми при сборе, обработке и использовании нейроданных?* Основным средством решения данного вопроса должна стать разработка этических документов, подобных этическим рекомендациям ЮНЕСКО – «Draft Recommendation on the Ethics of Neurotechnology» (2025)[44]. На сегодняшний день такие документы в Российской Федерации отсутствуют.

Здесь также следует отметить, что процесс сбора и обработки нейроданных в медицинских целях предполагает жестко регламентированную процедуру, соответствующую не только положениям Закона о персональных данных, но и требованиям к целям их обработки, установленным федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[45].

✓ *Каков должен быть правовой механизм обеспечения информационной безопасности при обработке нейроданных?*

Формирование такого механизма должно вестись с позиций системного подхода, предполагающего принятие новых либо внесение соответствующих изменений в целый ряд взаимосвязанных нормативных актов: упомянутых выше федеральных законов; документов стратегического планирования (в области обеспечения информационной безопасности, развития нейротехнологий, и т. д.); документов технического регулирования; кодексов и др.

Вышесказанное позволяет сделать вывод о том, что нейротехнологии, способные оказать положительное влияние на решение ряда вопросов, например, связанных с коррекцией тяжелых заболеваний, а также использоваться во взаимосвязи с искусственным интеллектом, значительно повышая эффективность последнего, содержат в себе серьезные риски для безопасности личности, связанные с потенциальной возможностью отслеживания мыслей, эмоций, воспоминаний человека, включая возможность их модификации, и, следовательно, управления поведением человека. Поскольку ключевую роль в данном процессе играет особый вид информации – нейроданные, последние нуждаются во всестороннем теоретическом осмыслении и адекватной правовой защите.

Э. Г. Хомяков,
канд. юрид. наук, доцент, доцент кафедры уголовного процесса и криминалистики
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Применение технологий искусственного интеллекта в цифровой криминалистике: стратегические приоритеты для правоохранительной системы Российской Федерации

Современный этап развития криминалистической науки и практики характеризуется стремительной цифровизацией всех аспектов расследования преступлений, что обусловливает необходимость интеграции передовых технологий искусственного интеллекта в деятельность правоохранительных органов. Цифровая криминалистика как «частная криминалистическая теория, представляющая собой систему научных положений и разрабатываемых на их основе технических средств, приемов, методик и рекомендаций по обнаружению, фиксации, предварительному исследованию, использованию компьютерной информации и средств ее обработки в целях раскрытия, расследования и предупреждения преступлений»[46], требует качественного обновления методологического аппарата в условиях экспоненциального роста объемов цифровых данных.

[41] СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.
[42] СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.
[43] СЗ РФ. 2023. № 1 (ч. I). Ст. 1.
[44] [Электронный ресурс]. URL: https://unesdoc.unesco.org/ark:/48223/pf0000394866 (дата обращения: 20.03.2026).
[45] СЗ РФ. 2011. № 48. Ст. 6724.
[46] Цифровая криминалистика : учебник для вузов / под ред. В. Б. Вехова, С. В. Зуева. М. : Юрайт, 2023. С. 25 [Электронный ресурс]. URL: https://urait.ru/bcode/520165 (дата обращения: 20.04.2026).

Искусственный интеллект как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их»[47], способен значительно повысить эффективность раскрытия и расследования преступлений, значительно расширяя инструментарий субъектов криминалистической деятельности. Однако практическое применение технологий искусственного интеллекта требует выработки обоснованной и системной модели их внедрения, адаптированной к организационным и правовым особенностям российской правоохранительной системы.

Опыт применения подобных технологий в криминалистической деятельности демонстрирует их значительный потенциал в таких направлениях, как автоматизированный анализ больших массивов цифровых данных, например, в системах криминалистической регистрации, прогнозирование криминогенной обстановки на отдельных территориях и в населенных пунктах, биометрическая идентификация, обработка мультимедийного контента и т. д.

Например, в дактилоскопии широкое распространение получили автоматизированные дактилоскопические информационные (идентификационные) системы (АДИС)[48]. Так АДИС «Папилон», применяемая в МВД России почти 30 лет, в результате своего развития приобрела «мультибиометрический формат регистрационной записи, более совершенные алгоритмы кодирования и сравнения папиллярных узоров»; «применение нейросетевых алгоритмов на действующих базах данных» позволило «многократно снизить затраты труда операторов АДИС на просмотр рекомендательных списков» и «повысить результативность АДИС в части идентификации объективно сложных малоинформативных следов»[49].

В баллистической экспертизе аналогичный подход реализован в автоматизированных баллистических идентификационных системах (АБИС). Например, системы «Арсенал»[50] и «ПОИСК»[51], оснащенные оптико-электронными сканерами и сопряженные с цифровыми пулегильзотеками, обеспечивают высокоавтоматизированный сравнительный анализ баллистических микроследов на стреляных пулях и гильзах.

Несомненно, формирование стратегических приоритетов в области внедрения искусственного интеллекта в цифровую криминалистику должно происходить с учетом нескольких взаимосвязанных направлений.

Первостепенное значение имеет развитие нормативно-правовой базы, регулирующей применение алгоритмических систем в процессе доказывания. Существующее уголовно-процессуальное законодательство не содержит специальных норм, определяющих статус доказательств, сформированных с применением средств искусственного интеллекта[52], в частности систем машинного обучения для распознавания образов, нейросетевых моделей анализа метаданных, автоматизированных средств верификации биометрических параметров. Необходимо законодательное закрепление критериев допустимости таких доказательств, требований к объяснимости алгоритмов (explainable AI, XAI)[53], возможности независимой верификации результатов и обеспечения прав участников судопроизвод-

---

[47] Национальная стратегия развития искусственного интеллекта на период до 2030 года (п. 5а) : Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) [Электронный ресурс]. URL: https://base.garant.ru/72838946/ (дата обращения: 20.04.2026); Об искусственном интеллекте в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации : проект Федерального закона [Электронный ресурс]. URL: https://zsrf.ru/uploads/files/Проект%20ФЗ%20об%20ИИ.pdf (дата обращения: 20.04.2026).

[48] В международной практике известны как AFIS (Automated Fingerprint Identification System).

[49] Краткая история АДИС ПАПИЛОН. Нейросетевой анализ рекомендательных списков в АДИС ПАПИЛОН-9 [Электронный ресурс]. URL: https://www.papillon.ru/wp-content/uploads/ADIS_Neiro_Papillon.pdf (дата обращения: 20.04.2026).

[50] Арсенал – система идентификации оружия [Электронный ресурс]. URL: https://www.papillon.ru/products/programs/arsenal/ (дата обращения: 20.04.2026).

[51] Области применения Технологии «ПОИСК» и задачи баллистической экспертизы, решаемые с помощью данной технологии [Электронный ресурс]. URL: https://sbc.spb.ru/index.php?option=com_content&view=article&id=4&Itemid=1&lang=ru (дата обращения: 20.04.2026).

[52] Под средствами искусственного интеллекта в настоящем исследовании понимаются программно-аппаратные комплексы, алгоритмы машинного обучения, нейросетевые модели и иные технологические решения, реализующие функции, отнесенные к искусственному интеллекту в соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 года (Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации») и ГОСТ Р 71476-2024 (ИСО/МЭК 22989:2022) «Искусственный интеллект. Концепции и терминология искусственного интеллекта».

[53] ПНСТ 836-2023 (ISO/IEC DTR 5469) «Искусственный интеллект. Функциональная безопасность и системы искусственного интеллекта», раздел 8.3 «Степень понятности и объяснимости»: объяснимость – свойство системы искусственного интеллекта (ИИ-системы) отражать важные показатели, влияющие на результаты, в виде, понятном для людей; XAI – аббревиатура от Explainable Artificial Intelligence (объяснимый искусственный интеллект).

ства на оспаривание автоматизированных выводов. Параллельно требуется совершенствование стандартов аккредитации лабораторий, применяющих технологии искусственного интеллекта, с учетом требований ГОСТ ISO/IEC 17025-2019[54] и специфики валидации алгоритмических методов анализа.

Технико-методологическое направление развития цифровой криминалистики предполагает формирование единой информационно-аналитической системы для работы с электронными доказательствами. Ее архитектура должна обеспечивать унификацию форматов данных, выработку согласованных протоколов изъятия и исследования носителей информации, а также защищенный обмен материалами между органами предварительного следствия, судебно-экспертными учреждениями (организациями) и судами. Функционал системы целесообразно строить на базе специализированных программных модулей: автоматического анализа метаданных, реконструкции удаленных файлов, идентификации пользователей в защищенных сетях, лингвистического и акустического паттерн-анализа, а также выявления признаков монтажа и генерации синтетического контента (дипфейков). Ключевым условием реализации выступает опора на отечественные программно-алгоритмические решения. Это не только отвечает задачам обеспечения технологического суверенитета, но и минимизирует риски, связанные с использованием внешних разработок в чувствительных сферах информационной безопасности.

Эффективность внедрения интеллектуальных технологий в криминалистическую практику напрямую зависит от уровня профессиональной подготовки специалистов, осуществляющих их применение и интерпретацию результатов. В этой связи формирование компетенций экспертов нового поколения должно опираться на интеграцию устоявшихся методологических основ криминалистической техники (прежде всего из области дактилоскопии, трасологии, баллистики) с современными знаниями в области программирования, статистического анализа и машинного обучения.

Помимо создания специализированных образовательных программ в ведомственных учебных заведениях, направленных на обучение сотрудников работе с технологиями искусственного интеллекта и алгоритмической аналитикой, необходимо постоянное развитие системы непрерывного повышения квалификации для действующих сотрудников, с акцентом на практическое освоение инструментов цифровой криминалистики и критическое осмысление пределов применимости алгоритмических методов.

Не менее важным является формирование культуры ответственного использования искусственного интеллекта, основанной на понимании этических аспектов, рисков когнитивных искажений и необходимости сохранения профессионального контроля над ключевыми этапами расследования преступлений.

Внедрение алгоритмических инструментов в деятельность по раскрытию, расследованию и предупреждению преступлений неизбежно сопровождается рядом технологических и правовых рисков, требующих системного контроля. На практике наиболее критичными выступают сбои в работе моделей машинного обучения, способные генерировать ложные совпадения при идентификации, а также уязвимости инфраструктуры, используемой для хранения и обработки массивов персональных и биометрических сведений. Дополнительную сложность создают вопросы этического характера, прежде всего связанные с автоматизированным профилированием и допустимыми пределами сбора цифровых следов. Для нейтрализации указанных угроз целесообразно внедрять процедуры регулярной валидации алгоритмических моделей, включая тестирование на смещение выборки и воспроизводимость результатов.

Также необходимо регламентировать порядок ведомственного контроля за эксплуатацией систем искусственного интеллекта и закрепить в уголовно-процессуальном законодательстве право участников судопроизводства на истребование пояснений к результатам алгоритмической обработки цифровых данных, положенным в основу процессуальных решений, а также на их обжалование.

Без сомнения, любое применение технологий искусственного интеллекта должно соответствовать требованиям статьи 23 Конституции РФ и Федерального закона № 152-ФЗ «О персональных данных», исключая немотивированное вторжение в частную жизнь и гарантируя соразмерность используемых средств и методов расследования задачам доказывания.

В заключение следует отметить, что развитие цифровой криминалистики зависит не от скорости появления новых технологий, а от степени их интеграции в уголовно-процессуальное законодательство и практику расследования преступлений. Арсенал современных инструментов расследования в ближайшее время будет стремительно расширяться. При этом приоритетом должна стать

[54] ГОСТ ISO/IEC 17025-2019 «Межгосударственный стандарт. Общие требования к компетентности испытательных и калибровочных лабораторий».

интеграция алгоритмической аналитики в структуру методик расследования, где программные решения будут выполнять функцию вспомогательного инструмента, оставляя приоритет за решениями следователя. Это позволит сократить время обработки массивов информационных данных, сохранив за следователем и судом окончательную оценку криминалистически значимой информации и формирование выводов, отвечающих требованиям допустимости доказательств. Такой подход гарантирует, что технологии искусственного интеллекта будут работать на укрепление доказательственной базы, станут инструментом, усиливающим, а не подменяющим профессиональное суждение субъектов доказывания.

С. А. Стяжкина,
канд. юрид. наук, доцент, доцент кафедры уголовного права и криминологии
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Виктимологические аспекты информационной безопасности несовершеннолетних

Обеспечение информационной безопасности личности является одной из актуальных проблем современного общества. Особого внимания требует проблема защиты несовершеннолетних от различных информационных угроз. С расширением сферы применения информационных технологий и массовым внедрением цифровых ресурсов в повседневную жизнь увеличилось и количество девиаций в рассматриваемой среде. Преступность все больше и больше приобретает «цифровой» характер и переходит в виртуальную среду, характеризующуюся анонимностью, трансграничностью, оперативностью, безнаказанностью и т. д. «Цифровая среда формирует качественно иную социальную реальность, где ослабевают традиционные механизмы нормативного регулирования и социального контроля»[55].

В научной литературе все чаще используется термин «кибервиктимизация», под которой предлагается понимать «процесс или конечный результат становления жертвы преступления в сфере объединенных компьютерных сетей»[56].

Несовершеннолетние в силу особенностей их физиологического, психоэмоционального, социального развития являются наиболее уязвимой группой в сфере информационного воздействия и влияния. Именно дети и подростки представляют наибольший интерес для криминальных структур в целях их вовлечения в преступную деятельность посредством использования информационных технологий. Кроме того, современные цифровые ресурсы оказывают колоссальное воздействие на процесс формирования личности несовершеннолетнего, проводящего в сети «Интернет» большую часть своего свободного времени. Как справедливо отмечается в литературе, «Процесс кибервиктимизации несовершеннолетних имеет специфические характеристики, связанные с возрастными, психологическими и социальными особенностями данной категории лиц»[57].

Несовершеннолетние все чаще становятся жертвами киберпреступлений. Но особую тревогу вызывает процесс вовлечения несовершеннолетних в преступную деятельность посредством использования информационных технологий. Особенностью несовершеннолетних жертв является то, что они, будучи жертвами, сами становятся преступниками. Процесс кибервиктимазиции одновременно является и процессом криминализации несовершеннолетних лиц. Таким образом, деятельность по виктимологической профилактике преступлений, совершаемых в отношении несовершеннолетних, одновременно является и профилактикой их преступного поведения.

Процесс кибервиктимизации несовершеннолетних является результатом взаимодействия факторов как объективного, так и субъективного характера.

К объективным факторам, влияющим на виктимность несовершеннолетних, прежде всего относится широкая вовлеченность несовершеннолетних в киберпространство и практически стопроцентное использование информационных технологий несовершеннолетними. Безусловно, цифровые

[55] Бакулина Р. А. Социальные практики цифровой девиации и факторы кибервиктимизации // Казанский социально-гуманитарный вестник. 2025. № 4(71). С. 4–10.

[56] Жмуров Д. В. Кибервиктимизиция. Исследовательская матрица // Пролог: журнал о праве. 2021. № 3. С. 109–121.

[57] Степанова Н. К. Зарубежный опыт эффективной профилактики киберпреступности в отношении несовершеннолетних правоохранительными органами // Управление образованием: теория и практика / Education Management Review. 2025. Т. 15, № 8-1.

ресурсы необходимы современным детям для получения качественного образования, общения, развития, но нельзя заменять реальную жизнь виртуальной. Необходимо регулировать и контролировать соотношение пребывания ребенка в реальной и цифровой среде. Как справедливо отмечается в литературе, что именно «объективные свойства цифровой среды – анонимность, невидимость и опосредованность взаимодействия – усиливают склонность к девиантным и деструктивным формам поведения»[58]. Специфика виртуального общения такова, что позволяет безнаказанно совершать девиантные поступки и уходить от ответственности, отсутствие моральных норм и принципов взаимодействия в сети снимает всю ответственность с личности за агрессию, обман, издевательства, оскорбления и т. д.

Усугубляется ситуация тем, что в отношении большинства несовершеннолетних отсутствует контроль и надзор за их «виртуальным» общением, потребляемым контентом, временем, проведенным в сети «Интернет». Дети проводят в сети большую часть своего времени, общаясь и взаимодействуя с другими лицами и группами, получая информацию, не всегда позитивно влияющую на их развитие, вступая в группы и сообщества. Неконтролируемая среда общения, развития, формирования личности ребенка создает серьезные угрозы его безопасности не только информационной, но психологической и физической. На этом фоне в научной среде появился термин «цифровая беспризорность», которая и приводит к девиантному поведению подростков. «Именно состояние цифровой беспризорности приводит к обращению к контенту противоправного характера»[59]. Отсутствие адекватного контроля и надзора за пребыванием ребенка в виртуальной среде создает благоприятные условия как для процесса криминализации личности, так и ее виктимизации. Институт статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ изучил, насколько включены в процессы цифровизации современные дети, и как эту включенность пытаются контролировать их родители. «В целом две трети взрослых интернет-пользователей (от 18 лет) считают необходимым до определенного возраста детей контролировать время, которое они проводят в сети. Почти половине взрослых такой контроль представляется обоснованным только в отношении дошкольников и младших школьников; 20 % готовы его устанавливать до 14 лет, еще меньше (8 %) – вплоть до совершеннолетия ребенка»[60]. Таким образом, мы видим, что большинство опрошенных не готовы контролировать время, проведенное в сети детьми старше 14 лет. Но именно несовершеннолетние этой возрастной группы наиболее подвержены процессу вовлечения их в преступную деятельность, а также обладают повышенной виктимностью, особенно по преступлениям против собственности, так как у многих из них есть карты, сбережения, накопления.

К субъективным факторам повышенной уязвимости несовершеннолетних в сфере криминализации и кибервиктимизации относятся социально-психологические особенности данной возрастной группы. Для несовершеннолетних характерны такие качества, как эмоциональная неустойчивость, повышенная внушаемость и слабо выраженные волевые качества, импульсивность и вспыльчивость, стремление к независимости и недостаточная сформированность критического мышления, неуверенность в себе и стремление к рискованному поведению. Эти качества делают подростков легкой добычей для преступников, использующих несовершеннолетних как орудие своих преступлений. Информационные технологии позволяют легко находить потенциальных жертв и, используя знания психологии и социологии, манипулировать подростками в целях вовлечения их в преступную деятельность. Объединяя их в группы и сообщества, криминальные структуры формируют взгляды и убеждения, новые правила и формы общения, преследуя деструктивные цели. Следует отметить, что именно в это время складываются устойчивые формы поведения, черты характера и способы эмоционального реагирования, которые в дальнейшем во многом определяют жизнь взрослого человека, его физическое и психическое здоровье, общественную и личную зрелость. От того, кто и как оказывает влияние на формирование личности ребенка, зависит и наше будущее. К сожалению, следует признать, что сегодня определяющая роль в процессе социализации личности принадлежит Интернету. Виртуальное пространство формирует среду, в которой проводит большую часть времени подросток.

Представляется, что необходимо принимать меры, направленные на контроль и ограничение виртуальных сфер и контентов, негативно влияющих на формирование личности несовершеннолетнего. Более того, необходимо ограничивать время, которое проводит подросток в виртуальном

[58] Дадаева Т. М., Ларихина Т. В. Отношение молодежи к деструктивным практикам в цифровом пространстве // Society and Security Insights. 2022. № 5 (4). С. 108–125.

[59] Воронин М. Ю. Цифровая беспризорность: проблема глобального современного общества // Вестник МГЛУ. Образование и педагогические науки. 2021. Вып. 1 (838). С. 261.

[60] Дети в Интернете [Электронный ресурс] // Институт статистических исследований и экономики знаний : [сайт]. URL: https://issek.hse.ru/news/837320649.html (дата обращения: 20.04.2026).

пространстве. Несовершеннолетние должны быть ограничены как в количественных показателях использования информационных ресурсов, так и в качественных, связанных с содержательной частью контента. Поэтому ограничения должны носить и технический, и организационный, и правовой характер. Эти меры должны быть направлены на нейтрализацию факторов, влияющих на «цифровую беспризорность» несовершеннолетних.

Л. А. Кротова,
канд. юрид. наук, доцент, доцент кафедры уголовного права и криминологии
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

К вопросу об информации как конструктивном признаке преступлений в сфере экономической деятельности

В современном мире практически невозможно найти сферу жизнедеятельности общества, которая не была бы связана с информационными ресурсами. Не является исключением и экономическое пространство, где соответствующие ресурсы все более активно участвуют в процессах экономического взаимодействия между людьми, и их значение постоянно возрастает, свидетельством чего служит появление в главе 22 уголовного закона новых составов преступлений, где информация (сведения, данные) предусматриваются в качестве конструктивных признаков.

Еще в начале текущего века в науке уголовного права совершенно справедливо были поставлены вопросы, во-первых, об ограниченности подхода к характеристике информационных преступлений как противоправных деяний исключительно в области компьютерной информации (киберпреступления) и, во-вторых, о настоятельности «формулирования нового направления в развитии уголовно-правовых средств обеспечения защиты сферы экономической деятельности от информационных посягательств»[61]. Более того, был предложен вариант доктринального определения понятия преступления информационного характера в сфере экономики как «виновно совершенное информационными или материальными способами общественно опасное деяние (бездействие), направленное на информационную составляющую экономической деятельности»[62].

Информация, будучи компонентом содержания составов преступлений, предусмотренных главой 22 УК РФ, выступает в качестве объективных признаков, однако базовой для ее характеристики служит дефиниция, сформулированная законодателем в источниках информационного права как самостоятельной отрасли, а именно «сведения (сообщения, данные) независимо от формы их представления»[63].

Относительно уголовно-правовой охраны общественных отношений, так или иначе связанных с использованием данного феномена, высказано мнение о необходимости конкретизации природы этих данных путем указания на правовое регулирование их оборота. Тем самым, как полагают авторы, обращаясь к Модельному закону «Об информатизации, информации и защите информации»[64], можно было бы приблизиться к формулировке универсального правового понятия информации, единого для всех отраслей[65].

Однако возможность практической реализации поставленной задачи вызывает сомнение, причем даже в пределах уголовно-правовой отрасли, не говоря уже о системе российского права в целом.

---

[61] Турышев А. А. Информация как признак преступлений в сфере экономической деятельности : автореф. дис. … канд. юрид. наук. Омск, 2006. С. 6.

[62] Турышев А. А. Указ. соч. С. 6.

[63] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2025) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 20.04.2026). Далее – ФЗ РФ от 27.07.2006 № 149-ФЗ.

[64] Модельный закон «Об информатизации, информации и защите информации», принят на двадцать шестом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (постановление № 26-7 от 18 ноября 2005 г.) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 05.04.2026). Согласно ст. 2 данного закона под информацией надлежит понимать «сведения или данные, порядок использования которых, независимо от способа их представления, хранения или организации, подлежит правовому регулированию в соответствии с настоящим Законом и иными национальными законами».

[65] Стяжкина С. А. Информация как объект уголовно-правовой охраны: понятие, признаки, виды // Вестник Удмуртского университета. Серия «Экономика и право». 2015. Т. 25, вып. 2. С. 158.

В указанном выше Модельном законе информация регламентируется лишь в одном аспекте (как объект правового регулирования), в то время как в уголовном законодательстве ее правовое значение определяется иначе. Информация в нормах УК РФ «представлена составной частью такого элемента состава преступления, как объект, то есть является предметом преступления, а также факультативным признаком объективной стороны как средства совершения преступления»[66]. Следовательно, признак наличия правового регулирования оборота информации характерен лишь для определенного вида информации как структурного элемента составов преступлений в сфере экономической деятельности, т. е. не обладает универсальностью даже в рамках главы 22 УК РФ.

Таким образом, именно «слишком общее определение» информации как «сведения (сообщения, данные) независимо от формы их представления» (ст. 2 ФЗ РФ от 27.07.2006 № 149-ФЗ) следует признать не только достаточным для целей в том числе и уголовного права, но и наиболее результативным. Факт отсутствия единого легального определения этого термина в рамках уголовного законодательства вряд ли можно рассматривать как проблему, требующую ответствующего решения.

В то же время в научных исследованиях информационный компонент зачастую рассматривается в качестве объекта уголовно-правовой охраны, с чем не представляется возможным согласиться. Во многом такая позиция имеет законодательное обоснование, поскольку ст. 5 ФЗ РФ от 27.07.2006 № 149-ФЗ определяет информацию именно как объект правовых отношений. Однако в доктрине справедливо указывается на «недопустимость смешивания понятий «объект преступления» в уголовном праве и «информационный объект» в информационном праве, поскольку для уголовного права в качестве объекта преступления признается то, на что преступление направлено и чему причиняет или может причинить вред»[67].

Поддерживая наиболее представительный по числу сторонников подход к трактовке понятия объекта преступления как общественных отношений (интересов), охраняемых уголовным законом, информация, будучи конструктивным признаком, связанным с указанным элементом, представляет собой предмет преступления, воздействуя на который, причиняется вред общественным отношениям (благам, интересам), либо создается угроза такового.

Правовое понятие «информация» определяется законодателем с использованием терминов «данные», «сведения». Несмотря на формальное их соотношение как общего (информация) и частного (данные, сведения), вряд ли в содержательном отношении между ними имеют место существенные различия. Причем в нормативных актах конкретных отраслей права в равной мере задействованы все три термина как взаимозаменяемые. В связи с этим не представляются убедительными доводы о необходимости унификации уголовного законодательства путем использования единого термина «информация» на том основании, что именно он присутствует «в законодательстве иных отраслей права, которое зачастую составляет бланкетное содержание уголовно-правовых норм»[68].

Функциональная роль информации в конструкции различных составов преступлений не одинакова. Она может быть представлена в качестве предмета, орудия, средства, способа совершения преступлений, в связи с чем формирование единого понятия информации для целей уголовного права представляется затруднительным и, кроме того, весьма сомнительным в плане практического значения.

Предмет как самостоятельный признак преступлений в сфере экономической деятельности предусмотрен в следующих составах: фальсификация Единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета (ст. 170.1 УК РФ); внесение заведомо ложных сведений в межевой план, технический план, акт обследования, проект межевания земельного участка или земельных участков либо карту-план территории (ст. 170.2 УК РФ); злостное уклонение от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах (ст. 185.1 УК РФ); незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ); неправомерное использование инсайдерской информации (ст. 185.6 УК РФ); неправомерные действия при банкротстве (ст. 195 УК РФ).

---

[66] Яшков С. А. Информация как предмет преступления : автореф. дис. … канд. юрид. наук. Екатеринбург, 2005. С. 20; Коняхин В. П., Арсланов Р. Г. Информация как предмет и средство совершения преступлений в сфере экономической деятельности [Электронный ресурс] // Российский следователь. 2016. № 8. Режим доступа: СПС «КонсультантПлюс» (дата обращения: 20.04.2026); и др.

[67] Елин В. М. Уголовно-правовая охрана некоторых категорий информации ограниченного доступа : монография [Электронный ресурс]. М. : Академия сферы социальных отношений, 2010. С. 26. URL: https://www.hse.ru/data/ (дата обращения: 20.04.2026).

[68] Коняхин В. П., Арсланов Р. Г. Указ. соч.

Информация, представленная в каждом из данных составов преступлений в этом качестве, характеризуется различными свойствами, что обусловлено особенностями регулятивных отношений, охраняемых в рамках главы 22 УК РФ. Это информация как с ограниченным доступом, т. е. сведения, составляющие коммерческую, налоговую, банковскую тайну, а также иную конфиденциальную информацию[69] (инсайдерскую), так и не нуждающаяся в защите на законодательном уровне (например: данные для внесения в единый государственный реестр юридических лиц – ст. 170.1 УК РФ; сведения об имуществе, о его размерах, местонахождении либо иной информации об имуществе, имущественных правах или имущественных обязанностях – ч. 1 ст. 195 УК РФ).

Информация в сфере экономической деятельности, в силу взаимосвязи с объектом уголовно-правовой охраны, информация может быть исключительно достоверной и документированной, т. е. зафиксированной «на материальном носителе путем документирования информации с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель»[70].

С учетом документированного характера информации как конструктивной составляющей рассматриваемых составов вызывает возражения позиция исследователей, утверждающих, что «к предмету преступления, предусмотренного ст. 170.1 УК РФ, относятся: анкета зарегистрированного лица, передаточное распоряжение, залоговое распоряжение, документы, которые зарегистрированные лица обязаны передать регистратору… »[71] и др. Ценностью, как необходимым свойством предмета, обладает не материальный носитель (журналы, выписки, анкеты и др.), а содержащиеся в нем сведения. Именно таковые следует рассматривать в качестве самостоятельного структурного компонента составов преступлений в сфере экономической деятельности.

Информация как средство совершения преступления представлена в ряде составов преступлений главы 22 уголовного закона: регистрация незаконных сделок с землей (ст. 170 УК РФ); фальсификация финансовых документов учета и отчетности финансовой организации УК РФ (ст. 172.1 УК РФ); невнесение в финансовые документы учета и отчетности кредитной организации сведений о размещенных физическими лицами и индивидуальными предпринимателями денежных средствах (ст. 172.3 УК РФ); незаконное осуществление деятельности по возврату просроченной задолженности физических лиц (ст. 172.4 УК РФ); организация деятельности по представлению в налоговые органы Российской Федерации и (или) сбыту заведомо подложных счетов-фактур и (или) налоговых деклараций (расчетов) (ст. 173.3 УК РФ); незаконное получение кредита (ст. 176 УК РФ); принуждение к совершению сделки или к отказу от ее совершения (ст. 179 УК РФ); злоупотребления при эмиссии ценных бумаг (ст. 185 УК РФ); манипулирование рынком (ст. 185.3 УК РФ); фальсификация решения общего собрания акционеров (участников) хозяйственного общества или решения совета директоров (наблюдательного совета) хозяйственного общества (ст. 185.5 УК РФ); совершение валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов (ст. 193.1 УК РФ); уклонение от уплаты налогов и (или) сборов с физического лица (ст. 198 УК РФ); уклонение от уплаты налогов и (или) сборов с организации (ст. 199 УК РФ); уклонение страхователя – физического лица от уплаты страховых взносов на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний в государственный внебюджетный фонд (ст. 199.3 УК РФ); уклонение страхователя-организации от уплаты страховых взносов на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний в государственный внебюджетный фонд (ст. 199.4 УК РФ).

Особенность информации как средства совершения большей части преступлений, предусмотренных главой 22 УК РФ, – ее несоответствие действительности. В конкретных составах соответствующих преступлений данное свойство информации определяется путем использования различных понятий:

– заведомо ложные сведения;
– заведомо недостоверные сведения;

---

[69] В ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ дано понятие «конфиденциальности информации» как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя». Конкретные виды таких сведений предусмотрены в Указе Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 20.04.2026); и др.

[70] П. 11 ст. 2 ФЗ РФ № 149-ФЗ.

[71] Сальников М. М. Уголовно-правовые и криминологические меры противодействия нарушениям прав владельцев ценных бумаг : автореф. дис. … канд. юрид. наук. М., 2014. С. 9.

– заведомо неполные сведения;

– умышленно искаженные сведения;

– заведомо подложные счета-фактуры, налоговые декларации (расчеты), что наглядно представлено в таблице 1.

Таблица 1

Информация, не соответствующая действительности				
Заведомо ложные сведения	Заведомо недостоверные сведения	Заведомо неполные сведения	Умышленно искаженные сведения	Заведомо подложные счета-фактуры, налоговые декларации (расчеты)
Ст. 172.4, 176, 185.3, 198, 199	Ст. 172.1, 185, 185.5, 193.1, 199.3, 199.4	Ст. 172.1	Ст. 170	Ст. 173.3

Проблема соотношения ложных и недостоверных сведений как элементов структуры составов преступлений актуальна не только применительно к охране отношений в сфере экономической деятельности, но достаточно широко обсуждается и в рамках других уголовно-правовых институтов. Следует отметить отсутствие единообразного подхода к его решению. Так, А. Шеслер, давая оценку введению специальных составов мошенничества в УК РФ, пришел к выводу, что «ложные и недостоверные сведения, о которых речь идет в ч. 1 ст. 159.1 УК РФ, – это одно и тоже… »[72].

Другие авторы, принимая во внимание аргументацию, приводимую судами по ряду уголовных дел, считают необходимым разграничивать эти понятия[73]. Так, согласно разъяснениям, сделанным для целей ст. 207.1 и 207.2. УК РФ, под «заведомо ложной информацией следует понимать такую информацию (сведения, сообщения, данные и т. п.), которая изначально не соответствует действительности, о чем достоверно было известно лицу, ее распространявшему. О придании ложной информации вида достоверной могут свидетельствовать, например, формы, способы ее изложения (ссылки на компетентные источники, высказывания публичных лиц и пр.), использование поддельных документов, видео- и аудиозаписей либо документов и записей, имеющих отношение к другим событиям»[74].

Безусловно, приведенные выше позиции суда не решают в полной мере проблему соотношения указанных выше понятий, обозначающих такой конструктивный признак состава преступления, как средство его совершения. В определенной степени рассматриваемые понятия синонимичны, что обуславливает целесообразность постановки вопроса об унификации уголовного законодательства с тем, чтобы максимально минимизировать используемую терминологию для обозначения общего понятия «информация-средство» применительно к преступлениям в сфере экономической деятельности как в целях упрощения диспозиций норм главы 22 УК РФ, так и оптимизации судебной практики.

[72] Шеслер А. Мошенничество: проблемы реализации законодательных новелл // Уголовное право. 2013. № 2. С. 70.

[73] Федченко А. В. Заведомо ложные и недостоверные сведения в мошенничестве в сфере кредитования [Электронный ресурс] // Актуальные вопросы юриспруденции : сб. науч. тр. по итогам междунар. науч.-практ. конф. Екатеринбург, 2017. № 4. URL: https://izron.ru/articles/ (дата обращения: 20.04.2026); Балекина В. М. Понятие заведомо недостоверной информации, распространяемой под видом достоверных сообщений в праве // Административное и муниципальное право. 2022. № 2. URL: https://www.nbpublish.com/library (дата обращения: 20.04.2026); и др.

[74] Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2 (утв. Президиумом ВС РФ 30 апреля 2020 г.) // Бюллетень Верховного Суда РФ. 2020. № 6. С. 13.

Аналогичное разъяснение дано правоохранительными органами для целей ст. 159.1 УК РФ. См.: Прокурор разъясняет. Управление по надзору за уголовно-процессуальной и оперативно-розыскной деятельностью разъясняет ответственность за мошенничество в сфере кредитования [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/web/proc_37/activity/legal-education/explain?item=24728973 (дата обращения: 20.04.2026).

А. А. Сметанин,
начальник КБ 794, ООО «ИРЗ»,
И. В. Багратионов,
обучающийся ФГБОУ ВО «Ижевский государственный технический университет имени М. Т. Калашникова»,
г. Ижевск

Методология безопасной разработки ПО для собственных нужд организации – субъекта КИИ

Многие субъекты КИИ разрабатывают программное обеспечение собственными силами, ошибочно полагая, что требования приказов ФСТЭК их не касаются, ведь продукт не продается, и, значит, сертификация не обязательна. Нередки случаи, когда служба информационной безопасности (ИБ) крупного предприятия, относящегося к КИИ, обнаруживает, что отдел автоматизации или АСУ ТП «для себя» написал несколько утилит или даже серьезных приложений, которые работают в промышленном контуре, но при этом (примеры ошибок):

– код хранится у программиста в личном репозитории на GitHub;
– используются непроверенные opensource библиотеки с неизвестными уязвимостями;
– отсутствует какая-либо документация по безопасности.

Согласно КоАП РФ (ст. 13.12–13.13) штрафы на юридических лиц за нарушение требований защиты информации могут достигать 300 000 рублей, не говоря уже о предписаниях о приостановке деятельности до устранения нарушений.

Однако требования ФСТЭК России в данном случае не отменяются, а трансформируются. Объектом контроля становится не сам программный продукт, а безопасность процессов его создания и последующей эксплуатации в составе аттестованной информационной системы. Задача разработчика – доказать регулятору, что создаваемое ПО не станет причиной проникновения злоумышленника в контур предприятия.

Основные шаги

Для выстраивания процессов безопасной разработки служат те же нормативные документы, что и для коммерческих вендоров, однако их применение имеет специфику, обусловленную статусом организации.

Нормативные документы и требования:

– приказ ФСТЭК № 239 (п. 29.3): Требования к оператору объекта КИИ по организации процессов создания и модификации ПО;

– ФЗ-187 «О безопасности критической информационной инфраструктуры (КИИ) РФ»: Основной закон в сфере безопасности КИИ;

– ГОСТ Р 56939-2024: Методологическая основа для построения внутренних процессов безопасной разработки;

– приказы ФСТЭК № 21, № 235: Требования к защищенности информационных систем, куда внедряется ваше ПО.

При анализе документов, касающихся разработки ПО для собственных нужд организаций, выделяются три основные задачи, которые нужно закрыть прежде, чем начинать производство:

1. Обеспечить защищенность кодовой базы (контроль доступа и хранения).
2. Гарантировать безопасность кода (отсутствие закладок и критических уязвимостей).
3. Выстроить безопасный процесс внедрения и эксплуатации (контроль целостности, регламенты обновления).

Внедрение безопасной разработки

Переход к регламентированной безопасной разработке целесообразно осуществлять поэтапно. Попытка внедрения без плана может привести к пустой трате времени и бюджета организации.

1. Аудит текущего состояния. Цель этапа: выявить разрывы между текущей практикой и требованиями ГОСТ Р 56939-2024.

В ходе аудита проверяются[75]:

– способы хранения исходного кода (корпоративные репозитории или папки на ноутбуках разработчиков);

[75] Баранова Е. К., Бабаш А. В., Баранова Е. Е. Информационная безопасность и защита информации : учеб. пособие. М. : ИНФРА-М, 2023. 322 с.

– используемые средства контроля версий;
– наличие и регулярность анализа кода на уязвимости;
– полнота документации (модели угроз, инструкции).

Результатом становится отчет с «дорожной картой» – перечнем недостающих процессов и планом их внедрения с указанием сроков и ответственных.

2. Организационное оформление документов.

Для ФСТЭК критически важно, чтобы процессы были не просто реализованы технически, но и формально утверждены. Без утвержденных документов регулятор может посчитать, что процессы работают «на общественных началах», а значит, ненадежно.

На данном этапе разрабатываются и утверждаются[76]:

– Политика безопасной разработки ПО – документ верхнего уровня, утверждаемый руководителем организации. Он декларирует, что компания намерена следовать принципам безопасной разработки.

– Руководство по безопасной разработке ПО – детальный документ, описывающий требования к среде разработки, процедуры анализа кода, порядок работы с библиотеками и управление учетными записями.

3. Техническое оснащение.

Разработка для КИИ считается важной частью процесса внедрения ПО, чтобы подтвердить безопасную разработку нужны документы (см. табл. 1)[77].

Таблица 1

Минимальные требования к техническому оснащению и подтверждающие документы

Направление	Техническая реализация	Подтверждающие документы
Выделенная инфраструктура	Серверы систем контроля версий (GitLab, Bitbucket) и репозитории артефактов (Nexus, Artifactory) размещаются в защищенном сегменте сети с ограниченным доступом	Схема сети с выделением сегмента разработки; политика управления доступом; журналы (логи) доступа к репозиториям
Усиленная аутентификация	Подключение к среде разработки – только по VPN с использованием двухфакторной аутентификации (токены, сертификаты)	Приказ (или иной распорядительный документ) об обязательном использовании VPN и 2FA; инструкция для разработчиков по подключению; журналы подключений
Антивирусная защита	Рабочие станции разработчиков оснащаются сертифицированными средствами защиты (СЗИ от НСД, антивирусы)	Акт установки/инвентаризации ПО; копии сертификатов ФСТЭК на используемые СЗИ; политика антивирусной защиты
Инструменты анализа	Внедрение систем статического анализа кода (SAST) и анализа состава ПО (SCA) с интеграцией в процесс сборки (CI/CD)	Протоколы (отчеты) статического анализа; реестр используемых библиотек (SBOM); документ, регламентирующий порядок проведения анализа (кто, когда, как проверяет, пороговые значения для остановки сборки)

4. Интеграция безопасности в процессы разработки (DevSecOps).

Для того, чтобы поддерживать безопасную разработку, следует придерживаться правил ShiftLeft (безопасность на ранних этапах разработки) и «Красной черты» (при обнаружении критической уязвимости SAST-анализатором сборка проекта останавливается, и код не может попасть на следующие стадии разработки)[78].

Следует следить за библиотеками. Для этого создаётся «белый список» разрешенных Open-source библиотек, по используемым версиям которых проводится мониторинг баз уязвимостей (CVE). Хранение проверенных версий библиотек.

---

[76] Подотыкин Н. Почему построение процессов РБПО превратилось из рекомендации в обязательное условие. CISO Club, 2025 [Электронный ресурс]. URL: https://cisoclub.ru/pochemu-postroenie-processov-rbpo-prevratilos-iz-rekomendacii-v-obyazatelnoe-uslovie/ (дата обращения: 15.03.2026).

[77] УЦСБ. Центр кибербезопасности УЦСБ и Атомик Софт: опыт внедрения безопасной разработки. 2024 [Электронный ресурс]. URL: https://ucsb.ru/press-center/news/tsentr-kiberbezopasnosti-utssb-i-atomik-soft-opyt-vnedreniya-bezopasnoy-razrabotki/ (дата обращения: 16.03.2026).

[78] Гатчин Ю. А. Теория информационной безопасности и методология защиты информации. СПб. : Университет ИТМО, 2022. 198 с.

5. Внедрение и эксплуатация.

Разработанное ПО внедряется в аттестованную информационную систему (АСУ ТП, ИСПДн и т. д.). Чтобы не нарушить аттестат, необходимо:

1) **Паспортизация портов.** Перед внедрением служба ИБ должна получить от разработчиков точную информацию: какие порты открывает приложение, какие протоколы использует, куда обращается.

2) **Выделенный контур.** Запрещено ставить новое ПО сразу в продуктовую среду. Обязательно развертывание на тестовом полигоне.

3) **Контроль целостности.** При передаче в эксплуатацию инсталляционный пакет должен передаваться с контрольной суммой (хэшем) или цифровой подписью. При каждой загрузке модуля должна проверяться его целостность.

4) **Регламент обновления.** Должна быть формальная процедура вывода новых версий. Если в коде найдена критическая уязвимость, разработчик обязан в установленный срок (например 72 часа) предоставить патч и протоколы его тестирования[79].

В результате проведенного исследования можно сделать вывод, что внедрение принципа безопасной разработки на предприятии КИИ поможет организации умело вкладывать ресурсы в проекты, избежать отставания в цифровизации производства и обрести гибкость ПО. Комплексный подход, описанный выше, позволяет превратить отдел разработки из источника потенциальных угроз в надежный оплот кибербезопасности предприятия.

Н. П. Шайхутдинова,

канд. юрид. наук, доцент, доцент кафедры экологического, трудового, административного права, основ права и российской государственности ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

Влияние цифровизации на занятость населения

В современных реалиях цифровизация постепенно проникает во все сферы жизни прогрессивного общества. Не является исключением также и сфера использования наемного труда. Ю. В. Иванчина и Е. А. Истомина в своей работе подчеркивают, что «цифровые технологии прямо влияют на возможности экономически активного населения работать и обеспечивать себе таким образом средства к существованию, на занятость населения, на уровень безработицы и, как следствие, на принципиальную необходимость социальной защиты и на ее количественные и качественные характеристики»[80].

Трансформация традиционных моделей социально-трудовых отношений происходит в результате влияния цифровой экономики на рабочие места и занятость в целом.

С появлением цифровизации порождаются новые профессии с использованием искусственного интеллекта (например дата-аналитики), меняются способы взаимодействия участников трудовых отношений (например дистанционная работа), а также появляются новые формы коммуникации в процессе труда (например удаленная работа посредством платформенной занятости). Правовые институты трудового права тоже претерпевают изменения с внедрением цифровых технологий, поскольку право не может игнорировать прогрессивные изменения. Но в то же время, имея социальную направленность правового регулирования, трудовое право должно обеспечить механизмы правовой защиты в условиях цифровизации путем создания баланса интересов участников трудовых отношений. Трудовое право, как социально-ориентированная отрасль права, может реализовать баланс интересов посредством ограничения возможности работодателей по эксплуатации технологий, угрожающих работникам, но при одновременной адаптации правовых норм для сохранения эффективности.

Одной из основных задач трудового законодательства в соответствии с частью 2 статьи 1 Трудового кодекса Российской Федерации[81] (далее – ТК РФ) предусмотрено создание необходимых правовых условий для достижения оптимального согласования интересов трех заинтересованных сторон

---

[79] Заярный Н. Безопасность по умолчанию: как подход Secure by Design меняет защиту АСУ ТП. IT Sec, 2025. URL: https://itsec.ru/articles/bezopasnost-po-umolchaniyu-kak-podhod-secure-by-design-menyaet-zashchitu-asu-tp (дата обращения: 18.03.2026).

[80] Иванчина Ю. В., Истомина Е. А. Цифровизация социально-трудовых отношений в изменяющемся мире: сравнительно-правовой анализ // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6, № 4 (24). С. 194.

[81] Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 29.12.2025, с изм. от 06.02.2026) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 05.04.2026).

в сфере труда, а именно: работника, работодателя и государства. Цифровизация сферы трудовых и непосредственно связанных с ними отношений налагает определенные особенности участия государства во взаимодействии работника и работодателя. Дальнейшее углубление цифровизации в сферу трудового права порождает необходимость введения дополнительных правовых норм в целях социальной защиты наиболее слабой стороны трудовых отношений – работника, а также государственной поддержки работодателей в новых условиях цифровой реальности.

Трудовое право не может не учитывать изменения в государственной политике, технике, технологии, но при этом не должно утратить и своего направления социальной защиты сторон трудовых отношений. Как вариант компромисса в условиях современных вызовов с углублением цифровизации является адаптация трудовых отношений к новым экономическим условиям. Таким образом, каждый социально-ориентированный правовой институт в системе трудового права может приобрести определенные ответные нормы в целях противодействия ущемлению прав сторон трудовых отношений и адаптации их в условиях цифровизации.

Цифровые технологии, проникая во все сферы жизни общества, широко представлены в том числе на рынке труда посредством цифровой организации трудовых процессов. Об этом свидетельствует появление цифровых торговых площадок, электронных офисов, платформенная занятость, замещение человеческого труда технологическими решениями с привлечением искусственного интеллекта, роботизация производства. При этом возрастает цифровая мобильность работников, способных выполнять трудовые функции вне стационарного рабочего места, в другой локации, в том числе за пределами офиса, конкретного населенного пункта или даже страны.

Цифровизация тесно связана с правовыми норами института занятости и трудоустройства, поскольку рынок труда трансформируется посредством цифровых технологий, но при этом темпы и направления цифрового развития определяются посредством уровня занятости населения. Но следует подчеркнуть неоднозначный характер влияния цифровизации на занятость населения.

Ключевые вызовы цифровизации для трудового права могут оказывать негативное влияние на сферу занятости, поскольку внедрение цифровых аналогов постепенно приводит к вытеснению с рынка труда части работников в результате автоматизации и оптимизации процессов при использовании цифровых технологий. Это приводит к изменению структуры занятости, поскольку автоматизация снижает спрос на ряд профессий, предусматривающих формализованные, повторяющиеся операции. Следует согласиться с позицией М. В. Поляковой в том, что «подобный феномен обуславливается тем, что автоматизация, в первую очередь, затрагивает наименее защищенные категории работников. Поэтому процесс может привести к поляризации рынка труда, когда растущий спрос на высококвалифицированных специалистов в условиях цифровизации вытесняет ряд традиционных профессий»[82].

Но, с другой стороны, внедрение цифровых технологий требует создания новых рабочих мест, особенно в сфере информационно-коммуникационных технологий и в секторе услуг. При этом возникают новые виды деятельности, для которых необходимо освоение работниками новых компетенций для решения сложных, творческих вопросов, умение быстро адаптироваться и осваивать новые знания. Приобретение новых цифровых навыков и способностей работать с информацией в цифровой среде возможно в результате дополнительного профессионального образования и профессиональной переподготовки. Отсутствие баланса в цифровом развитии разных сфер экономики и регионов затрудняет своевременное овладение работниками необходимыми знаниями и навыками, что также приводит к угрозе структурной безработицы и, как следствие, социального неравенства. Отсутствие необходимых знаний у работодателей в условиях цифровизации также не позволяет им оперативно внедрять современные цифровые технологические процессы и модели организации труда. В таких условиях особую роль приобретают меры государственного регулирования на рынке труда. Особое значение приобретает адаптация трудового законодательства при регулировании цифровых форм занятости и внедрении механизмов социальной защиты работников. Внесение соответствующих изменений в нормы трудового права будет способствовать более эффективному внедрению цифровых технологий в сферу наемного труда.

Прежде всего, речь идет об организации системы первоначального обучения работников или их переобучения по освоению навыков работы с различными формами цифровой информации. Формы, стадии, форматы обучения и переобучения могут зависеть от уровня обучающихся, целевой направленности деятельности работодателя, а также его технической возможности. Различные формы обучения могут быть организованы на стадии поиска подходящей работы гражданами, зарегистрированными в органах службы занятости в качестве ищущих работу или безработных граждан. В данном

[82] Полякова М. В. Влияние цифровой трансформации на рынок труда в Российской Федерации // Прогрессивная экономика. 2025. № 5. С. 268.

случае необходима финансовая поддержка со стороны государства для возможного внедрения программ первоначального обучения или переобучения. Для лиц, обладающих определенным базисом первоначальных знаний по использованию цифровой информации, возможна организация переобучения или профессиональной переподготовки, что позволит обучить квалифицированные трудовые ресурсы в более короткие сроки. Работодателям, заинтересованным в применении цифровых технологий, также целесообразно организовать обучение или переобучение своих работников или лиц, вновь поступающих на работу, в различных организационных формах ученичества посредством заключения ученического договора в соответствии с главой 32 ТК РФ. Программы обучения для каждого работодателя должны быть составлены в соответствии с потребностями его уставной деятельности, а также с учетом общих требований законодательства по защите информации. Действующее трудовое законодательство предусматривает различные формы ученичества, в том числе в форме бригадного, индивидуального и курсового обучения, каждая из которых может быть применена работодателем в рамках ученического договора при передаче знаний для осуществления деятельности с применением цифровых технологий. Обучение также может проводиться в форме наставничества в соответствии со статьей 351.8 ТК РФ и в рамках действия Концепции развития наставничества в Российской Федерации на период до 2030 года и плана мероприятий по ее реализации[83].

В целях увеличения социальных гарантий работников целесообразно принятие правовых норм, сдерживающих темпы внедрения цифровых технологий, влекущих за собой высвобождение работников. В числе таких норм обязанность работодателя направлять работников на переобучение за счет собственных средств в случае замены их функциональных обязанностей искусственным интеллектом, а также обязанность принимать участие в последующем трудоустройстве этих работников. Аналогичную позицию, которую следует поддержать, изложила И. А. Филипова в своей работе[84].

Также участие первичной профсоюзной организации или иного представительного органа работников при внедрении в деятельность работодателя цифровых технологий, влияющих на правовое положение работников, позволит в большей степени защитить их социальные права. Так, законодательное требование установления процедур учета мнения представительного органа трудового коллектива, а в некоторых случаях получение его согласия может повлиять на беспрепятственную произвольную замену работников в случае создания новых роботизированных рабочих мест и, как следствие, избежать масштабного высвобождения работников.

Большинство вопросов, связанных с внедрением в деятельность работодателей цифровых технологий, могут найти отражение в рамках института социального партнерства, обеспечивая согласование интересов работодателей и работников по вопросам регулирования трудовых и иных непосредственно связанных с ними отношений. В зависимости от уровня социального партнёрства к решению вопросов цифровизации в сфере наемного труда могут быть привлечены органы государственной власти и органы местного самоуправления. Такой подход позволит в наибольшей степени положительно повлиять на социально-трудовые гарантии участников трудовых отношений и полностью соответствует принципам социального партнёрства, обеспечивая равноправие, уважение и учет интересов сторон, в соответствии со статьей 24 ТК РФ.

Следует заметить, что организация работодателем мероприятий по обучению и переобучению работников может явиться временной необходимостью, поскольку имеет место определенный переходный период внедрения цифровых технологий в сферу труда. В дальнейшем подготовка специалистов в соответствующей цифровой сфере деятельности преимущественно будет осуществляться образовательными организациями на различных уровнях. Свои требования в части наличия специальных необходимых знаний и навыков у работников работодатели с учетом видов профессиональной деятельности могут представить в проектах соответствующих профессиональных стандартов. Согласно пункту 2 Правил разработки и утверждения профессиональных стандартов «проекты профессиональных стандартов могут разрабатываться работодателями и их объединениями, профессиональными сообществами, научными, образовательными, саморегулируемыми и иными некоммерческими организациями»[85]. Таким образом, влияние цифровизации на занятость населения будет способствовать дальнейшей реализации производственных целей работодателя и одновременно стабильности трудовых отношений.

---

[83] Об утверждении Концепции развития наставничества в Российской Федерации на период до 2030 года и плана мероприятий по ее реализации : распоряжение Правительства РФ от 21.05.2025 № 1264-р [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 05.04.2026).

[84] Филипова И. А. Трудовое право: вызовы информационного общества // Право. Журнал высшей школы экономики. 2020. № 2. С. 174.

[85] Правила разработки и утверждения профессиональных стандартов, утверждены постановлением Правительства Российской Федерации от 10.04.2023 № 580 (ред. от 06.03.2026) // СПС «КонсультантПлюс» (дата обращения: 10.04.2026).

Е. В. Шевченко,
канд. юрид. наук, доцент кафедры гражданского права и процесса,
Северный институт (филиал) «ВГУЮ (РПА Минюста России)»,
К. С. Быченков,
обучающийся 3 курса, «Судебная и прокурорская деятельность»,
Северный институт (филиал) «ВГУЮ (РПА Минюста России)»,
г. Петрозаводск

Искусственный интеллект как инструмент обеспечения технологического суверенитета России

В последние годы искусственный интеллект перестал быть исключительно предметом научных исследований и футуристических прогнозов. Применение комплексных технологических решений связано с ростом объёмов информации, усложнением управленческих процессов и необходимостью принимать решения в условиях ограниченного времени. Российское государство не может игнорировать данный инструмент, способный повысить эффективность деятельности многих государственных институтов, и готово осуществлять всестороннюю комплексную поддержку развитию сложных технологий, выражающуюся в подготовке соответствующих кадров, созданию самостоятельной инфраструктуры, а также формированию законодательства, связанного с данной деятельностью.

Указанный процесс происходит поэтапно, и мы можем видеть, что начался он с использования искусственного интеллекта (далее – ИИ) в сфере экономики, поскольку позволяет быстро анализировать огромные объёмы данных и выявлять скрытые зависимости. С его помощью компании могут оценивать финансовые риски, прогнозируя спрос, улучшая логистику, управляя производством. А раз можно просчитать риски, значит, можно рассчитать, как снизить расходы, улучшить планирование и стать более конкурентоспособными. Особенно активно ИИ используют банки и финансовые организации для проверки платежей, оценки кредитоспособности и поиска подозрительных транзакций. Кредитный скоринг – термин, вошедший в жизнь кредитных организаций, представляет собой процесс финансовой оценки платежеспособности клиента, неважно физического или юридического лица, на основании его кредитной истории, финансовых возможностях и других объективных факторах. Такие же модели помогают банкам решать, какой продукт предпочтительнее, например: кредит или кредитная карта, кредитная линия и т. д.

В феврале 2024 г. Центробанк РФ разместил запрос котировок на выполнение работ по созданию системы роботизации бизнес-процессов с начальной ценой более 54 млн рублей. Из опубликованного техзадания следовало, что предметом работ была роботизация таких процессов, как рассмотрение обращений граждан и юридических лиц, а также поддержка потребителей финансовых услуг с применением ИИ.

И на сегодняшний день наш финансовый регулятор уже использует ИИ при ответах на обращения физических лиц, поступающих к нему в соответствии с Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»[86].

Кроме того, по словам главы ЦБ РФ Эльвиры Набиуллиной, продолжается разработка ИИ-помощника, который будет анализировать договоры на оказание финансовых услуг и излагать их суть человеку в доступной форме[87].

Тестирование этой технологии запланировано до конца первого квартала 2026 года не менее чем в 10 российских банках, и на этом этапе мы видим использование ИИ-технологий и в экономической, и уже в правовой сфере.

В начале января 2026 года Владимир Путин поручил разработать и утвердить национальный план по внедрению технологий ИИ в отраслях экономики, социальной сферы и государственном управлении на федеральном уровне и на уровне субъектов РФ, что позволит централизовано и при участии федеральных средств способствовать становлению государственного технологического суверенитета[88]. Здесь является значимым возможное создание и развитие отечественного программного

[86] Центральный банк РФ (ИИ для обработки обращений) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Проект:Центральный_банк_РФ_%28ИИ_для_обработки_обращений%29 (дата обращения: 10.02.2026).

[87] Там же.

[88] Национальная стратегия развития искусственного интеллекта [Электронный ресурс]. URL: https://www.tadviser.ru/index.php (дата обращения: 22.02.2026).

обеспечения для защиты данных и создания защищенных каналов связи, которое будет составлять основу национальных платформ с возможностью самодостаточной работы, т. е. такого жизненного цикла цифровых активов, которые не зависят от внешних технологий.

Кроме того, создание отечественного программного обеспечения неразрывно связано с темой поддержания информационной безопасности государства. Сегодня деятельность транснациональных корпораций, например, в виде кибератак направлена на возможность влиять на экономические и политические процессы, происходящие в разных странах, и, как следствие, уникальность тех или иных технологий и программ позволяют говорить о некоей защищенности хотя бы на какой-то период.

Создание автономной инфраструктуры направлено также на формирование технологического суверенитета, что, в свою очередь, требует развития образования, создания научных центров, поддержки грантов. Но помимо технологической и организационной стороны важно не забывать про нормативно-правовую составляющую данного процесса.

Реализация технологического суверенитета в рамках правового поля происходит в России через формирование и поддержку соответствующих национальных проектов, которые определяются на основании поручений по реализации Посланий Президента Федеральному Собранию. Например, национальный проект «Экономика данных и цифровая трансформация государства» (рассчитан на период с 2025 до 2030 годов) направлен на формирование цифровых платформ во всех основополагающих отраслях экономики, социальной сферы и в сфере государственного правления[89]. После определения приоритетов начинается правовая работа Правительства РФ, которое утверждает порядок поддержки и развития конкретных проектов. Например, распоряжением Правительства РФ от 20 мая 2023 года № 1315-р утверждена Концепция технологического развития на период до 2030 года, в которой упор делается на развитие сферы высокотехнологичных отраслей экономики России посредством разработки и реализации государственных программ на всех уровнях от федерального до муниципального при участии государственных корпораций, акционерных обществ и банковского капитала[90].

Важную роль, на наш взгляд, играет и доработка, а может и пересмотр тех нормативно-правовых актов, которые относятся к исследуемой сфере. Например, Федеральный закон РФ от 23 августа 1996 г. № 127-ФЗ «О науке и государственной научно-технической политике» содержит устаревшие определения, излишнюю декларативность и, как следствие, выглядит морально устаревшим и требующим внесения изменений[91].

Поскольку сфера интересов авторов лежит в юриспруденции, использование ИИ в данной сфере представляется подлежащей детальному изучению. Современные правовые системы характеризуются большим объемом нормативных актов и судебной практики, что затрудняет их анализ. Использование интеллектуальных программ позволяет автоматизировать поиск судебных решений, систематизировать нормы права и ускорить подготовку процессуальных документов. В результате повышается оперативность рассмотрения дел и обеспечивается единообразное применение законодательства.

Вместе с тем, как в случае использования ИИ при подготовке ответов на обращения граждан Центробанком РФ, возникает риск подмены профессиональной юридической оценки и системного толкования норм права не участниками судебных процессов и судьями, выносящими решения, а ИИ. Похожие прецеденты уже существуют, например, чат-боты на базе искусственного интеллекта – генерируют нужный текст в зависимости от запроса и не дают достоверный ответ со ссылками на источники информации[92].

Кроме того, элементы искусственного интеллекта применяются в деятельности правоохранительных органов. Область использования ИИ в данной сфере приводит к выявлению повторяющихся схем преступлений, анализу и обработке доказательств, а также для анализа общей информации о видах преступлений, что позволяет повысить эффективность расследований и рационально распределять ресурсы. Однако главной проблемой здесь остается, что данная деятельность напрямую связана с соблюдением прав и свобод человека и гражданина, следовательно, любое нарушение конфиденциальности в деятельности правоохранительных органов может привести к утечке информации,

[89] Национальный проект «Экономика данных и цифровая трансформация государства» [Электронный ресурс]. URL: http://government.ru/rugovclassifier/923/about/ (дата обращения: 20.02.2026).

[90] Об утверждении Концепции технологического развития на период до 2030 года : распоряжение Правительства РФ от 20 мая 2023 года № 1315-р [Электронный ресурс]. URL: http://publication.pravo.gov.ru/document/0001202305250050 (дата обращения: 20.02.2026).

[91] О науке и государственной научно-технической политике : Федеральный закон РФ от 23 августа 1996 г. № 127-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_11507 (дата обращения: 20.02.2026).

[92] Решение Арбитражного суда Самарской области от 19.05.2025 по делу № А55-28080/2024 [Электронный ресурс]. URL: https://www.zakonrf.info/arbsud/doc-e3b3e3ed-4f51-5a5f-9e3c-81233bbe1a93/ (дата обращения: 20.02.2026).

которая при незаконном использовании приведет не к виртуальным, а реальным человеческим потерям и, следовательно, подрыву общественного доверия к использованию ИИ государством.

Следовательно, требуется нормативное регулирование использования технологий ИИ в судебной деятельности, деятельности правоохранительных органов. Применение общих норм права либо аналогии права, равно как и распространение экспериментальных режимов на данную деятельность государства, не возможно. Здесь необходимо принятие адресных нормативных правовых актов.

Таким образом, можно выделить ряд проблем, с которыми мы сталкиваемся при использовании технологий ИИ в описываемой сфере на современном этапе. Во-первых, отсутствие самодостаточных цепочек полного цикла для создания единых профильных технологических платформ с учетом направления специфики той области, в которой идет применение ИИ, замедляет процесс его внедрения на уровне государственно значимых сфер. Во-вторых, отсутствие системной нормативной базы стандартов применения ИИ тормозит процесс его правового регулирования, а также негативно сказывается на формировании российского технологического суверенитета.

Вместе с тем искусственный интеллект способствует ускорению процессов, повышению качества анализа и снижению нагрузки на специалистов, что является инструментом повышения эффективности в экономике и правоприменении государства. Однако максимальный эффект возможен лишь в рамках четкого правового регулирования и создания полного цикла, обеспечивающего научно-техническую безопасность. При этом на сегодняшний день приоритетным является уже не создание разрозненных программ с ИИ, подконтрольных тем или иным лицам, организациям, органам власти, а создание единых национальных платформ, обеспечивающих высокий уровень научно-технической безопасности соответствующего направления деятельности российского государства, которое как внутри страны, так и во внешних отношениях связывали бы со становлением государственного технологического суверенитета.

Е. В. Соломатова,
старший преподаватель кафедры информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Правовое регулирование больших данных (сравнительный анализ опыта зарубежных стран и России)

Одной из актуальных проблем правового регулирования современных сквозных цифровых технологий, стоящей не только перед РФ, но и перед зарубежным законодателем и мировым правовым сообществом в целом, исследователи называют выработку релевантной модели нормативного правового регулирования общественных отношений, возникающих в связи с функционированием технологий больших данных (далее – БД). Следует отметить, что, несмотря на их активное применение как в сфере государственного и муниципального управления, так и в коммерческом секторе, само понятие БД не получило унифицированного доктринального либо нормативного закрепления. Проведенное исследование позволяет заключить, что наиболее развитые экономики мира выработали определенные подходы к правовому регулированию применения вышеназванных технологий, представляющие наибольший интерес с позиции возможности диффузии норм зарубежного права в отечественную практику. По нашему мнению, внимания заслуживают подходы к правовому регулированию ЕС, США и КНР, как носителей существенно отличающихся ценностных ориентиров.

Рассматривая правовую политику ЕС в области регулирования технологий больших данных, в первую очередь стоит отметить подход законодателя к расширению толкования понятия персональные данные и включение в них больших данных. Исходя из расширенного толкования понятия персональных данных, закрепленных в Регламенте по защите персональных данных (далее – Регламент, GDPR[93]), к ним относятся данные онлайн-идентификаторов, IP-адреса, геолокации и т. п., а также показатели физической, физиологической, умственной, генетической, социальной или иной идентичности человека. Регламент по защите персональных данных рассматривает большие данные именно с позиции максимально широкого подхода к трактованию персональных данных, предусматривая

[93] Регламент по защите персональных данных – General Data Protection Regulation [Электронный ресурс]. URL: https://gdpr-info.eu/ (дата обращения: 18.11.2025).

возможность применения льготного режима обработки обезличенных данных при обеспечении защиты пользователей и наложение санкций за нарушения режима их правомерного использования. Политика ЕС в отношении правового регулирования характеризуется последовательностью регламентации и распространяется на сбор, обработку, обезличивание, использование и уничтожение данных. Агрегация данных строится на принципах законности, справедливости и прозрачности; ограничения цели и минимизации данных, точности, целостности и конфиденциальности, а также ограничения хранения. GDPR также предполагает создание специализированного надзорного органа – Европейского совета по защите данных (EDPB[94]), обеспечивающего единообразие правовой политики в сфере оборота данных, как персональных, так и больших, и централизованный контроль за применением Регламента. Кроме того, GDPR предусматривает реализацию принципа экстерриториальности норм[95].

Таким образом, несмотря на то, что Регламент по защите персональных данных лишь косвенно, в силу широкого трактования понятия персональных данных, относится к большим данным, фактически он устанавливает правовые нормы, применимые к их обороту. Исследователи отмечают, что такой методичный риск-ориентированный подход к правовому регулированию технологий больших данных, потенциально влекущий введение жестких ограничений, способен снизить динамику экономического развития и отрасли, и ЕС в целом.

Относительно модели правовой политики США в области регулирования технологий больших данных можно заключить, что, невзирая на лидирующие позиции Америки в сфере цифровых технологий, унифицированного подхода к регламентации больших данных она не имеет. Так, нормы, регламентирующие правомерное применение технологий больших данных, закреплены в разнородных нормативных правовых актах[96] (далее – НПА). Кроме того, в США нет федерального органа исполнительной власти, уполномоченного в области нормотворческой деятельности в сфере оборота как персональных, так и больших данных, контролирующего органа в указанных сферах, а отдельные полномочия в данной сфере возложены на Федеральную торговую комиссию (далее – ФТС). В качестве причин отсутствия системного регулирования агрегации больших данных и оборота персональных данных исследователи называют активную лоббистскую деятельность крупных компаний-агрегаторов данных, препятствующих введению жестких ограничений в отношении оборота данных; рассмотрение больших данных, равно как и персональных данных, с позиции реализации права на неприкосновенность частной жизни детерминированное прецедентным характером формирования правоприменительной практики; мотивация ФТС заинтересованности операторов к детализированному саморегулированию правил конфиденциальности.

Многие исследователи отмечают, что американская модель охраны данных, рассматривающая конфиденциальность с позиции товара, закономерно влечет возникновение затруднений для потребителей, создавая множество правил, не позволяющих субъекту обработки данных иметь исчерпывающее представление о способах сбора, обработки и хранения его персонифицированной информации. Вышеизложенное позволяет заключить, что американское правовое регулирование отличается значительной диспозитивностью, оставляя решение многих вопросов в указанной сфере на усмотрение субъектам федерации и хозяйствующим субъектам. Такой подход, создавая комфортные условия для развития бизнеса и внедрения передовых технологий, таит определенные угрозы, обусловленные смещением баланса интересов в сторону бизнеса, и требуя от потребителей высокого уровня правовой и технической грамотности.

Заслуживает внимания и концепция Китая в области обработки больших данных, детерминированная особенностями китайской модели государственного управления. Показательным, на наш взгляд, является признание данных, генерирование которых осуществляется на территории КНР, национальным достоянием наравне с землей, капиталом, технологиями, что свидетельствует о признании экономической ценности больших данных на государственном уровне, а их агрегирование – новой отраслью народного хозяйства.

Несмотря на отсутствие специализированного закона, регулирующего правоотношения, возникающие при агрегации больших данных, специалисты заключают, что отправной точкой в построении китайской системы правовой регламентации технологии больших данных явился Закон

[94] Европейский совет по защите данных – European Data Protection Board.

[95] После вступления в силу GDPR в адрес американских компаний Google и Facebook в связи с наличием принудительного соглашения, противоречащего нормам Регламента, были предъявлены исковые требования на общую сумму 7,6 млрд евро.

[96] Закон о точной отчетности по кредитам (FCRA); Закон о конфиденциальности электронных коммуникаций (ECPA); Закон о компьютерном мошенничестве и злоупотреблениях (CFAA); Закон о мобильности и подотчетности медицинского страхования (HIPAA); Закон о финансовой модернизации (Financial Service Modernization Act) и др.

о кибербезопасности КНР[97], фиксирующий государственную политику в сфере защиты персонализированных данных. Данный закон содержит директиву осуществлять хранение данных эндемичных пользователей на территории КНР и рассматривает возможность утечки информации о таких пользователях в качестве угрозы национальной безопасности. Следующим этапом исследователи выделяют принятие Закона о защите личной информации[98], признаваемого первым НПА, всесторонне регламентирующим вопросы защиты данных и обеспечения режима их конфиденциальности. Правовые нормы сфокусированы на противодействии неправомерному использованию данных, взломам хранилищ и утечке персонифицированных данных, включая и их обработку с применением технологий больших данных. Очередной этап выстраивания модели правовой политики Китая ученые связывают с вступлением в силу Закона о безопасности данных[99] (далее – DSL), закрепившего понятие данных и установившего стадии их обработки. Защита данных признается задачей государственной власти и строится исходя из значимости данных и степени ущерба, который может быть нанесен государству при распространении указанных данных. Принципиально значимыми положениями DSL, на наш взгляд, можно назвать запрет трансграничной передачи персональных данных и ключевых данных, а также легализацию торговли данными, послужившую триггером для развития бирж данных. Также стоит отметить и развитие в КНР деятельности, направленной на защиту национальной безопасности и частноправовых интересов, регулирование экспорта данных, защиту прав и законных интересов субъектов личной (персональной) информации[100]. Вместе с тем регулирование оборота данных в Китае осуществляет ряд государственных органов – Национальное управление данными, Национальная комиссия по развитию и реформам Государственного совета КНР, Управление кибербезопасности, Министерство промышленности и информационных технологий.

Таким образом, особенностью китайской государственной правовой политики в области агрегирования больших данных можно считать признание данных стратегическим национальным экономическим активом, введение национального суверенитета данных, формирование торговых рынков данных. КНР придерживается последовательной стратегии развития индустрии больших данных, благодаря государственному контролю наращивая инфраструктуру БД, обеспечивая условия для гражданского оборота данных и их защиты. На наш взгляд, опыт китайских регуляторов по категорированию данных, исходя из степени потенциального ущерба безопасности государства для установления режимов обработки больших данных, представляется заслуживающим внимания с точки зрения их потенциального комплаенса.

По итогам проведенного анализа можно констатировать, что большинство стран мира к регламентации технологий больших данных применяет мягкий подход правового регулирования, отдавая предпочтение развитию технологий и их техническому регулированию, ЕС же придерживается жесткого подхода, направленного на обеспечение соблюдения прав и законных интересов своих граждан.

В России программные документы, такие как постановление Правительства РФ от 18.04.2016 № 317[101] и принятые в его развитие дорожные карты, предваряли этап непосредственного формирования подходов к правовому регулированию больших данных, имели целью создание и развитие передовых технологий, способствующие актуализации НПА современным условиям и продвижению российского бизнеса на мировом рынке. Отправной точкой в формировании отечественной правовой политики, ориентированной на прогрессию технологий БД и инновационного потенциала страны можно считать принятие в 2017 г. Национальной программы «Цифровая экономика» (далее – НП[102]), в которой ключевая роль отводится именно этим прорывным цифровым технологиям. Стоит также отметить, что технологии БД упоминались и в Стратегии развития отрасли информационных технологий в РФ[103], однако нормативного закрепления понятие «большие данные» ни в одном из указан-

[97] Закон о кибербезопасности Китайской Народной Республики – Cyber security law (CSL) [Электронный ресурс]. URL: https://baike.baidu.com/item/ (дата обращения: 31.01.2023).

[98] Закон о защите личной информации – Personal Information Protection Law (PIPL) [Электронный ресурс]. URL: https://www.chinalawtranslate.com/en/Personal-Information-Protection-Law/ (дата обращения: 18.11.2025).

[99] Закон о безопасности данных – Data Security Law of the People's of China (DSL) [Электронный ресурс]. URL: http://en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311.htm/ (дата обращения: 18.11.2025).

[100] Регламент защиты критически важной инфраструктуры, Меры проверки сетевой безопасности, утверждены приказом Государственной службы интернет-информации 08.2021.

[101] О реализации Национальной технологической инициативы : постановление Правительства РФ от 18.04.2016 № 317 // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru, 20.04.2016.

[102] Национальная программа «Цифровая экономика» (утв. распоряжением Правительства РФ от 28.07.2017 № 1632-р) [Электронный ресурс] // Официальный сайт Правительства РФ. URL: http://government.ru (дата обращения: 20.10.2025).

[103] Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года : Распоряжение Правительства РФ от 01.11.2013 № 2036-р [Электронный ресурс] // Официальный сайт Правительства РФ. URL: http://government.ru (дата обращения: 20.10.2025).

ных документов стратегического планирования не получило. Таким образом, в настоящее время в российском законодательстве наблюдается правовая неопределенность, когда, с одной стороны, любая информация, прямо или косвенно относящаяся к определенному или определяемому лицу регулируется законодательством о персональных данных, а с другой стороны, такое регулирование не учитывает всех сущностных характеристик больших данных. Принятый в 2018 г. Указ Президента РФ от 07.05.2018 № 204[104] преследовал цель форсирования технологического прогресса России в инновационных высокотехнологичных отраслях экономики. В 2019 г. на смену НП пришла новая национальная программа[105], включавшая в том числе проект «Нормативное регулирование цифровой среды», а в 2020 г. и «Искусственный интеллект».

С точки зрения ужесточения требований к обороту персональных данных и, как следствие, больших данных, вбирающих в себя персональные данные, интерес представляет так называемый «Пакет Яровой» – федеральные законы о внесении изменений в ФЗ «О противодействии терроризму»[106], Уголовный кодекс и Уголовно-процессуальный кодекс РФ[107], – предусматривающий введение норм, обязывающих операторов связи и организаторов распространения информации, помимо персональных данных, хранить пользовательские метаданные, что позволяет сделать заключение о его нацеленности на регулирование распространения в первую очередь больших данных и отчасти персональных данных. Аналогичные цели преследует и Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ[108], инициировавший формирование и реализацию механизма локализации персональных данных россиян. В этой связи нам представляется обоснованным проведение параллели с китайским CSL, рассматривающим утечку персонализированной информации с позиции угрозы национальной безопасности и также предписывающий локализацию хранения пользовательских данных.

Кроме того, исследователи отмечают, что попытки узаконить понятие «большие данные» предпринимаются, что свидетельствует об осуществлении определенных шагов, предусмотренных документами стратегического планирования, но до настоящего времени эти шаги успеха не имеют. Так, законопроект, подготовленный Минкомсвязи России, предусматривающий внесение изменений в ФЗ «Об информации», закрепляющий понятие большие данные, был отклонен. Указанный законопроект вызвал критику со стороны бизнес-сообщества, отмечающего возможность реализации угрозы развитию отрасли ввиду установления существенных ограничений оборота больших данных. В этой связи представители Ассоциации БД отмечали, что понятие больших данных сформулировано настолько широко и расплывчато, то потенциально может включать любые общедоступные данные[109]. Помимо нормативного регулирования в РФ также развиваются этическая и техническая регламентация БД. Так, в России в 2019 г. Ассоциация БД совместно с Институтом развития Интернета разработали соответствующий этический Кодекс[110]. Кроме того, применяются национальные стандарты, гармонизированные со стандартами ИСО/МЭК[111].

---

[104] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : Указ Президента РФ от 07.05.2018 № 204 [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru, 07.05.2018 (дата обращения: 20.10.2025).

[105] Паспорт национальной программы «Цифровая экономика Российской Федерации», утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16 [Электронный ресурс] // Официальный сайт Правительства РФ. URL: http://government.ru (дата обращения: 20.10.2025).

[106] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон от 06.07.2016 № 374-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru, 07.07.2016 (дата обращения: 20.10.2025).

[107] О внесении изменений в Уголовный кодекс и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон от 06.07.2016 № 375-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru, 07.07.2016 (дата обращения: 20.10.2025).

[108] О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях : Федеральный закон от 21.07.2014 № 242-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru, 22.07.2014 (дата обращения: 20.10.2025).

[109] Яхтин В. А. Национальные информационные риски больших данных // Вестник Волгоградского государственного университета. Экономика. 2021. № 3. С. 19.

[110] Кодекс этики использования данных [Электронный ресурс]. URL: //bigdata.iis.ru (дата обращения: 03.03.2026).

[111] ГОСТ Р ИСО/МЭК 20546-2021 Информационные технологии (ИТ). Большие данные. Обзор и словарь – docs.cntd.ru; ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования – docs.cntd.ru.

Вышесказанное позволяет заключить, что Россия в вопросах построения государственной политики в сфере регламентации технологий больших данных избрала собственный, отличный от других государств, путь, характерной особенностью которого выступает локализация пользовательских данных, существенные ограничения трансграничной передачи данных, обеспечивающая централизацию внутреннего контроля за оборотом данных. Вместе с тем исследователи подчеркивают целесообразность законодательного комплаенса, позволяющего адаптировать под российскую специфику уже апробированные за рубежом НПА и перенять лучшие нормативные практики.

А. В. Семушин,

старший преподаватель кафедры теории государства и права и публично-правовых дисциплин юридического факультета Казанского инновационного университета имени В. Г. Тимирясова, г. Казань,

Нормативная институализация искусственного интеллекта в российском праве

Последние годы технологического развития характеризуются взрывным внедрением во все сферы жизнедеятельности так называемого «искусственного интеллекта». Реальные и потенциальные возможности искусственного интеллекта привели к признанию его «вектором развития» на предстоящие десятилетия, революционным прорывом. Российская Федерация не стоит на обочине мировых тенденций и также является активным участником его развития, находясь в середине второго десятка стран в области цифровых технологий искусственного интеллекта[112].

Социальная значимость искусственного интеллекта (ИИ) неизбежно привела и к необходимости правовой регуляторики сопряженных с его применением общественных отношений. Создание нормативно-правовой системы искусственного интеллекта акцентировано практически во всех документах российского стратегического планирования. При этом проблемой формирования его регуляторной базы является отсутствие однозначного понимания содержания термина «искусственный интеллект»[113].

В связи с чем в научных публикациях отмечается необходимость определения правового статуса искусственного интеллекта в качестве первоочередной задачи.

Молниеносное и революционное появление искусственного интеллекта в нашей жизни, повсеместное употребление данного термина в различных ипостасях, футурологические перспективы ИИ и превращение его в социальный феномен породили неопределенность в восприятии искусственного интеллекта. Как верно отмечает А. А. Гибадуллин, наряду с техническими и научными аспектами, вокруг ИИ возникли различные мифы и легенды, которые отражаются не только в общественном сознании, но и в культурных представлениях о его будущем[114].

«Мифологичность» искусственного интеллекта привела и к существенным различиям в его научном, правовом понимании. В настоящее время в академической среде в целом сложились два подхода. Сторонники первого допускают наделение ИИ статусом субъекта права, для чего предлагаются различные юридические конструкции: концепции «электронного лица» и «техноперсонализма», распространение на ИИ статуса юридического лица либо полный пересмотр традиционного понятия «субъекта права», с целью распространения его и на искусственный интеллект. Сторонники второго отрицают такую возможность[115].

Различна и теоретическая определенность искусственного интеллекта:

– искусственный интеллект – это компьютерная технология и система, способная решать поставленные сложные задачи либо предпринимать «собственные» действия посредством машинного обучения в условиях реальной действительности[116];

---

[112] Об утверждении Концепции технологического развития на период до 2030 года (вместе с «Концепцией технологического развития на период до 2030 года» : распоряжение Правительства РФ от 20.05.2023 № 1315-р (ред. от 21.10.2024) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 27.02.2026).

[113] Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» : распоряжение Правительства РФ от 19.08.2020 № 2129-р [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 03.03.2026).

[114] Гибадуллин А. А. Мифы и легенды вокруг искусственного интеллекта, мифология искусственного интеллекта // Научный электронный журнал «Академическая публицистика». 2024. № 1-1/2024. eISSN: 2541-8076. С. 553.

[115] Гладкая Е. Н. Искусственный интеллект и носитель искусственного интеллекта в контексте развития права высоких технологий // Регулирование отношений в сфере технологий искусственного интеллекта и робототехники. Цифровые технологии и право : сб. науч. тр. III Междунар. науч.-практ. конф. : в 6 т. Казань, 2024. С. 16–20.

[116] Ивлиев Г. П., Егорова М. А. Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта // Журнал российского права. 2022. Т. 26, № 6. С. 32–46.

– искусственный интеллект – это компьютер, который может выполнять задачи, обычно требующие человеческого интеллекта, такие как распознавание зрительных образов, распознавание речи, принятие решений и перевод языка; это технология, основанная на таких дисциплинах, как информатика, биология, психология, лингвистика, математика и инженерия[117];

– искусственный интеллект – это искусственная сложная кибернетическая компьютерно-программно-аппаратная система с когнитивно-функциональной архитектурой и собственными или релевантно доступными (приданными) вычислительными мощностями необходимых емкостей и быстродействия[118];

– искусственный интеллект – совокупность моделей, методов и технологий для решения плохо формализуемых (интеллектуальных) задач[119].

Н. В. Остроумов, указывая, что с точки зрения гражданского права интеллектуальные компьютерные программы являются – программами ЭВМ, считает, что применять к искусственному интеллекту определение программы ЭВМ не корректно и следует отграничить компьютерную программу от искусственного интеллекта[120].

Нормативно дефиниция искусственного интеллекта тождественно формулируется в ряде актов, непосредственно его регулирующих, согласно которым искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений. Технологическое решение – технология, программа для электронно-вычислительных машин (программа для ЭВМ), база данных или их совокупность, а также сведения о наиболее эффективных способах их использования[121].

Кроме того, осуществляется и его техническое нормативирование. Приказом Росстандарта от 28.10.2024 № 1550-ст утвержден и введен в действие «ГОСТ Р 71476-2024 (ИСО/МЭК 22989:2022). Национальный стандарт Российской Федерации. Искусственный интеллект. Концепции и терминология искусственного интеллекта», в котором содержатся стандартизированные концепции и терминология технологии ИИ. Согласно ГОСТу искусственный интеллект – это компьютерные системы, способные выполнять задачи, которые обычно требуют интеллекта, и использующие методы из многих областей знаний, таких как информатика, математика, философия, лингвистика, экономика, психология и когнитивные науки[122].

Указанные нормативные акты содержат и иные понятия, являющиеся вариациями и производными искусственного интеллекта, такие как технологии (в том числе доверенные) искусственного интеллекта, система и модель искусственного интеллекта (в том числе большие генеративные модели), «сильный» и «слабый», «универсальный» и «узконаправленный», символьный (символический) искусственный интеллект.

---

[117] Котова Д. К. Искусственный интеллект в политике: отношение государств к искусственному интеллекту // Социально-гуманитарные проблемы образования и профессиональной самореализации (Социальный инженер-2023) : сб. материалов Междунар. науч. конф. молодых исследователей. М. : Рос. гос. ун-т им. А. Н. Косыгина, 2023. С. 198–200.

[118] Понкин И. В., Редькина А. И. Искусственный интеллект с точки зрения права // Вестник РУДН. Серия «Юридические науки». 2018. Т. 22, № 1. С. 91–109.

[119] Устинова В. Г., Соколова Т. Н. Искусственный интеллект и авторское право: кто владеет результатами творчества искусственного интеллекта // Проблемы правоохранительной деятельности на современном этапе : сб. тр. IV Всерос. (с междунар. участием) науч.-практ. конф. Кострома : Костромской гос. ун-т, 2025. С. 662–667.

[120] Остроумов Н. В. Искусственный интеллект в праве: обзор существующих концепций правового регулирования отношений с участием носителей искусственного интеллекта // Законность и правопорядок. 2021. № 3 (31). С. 61–66.

[121] О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года» : Указ Президента РФ от 10.10.2019 № 490 (ред.15.02.2024); Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года : распоряжение Правительства РФ от 19.08.2020 № 2129-р; О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве, об особенностях обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» : Федеральный закон от 24.04.2020 № 123-ФЗ (ред.08.08.2024); Об утверждении критериев определения принадлежности проектов к проектам в сфере искусственного интеллекта» : приказ Минэкономразвития России от 29.06.2021 № 392 [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 27.02.2026).

[122] ГОСТ Р 71476-2024 (ИСО/МЭК 22989:2022). Национальный стандарт Российской Федерации. Искусственный интеллект. Концепции и терминология искусственного интеллекта : приказ Росстандарта от 28.10.2024 № 1550-ст [Электронный ресурс] // СПС «Гарант» (дата обращения: 03.03.2026).

Следует отметить нормативную оговорку о том, что специфика применения искусственного интеллекта может привести в будущем к формулировке разных определений искусственного интеллекта в зависимости от области его использования и отходу от универсального определения этого термина[123].

Помимо дефиниции понятия искусственного интеллекта существенное значение в его правовой институализации имеет и разрешение вопросов юридической ответственности. В приведенных правовых актах четко постулируется подконтрольность искусственного интеллекта человеку, возложение во всех случаях ответственности на физических или юридических лиц и запрет ее переложения на системы искусственного интеллекта. Кардинальных изменений в институте юридической ответственности за вред, причиненный системами искусственного интеллекта, в будущем не предполагается[124].

Таким образом, нормативно, искусственный интеллект – это сложная, многоэлементная, обладающая повышенными возможностями, но всего лишь основанная на электронно-вычислительном программировании информационно-коммуникационная технология – средство решения различных задач, и является объектом, а не субъектом отношений. Исключительно личностная ответственность за последствия его применения, безусловно, постулирует отсутствие у искусственного интеллекта правосубъектности, и каких-либо оснований придавать ему соответствующий правовой статус в различных квазисубъектных формах, как предлагается рядом исследователей, не имеется.

В настоящее время регулирование вопросов искусственного интеллекта еще не приняло окончательную форму и этот процесс активно продолжается.

Ж. А. Русских,
ст. преподаватель кафедры информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
О. В. Дубовикова,
ст. преподаватель кафедры информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Методы обнаружения и предотвращения целевых фишинговых атак с использованием алгоритмов машинного обучения

Современные киберугрозы представляют собой быстро эволюционирующую систему, характеризующуюся высокой сложностью, автоматизацией и целенаправленностью. Оперативность, сложность и масштабность киберугроз позволяет охватывать различные сферы деятельности, проникать в глобальные цифровые инфраструктуры. За последние годы, помимо устойчивого роста успешных кибератак, киберугрозы претерпели серьезную трансформацию – как с точки зрения технологий, так и организации самих атак[125]. Искусственный интеллект стал мощным оружием в руках злоумышленников, кардинально изменил ландшафт киберугроз, вывел их на новый качественный уровень. Так, по мнению ведущих специалистов, около 85 % кибератак в мире в 2026 году будет производиться с использованием искусственного интеллекта. Искусственный интеллект помогает создавать новые вирусы, фишинговые сайты и дипфейки, находить уязвимости[126]. Другим ключевым изменением последних лет стало превращение киберпреступности в полноценную экономическую отрасль. Если ранее атаки чаще совершались отдельными злоумышленниками, располагающими ограниченным набором программно-технических средств, то сегодня наблюдается тенденция к формированию

[123] Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года : распоряжение Правительства РФ от 19.08.2020 № 2129-р [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 03.03.2026).

[124] О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») : Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) (дата обращения: 27.02.2026); Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» : распоряжение Правительства РФ от 19.08.2020 № 2129-р [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 03.03.2026).

[125] Киберугрозы 2026: что нас ждет [Электронный ресурс] // Fintech&Retail EURASIA. URL: https://fintech-retail.com/2026/03/10/kiberugrozi/ (дата обращения: 03.04.26).

[126] Сбер: в 85 % кибератак в 2026 году будет использоваться искусственный интеллект [Электронный ресурс] // ТАСС. URL: https://tass.ru/ekonomika/24014887 (дата обращения: 03.04.26).

организованных структурированных преступных сообществ, имеющих четкую специализацию по отдельным направлениям деятельности: от разработки вредоносного программного обеспечения и киберразведки, до реализации кибератак и продажи похищенных данных. Сформировалась особая бизнес-модель *Cybercrime-as-a-Service* (*CaaS*), когда весь спектр криминальных цифровых решений предлагается потенциальному заказчику. Теневые онлайн-площадки содержат каталоги специализированных продуктов и услуг, прозрачные тарифы и предоставляют техническую поддержку, обеспечивая, таким образом, доступность и простоту совершения преступлений.

В условиях международной напряженности кибератаки на российские организации усиливаются, растет число атакующих групп. В соответствии с отчетом, составленным по материалам компаний Positive Technologies, в 2025 году наблюдался общий рост числа кибератак, особенно на критическую информационную инфраструктуру и государственные учреждения, а также значительный финансовый ущерб от киберпреступности. За первое полугодие 2025 г. «наиболее распространенными методами успешных атак на организации стали использование вредоносного программного обеспечения (63 %), социальная инженерия (50 %) и эксплуатация уязвимостей (31 %)»[127]. Доли использования различных методов успешных атак на организации и частных лиц в первом полугодии 2025 г. представлены на рис. 1.

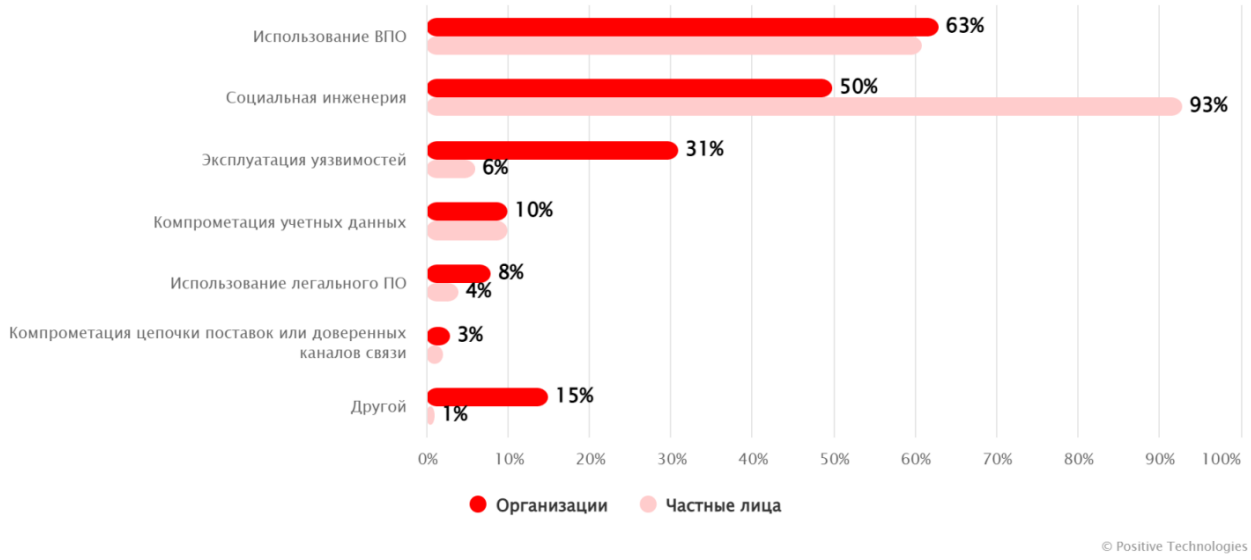

Рис. 1. Методы атак (доли успешных атак, 1-е полугодие 2025 г.)

При этом основной канал социальной инженерии – электронная почта (для организаций – 88 %) и сайты (для частных лиц – 69 %) (см. рис. 2).

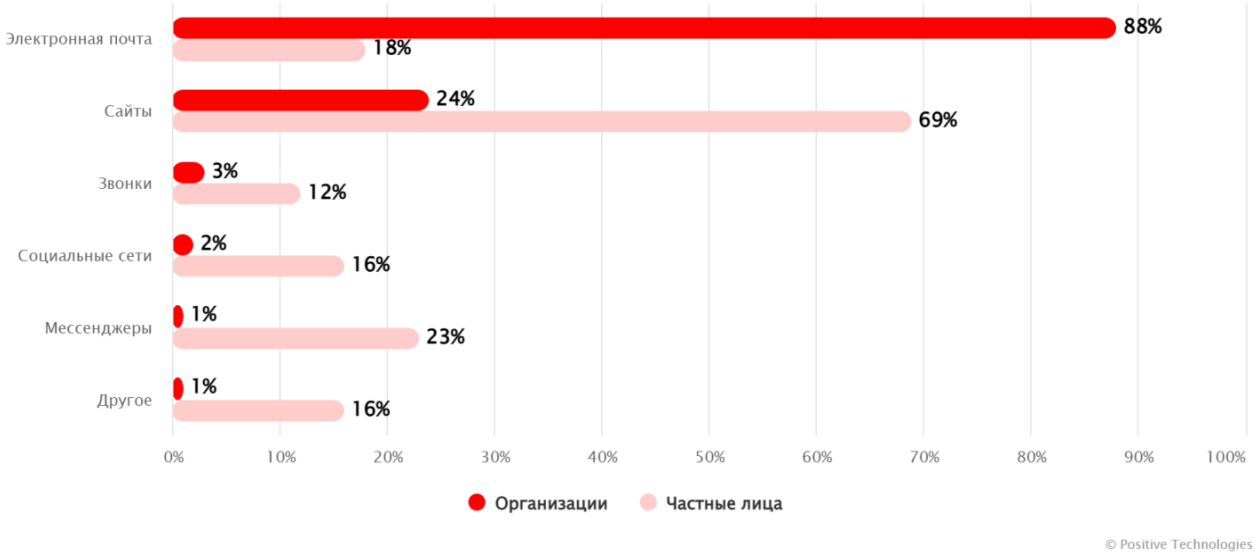

Рис. 2. Каналы социальной инженерии (доля успешных атак, первое полугодие 2025 г.)

[127] Вяткина А. Осипова А Актуальные киберугрозы: I–II кварталы 2025 года [Электронный ресурс]. URL: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/ (дата обращения: 03.04.26).

Социальная инженерия – манипуляция людьми с целью получения доступа к информации или ресурсам, либо выполнения определенных действий. Методы и технологии социальной инженерии основаны на использовании человеческой психологии, социологических приемах, а не на техническом взломе. Злоумышленники часто играют на сильных эмоциях: страхе, чувстве вины, любопытстве, жажде наживы.

Одним из наиболее значимых психологических факторов воздействия, используемых в социальной инженерии, является авторитет. Если сообщения поступают якобы от руководителя или специалиста, вероятность выполнения такого «поручения» значительно возрастает. Не менее важным является фактор срочности. Когда создается ощущение нехватки времени, пользователь принимает решения быстрее и менее обдуманно. Эти обстоятельства снижают уровень критического восприятия информации. Любопытство также играет значительную роль. Пользователь может открыть неизвестный файл или перейти по ссылке из Интернета. Более наглядно отображает значение различных психологических факторов, используемых социальной инженерией, таблица 1, представленная ниже.

Таблица 1

Распространенность психологических факторов в атаках социальной инженерии[128, 129]

Психологический факт	Доля использования (%)
Авторитет	28
Срочность	22
Любопытство	18
Выгода	16
Доверие	10
Давление	6

Несмотря на то, что методам социальной инженерии, а также ее профилактике уделяется большое внимание в научных исследованиях и СМИ, жертвами социальной инженерии зачастую становятся люди с высоким уровнем образования и большим опытом. Исследования показывают, что именно они и являются наиболее вероятными целями такого мошенничества, т. к. ожидаемо являются обладателями крупных денежных средств или больших полномочий в организации. Подверженность к подобным психологическим манипуляциям этой группы людей объясняется чрезмерной уверенностью в способности распознать угрозу, а как следствие, – невнимательность и большая восприимчивость к новым формам использования этих методов[130]. Высокий уровень успешных атак социальной инженерии в организациях подтверждает вышесказанное.

Наиболее распространенной техникой социальной инженерии на сегодняшний день является фишинг (более 60–70 % всех атак, использующих манипуляцию человека[131]). С другой стороны, фишинг продолжает оставаться одним из основных методов получения первоначального доступа к защищенным системам.

Фишинг – мошенническая практика, когда киберпреступники выдают себя за надежные источники для получения конфиденциальной информации пользователя. Одна из разновидностей фишинга – использование подменных доменных имен, которые похожи на настоящие.

В последнее время также наблюдается значительный рост фишинговых атак. В ряде отчетов отмечается, что фишинг и его разновидности (включая целевой фишинг) остаются стабильно результативными инструментами для злоумышленников, особенно в атаках на бизнес. Так, Роскомнадзор сообщил, что в 2026 г. при мониторинге сети было заблокировано более 119 000 фишинговых сайтов, что на 441 % больше, чем в 2025 г. Приведенные показатели демонстрируют как размах фишинговых инфраструктур, так и усиление мер противодействия им. Увеличение количества атак данного вида на своих клиентов фиксируют банки, IT-компании, телекоммуникационные операторы. Таким образом, фишинг остается самой массовой и опасной киберугрозой. Эксперты отмечают, что в 2025–2026 гг. атаки смещаются в сторону целевого фишинга, направленного на топ-менеджмент и ключевых сотрудников компаний.

---

[128] Cory Marchand. The Psychology of Social Engineering [Электронный ресурс]. URL: https://www.coalitioninc.com/blog/security-labs/the-psychology-of-social-engineering (дата обращения: 03.04.26).

[129] John Owen. Psychological Mechanisms in Social Engineering Attacks [Электронный ресурс] // Easy Chair Preprint. 2024. № 13835. URL: https://easychair.org/publications/preprint/51lT/open (дата обращения: 03.04.26).

[130] Mirjana Pejić Bach, Tanja Kamenjarska, Bersilav Žmuk Targets of phishing attacks: The bigger fish to fry // Procedia Computer Science. 2022. № 204. С. 448–455.

[131] Мельников А. И. Социальная инженерия в цифровой эпохе: анализ методов манипуляции человеческим фактором в целях кибератак // Социально-гуманитарные знания. 2024. № 1. URL: https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-v-tsifrovoy-epohe-analiz-metodov-manipulyatsii-chelovecheskim-faktorom-v-tselyah-kiberatak (дата обращения: 06.04.2026).

Целевой фишинг (spear phishing) – это разновидность фишинга, при котором злоумышленники целенаправленно атакуют конкретных лиц или организации. В отличие от массового фишинга такие атаки тщательно спланированы: преступники собирают информацию о жертве, подделывают письма от доверенных отправителей и используют другие методы социальной инженерии для достижения своих целей. Последствия могут выражаться в утечке конфиденциальных данных, финансовых потерях и компрометации корпоративных систем.

Целевые фишинговые угрозы: текущее состояние и тенденции развития

Как и для киберугроз в целом, так и для фишинга, одной из главных тенденций является активное использование технологий искусственного интеллекта, благодаря чему происходит эволюция фишинговых атак. По данным компании «Информзащита» искусственный интеллект используется в 80 % фишинговых атак. Искусственный интеллект может автоматически собирать и анализировать информацию о компаниях и их сотрудниках из открытых источников, в том числе и в социальных сетях. На основе этой информации он может разрабатывать персонализированные сценарии. Он способен генерировать сообщения, которые практически неотличимы от настоящей деловой переписки[132]: правильная грамматика, нужные формулировки и обращения, характерные для конкретного отправителя. Такие целевые угрозы вызывают полное доверие у жертвы.

Другой значимой тенденцией современных целевых фишинговых атак является использование сразу нескольких каналов для установления коммуникации с жертвой: по телефонному звонку, СМС-сообщению, сообщению по почте или в мессенджере, что позволяет усилить психологическое давление.

Наконец, еще одной значимой тенденцией является тот факт, что фишинг не является конечной целью. В современных кибератаках он практически всегда выступает начальным звеном проникновения или инструментом разведки в составе многоэтапных операций. Ниже представлены **основные типы сложных кибератак**, где целевой фишинг играет ключевую составную часть:

1. Крупные атаки APT-группировок. Целевой фишинг используется для компрометации конкретных сотрудников, кражи учетных данных или доставки костомизированного вредоносного программного обеспечения, что позволяет установить первоначальный доступ и начать скрытное закрепление в инфраструктуру. Так, в 2024–2025 гг. была «обнаружена новая волна кибератак APT-группировки CloudAtlas на предприятия оборонно-промышленного комплекса России. Вектором проникновения традиционно выступала фишинговая рассылка электронных писем с вредоносными документами Microsoft Office во вложении»[133].

2. Ransomware-атаки (атаки программ-шифровальщиков). Современные ransomware-группы проводят многоэтапные операции через фишинговые письма или сообщения в мессенджерах. Злоумышленники получают доступ к сети, крадут учетные данные привелигированных пользователей, отключают антивирусы или EDR-системы и создают бэкдоры перед массовым шифрованием и эксфильтрацией данных (несанкционированная передача конфиденциальной информации целевой системы за ее пределы). Так, в 2024–2025 гг. «российские госорганизации, а также IT-компании, промышленность и телекоммуникации подвергались сложным атакам со стороны группировки BO Team, которая успешно совмещает хактивизм с финансовыми мотивами»[134]. Злоумышленники использовали целевой фишинг для проникновения в системы организаций, а затем наносили ущерб хранимым данным (уничтожали, блокировали доступ к ним, шифровали, требовали выкуп за восстановление работы).

3. Мошенничество с деловой перепиской – кибератаки, которые направлены на компрометацию корпоративной почты. Традиционно они разворачиваются по следующему сценарию. Через фишинговые сайты на облачные почтовые платформы Microsoft 365, Google Workspace либо на внутренние порталы крадутся учетные данные. Затем злоумышленники имитируют переписку от имени руководителя, ведущих специалистов или партнеров организации для санкционирования платежей или передачи данных. Другой пример – злоумышленники, получив доступ к почтовым сервисам через фишинговое вложение с PDF-файлом, содержащим QR-код (еще один актуальный фишинговый тренд 2025 – по данным лаборатории Касперского «рост атак через QR-коды достиг критического уровня, показав 435 % увеличения случаев фишинга с августа по ноябрь 2025 г.»[135]), длительное время незаметно присутствуют в системе, наблюдая за перепиской. А в нужный момент при обсуждении

---

[132] Фишинг 2.0: почему нейросети делают атаки более убедительными и опасными [Электронный ресурс] // Пресс-релизы Финансового Университета при правительстве РФ. URL: https://www.fa.ru/university/structure/university/uso/press-service/press-releases/fishing-2-0-pochemu-neyroseti-delayut-ataki-bolee-ubeditelnymi-i-opasnymi (дата обращения: 06.04.2026).

[133] Вяткина А. Осипова А. Указ. соч.

[134] Там же

[135] QR-коды стали главным инструментом хакеров – рост атак в 5 раз. // ASECTOR. Аналитика. Тренды. Решения.. URL: https://asector.ru/news/2026_01_qr_kody_stali_glavnym_instrumentom_hakerov (дата обращения: 06.04.2026).

реального платежа подменяют реквизиты платежных документов и отправляют требование срочной оплаты от лица руководителя компании. Данный пример показывает, что фишинг лишь начальный этап, настоящая угроза – длительное присутствие в почте и имитация легитимных процессов.

4. Кибершпионаж и сбор разведданных – долгосрочный мониторинг инфраструктуры для кражи интеллектуальной собственности, переговоров или технической документации. Таргетированный (высокоперсонализированный) фишинг обеспечивает скрытный доступ, после которого устанавливаются инструменты перехвата трафика, кейлоггеры или легитимные утилиты, используемые для незаметного сбора информации. Так, например, «в серии атак, направленной на российские организации из сферы промышленности, энергетики и ЖКХ, группировка Phantom Core тоже использовала фишинговые письма, в которых содержались архивы с вредоносными LNK-файлами, замаскированными под PDF-документы. После открытия ярлыка запускался бэкдор, позволяющий злоумышленникам удаленно управлять зараженной системой. Атака была направлена на получение доступа к конфиденциальной информации и длительное скрытое пребывание внутри сети организации»[136].

5. Финансовое мошенничество и атаки на банковский сектор – целенаправленные операции против банков, платежных систем или их клиентов. Мошенники используют поддельные SMS (якобы от банков), поддельные страницы авторизации, звонки от службы безопасности банков, SIM-свопинг для перехвата реквизитов, несанкционированного доступа, обхода многофакторной аутентификации.

И другие виды угроз.

Таким образом, мы видим, что фишинг является лишь начальным этапом, входом для сложных составных кибератак. Мошенники постоянно совершенствуют свои методы и техники, но основной причиной по-прежнему остается человеческий фактор.

Рассмотренные выше актуальные тенденции еще раз доказывают, что фишинговые угрозы стали более профессиональными, масштабными, многоуровневыми, автоматизированными и чрезвычайно опасными.

Основные направления использования методов машинного обучения для обнаружения и предотвращения целевых фишинговых атак

Искусственный интеллект активно используется специалистами для разработки инструментов для борьбы с фишинговыми атаками. Необходимость использования этих технологий обусловлена несколькими причинами. Во-первых, генеративные модели позволяют злоумышленникам создавать десятки тысяч фишинговых сообщений за считанные минуты. Традиционные методы физически не успевают обрабатывать такой поток. Алгоритмы машинного обучения способны анализировать миллионы сообщений в реальном времени, блокируя угрозы до взаимодействия с пользователем. Современные *LLM* генерируют текст, практически неотличимый от человеческого, с учетом стиля, контекста, тона. Статические правила и регулярные выражения бессильны против таких атак. Модели на основе *NLP* способны выявлять самые незначительные аномалии, скрытые манипулятивные конструкции, семантические противоречия. В-третьих, атаки постоянно эволюционируют: злоумышленники обновляют промты, меняют тактики обхода фильтров, применяют так называемые *Adversarial-методы* (методы, предназначенные для введения нейронных сетей и других моделей ИИ в заблуждение). Традиционные методы (черные списки, сигнатурный анализ, правила) не успевают за эволюцией атак. ИИ-системы защиты могут обучаться на новых данных в режиме реального времени или с минимальной задержкой, автоматически обновлять веса и адаптироваться к новому ландшафту угроз. И, наконец, ИИ-фишинг сегодня редко ограничивается текстом. Это поддельные голоса, видео, динамически генерируемые URL, поведенческие триггеры. Только ИИ способен одновременно анализировать текстовые, визуальные, сетевые, поведенческие сигналы, выстраивать скоринг рисков.

Ниже представлены **основные направления** применения ИИ (в частности алгоритмов машинного обучения) для обнаружения и предотвращения фишинговых атак:

1. Анализ контента электронных писем с помощью систем обработки естественного языка (*NLP*) и нейросетей. Продвинутые модели *NLP* анализируют[137] контекст и тон сообщений для выявления манипулятивных формулировок (срочные запросы на перевод средств или изменения паролей). Технологии компьютерного зрения могут использоваться для анализа изображений в сообщениях, выявляя подозрительные элементы или фальшивые логотипы; несоответствия в стиле бренда при попытках имперсонации (имитации, подделки). Такие системы способны отличать легитимные корпоративные письма от поддельных.

[136] Вяткина А. Осипова А. Указ. соч.

[137] Cyber Security Report 2026. Top threats, emerging attacker techniques, and data-backed CISO recommendations for the year ahead. URL: https://www.checkpoint.com/about-us/contact-check-point/ (дата обращения: 06.04.2026).

2. Классификация и анализ URL-адресов – данное направление достаточно хорошо представлено в научных зарубежных и отечественных исследованиях, поскольку именно URL-ссылки являются наиболее распространенным вектором проведения фишинговых атак. Но для противодействия им требуется комплексный подход, включающий в зависимости от решаемых задач следующие группы методов[138, 139]:

- методы анализа содержимого URL-адреса;
- методы анализа контента веб-страницы;
- методы анализа сетевого трафика.

3. Поведенческий анализ и обнаружение аномалий (Behavioral Anomaly Detection) позволяет выявить отклонения от нормального поведения пользователей, которые могут указывать на фишинговую атаку. Осуществляется это через анализ характерных паттернов коммуникации конкретного адресата (стиль письма, время обращений, частота контактов и др.).

4. Противодействие ИИ-фишингу предполагает обнаружение контента, сгенерированного искусственным интеллектом (сообщения, созданные LLM).

5. Адаптивное обучение и непрерывная дообучаемость предполагают обновление моделей в реальном времени на основе новых образцов фишинга, в результате чего системы сохраняют эффективность даже при быстрой эволюции фишинговых тактик.

6. Оркестрация защиты и автоматизация реагирования позволяют сократить время реакции системы безопасности на угрозы и повысить ее эффективность. Оркестрация – это процесс интеграции и координации работы различных инструментов и систем безопасности для централизованного управления. Оркестрация выступает «дирижером» платформы: обеспечивает интеграцию разнородных средств защиты (межсетевых экранов, EDR-систем, SIEM, DLP) и их слаженное взаимодействие. Автоматизация реагирования предполагает выполнение «рутинных» задач безопасности без участия человека (отправка уведомлений, анализ логов, блокировка IP), что повышает скорость работы и снижает количество ошибок. Для этой цели создаются специальные программные решения – *SOAR* (Security Orchestration, Automationand Response), которые позволяют собирать данные о событиях информационной безопасности из различных источников, автоматизировать типовые сценарии реагирования на инциденты, объединять разрозненные защитные решения в единую систему управления. Методы машинного обучения обогащают *SOAR*, усиливают его, превращают в самообучающуюся систему реагирования.

7. Создание обучающих систем – искусственный интеллект может использоваться для разработки интерактивных обучающих программ, которые помогают пользователям распознать фишинговые атаки и обучают их безопасному поведению в сети.

Ниже представлен анализ методов машинного обучения для противодействия фишингу по некоторым наиболее важным и востребованным направлениям.

Методы машинного обучения для анализа контента с целью выявления фишинговых писем на основе NLP: общая характеристика

Для анализа текста писем и выявления фишинга на основе *NLP* (обработка естественного языка) применяют широкий спектр методов машинного обучения (*Machine Learning, ML*), которые особенно эффективны для сложных сценариев. Анализируются содержание, структура и лингвистические особенности письма, при этом исследователи применяют различные алгоритмы и техники машинного обучения[140, 141, 142, 143, 144, 145]. Их выбор зависит от множества факторов, включая количество

---

[138] Kutlyev D. Z., Shmanina A. V. Using machine learning algorithms to protectagainst URL phishing // Mavlyutovskie chteniya : XV Vserossiiskaya molodezhnaya nauchnaya konferentsiya [Mavlyutov Readings. Proceedings of the XV All-Russian Youth Scientific Conference]. Ufa, 2021. Vol. 4. P. 430–435.

[139] Лукманова К. А., Картак В. М. Распознавание фишинговых ссылок с использованием методов машинного обучения // Безопасность цифровых технологий. 2024. № 3 (114). С. 9–20.

[140] Said Sallouma, Tarek Gabera, Sunil Vaderaa, and Khaled Shaalan. Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey [Электронный ресурс]. URL: https://www.researchgate.net/publication/353246848_Phishing_Email_Detection_Using_Natural_Language_Processing_Techniques_A_Literature_Survey

[141] Shivam Pandey, Prashant Priyadarshi, Suman Devi. Phishing attack Detection using NLP and Machine learning [Электронный ресурс] // 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N). 2024. URL: https://ieeexplore.ieee.org/document/10895895/figures#figures

[142] Catal C. et al. Applications of deep learning for phishing detection: a systematic literature review // Knowledge and Information Systems. 2022. Т. 64, № 6. С. 1457–1500.

[143] Лукманова К. А., Картак В. М. Разработка системы защиты от фишинговых атак с использованием программно-аппаратной реализации методов машинного обучения // Моделирование, оптимизация и информационные технологии. 2024. № 12(4).

доступного размеченного материала, желаемые показатели точности и быстродействие модели, а также возможности ее интерпретации конечным пользователем. Для решения представленных задач используются как традиционные (классические) методы машинного обучения, так и методы глубокого обучения и нейросети.

Классические методы машинного обучения хорошо работают при наличии размеченных данных (письма с метками «фишинг»/«не фишинг») и позволяют быстро обучить модель. К ним относятся:

- **Наивный байесовский классификатор** (*Naive Bayes*) – один из самых популярных методов для фильтрации спама и фишинга. Он строит вероятностную модель, оценивая, насколько часто определенные слова или фразы встречаются в фишинговых письмах.
- **Метод опорных векторов** (*Support Vector Machine, SVM***)** основан на построении гиперплоскости, которая разделяет данные на два класса и таким образом строит границу между классами в многомерном пространстве признаков. Может обрабатывать и линейно разделимые данные, и данные с нелинейными зависимостями. Эффективен для задач классификации – фишинг/не фишинг.
- **Логистическая регрессия** (*Logistic Regression*) – метод использует логистическую функцию на основе взвешенной суммы признаков для предсказания вероятности принадлежности сообщения к фишинговым. Обучение модели происходит оптимизацией весовых коэффициентов признаков.
- **Случайный лес** (*Random Forest*) – ансамблиевый метод, представляющий собой совокупность деревьев, каждое из которых обучается на различных подмножествах данных и признаков. Затем результаты всех деревьев объединяются для получения итоговой классификации. Способен обрабатывать большие объемы данных и позволяет учитывать сложные нелинейные зависимости между различными признаками текста.
- **Градиентный бустинг** (*Gradient Boosting on Deciption Trees, GBDT*) – еще один ансамблиевый метод, основанный на построении линейной комбинации алгоритмов (обычно деревьев решений). Каждый следующий алгоритм уменьшает ошибку текущего ансамбля, а для обучения каждого последующего алгоритма используется градиент ошибки (функция, которая измеряет насколько ошибочны предсказания предыдущего шага). Этот метод позволяет находить зависимости в данных различной природы и эффективен при работе с большим объемом данных. Наиболее популярные реализации этого метода – *XGBoost, LightGBM*.

Глубокое обучение (*Deep Learning, DL*) – современный подход машинного обучения, совокупность методов с использованием многослойных нейронных сетей (с учителем, с частичным привлечением учителя, без учителя, с подкреплением), способных самообучаться на большом объеме данных. Глубокие нейронные сети могут обрабатывать разные типы данных и позволяют решать широкий круг задач, включая распознавание текстов, машинное зрение, фильтрацию сообщений, классификацию и др. В глубоком обучении у нейросетей несколько скрытых слоев. Они способны автоматически извлекать признаки из текста, изучать сложные языковые структуры, контекстуальные связи. К методам глубокого обучения относятся:

- **Рекуррентные нейронные сети** (*Recurrent neural network, RNN*) – вид нейронных сетей, разработанных для решения задач обработки последовательных пространственных цепочек или серий событий во времени, где следующая позиция зависит от предыдущего состояния. Используется для решения последовательных задач, т. е. прогнозируемых сценариев, в которых ответ зависит от предыдущих данных (в том числе в *LLM*, при анализе эмоционального фона, распознавании именованных сущностей, выявления контекста и зависимости между фразами, манипулятивных формулировок). У *RNN* есть своя память – внутреннее скрытое состояние, которое постепенно обновляется и накапливает информацию о том, что происходило ранее. Благодаря этому *RNN* могут обрабатывать не только элементы по отдельности (слова в предложении), но учитывают контекст всей последовательности. Улучшенными архитектурами *RNN* являются *LSTM* (*Long Short-Term Memory*), *GRU* (*Gated Reccurent Unit*), которые особенно хорошо проявили себя с длинными и сложными последовательностями.
- **Трансформеры (*Transformers*)** – новейшие архитектуры, которые на сегодняшний день вытеснили *RNN* при решении задач обработки текста, изображения и других данных. Трансформеры (особенно на основе модели *BERT*) стали популярны благодаря механизму внимания, в результате чего способны анализировать текст сообщения целиком и выявлять сложные признаки письма. В отличие от рекурентных сетей они более тяжеловесны – ресурсоемки и медлительны.

---

[144] Корнюхина С. П., Лапонина О. Р. Исследование возможностей алгоритмов глубокого обучения для защиты от фишинговых атак // International Journal of Open Information Technologies. 2023. Т. 11, № 6. С. 163–174.

[145] Болдырихин Н. В., Ядрец Э. А. Обнаружение фишинговых электронных писем с помощью рекуррентных нейронных сетей // Вопросы кибербезопасности. 2025. № 4. С. 134–141.

Выбор метода машинного обучения для выявления фишинговых сообщений зависит от ряда критериев: точность метода, количества ложноположительных и ложноотрицательных срабатываний, скорости работы, объема датасета, качества размеченных данных, специфики решаемой задачи, интерпретируемости результата. Ниже в таблице 2 приведено сравнение по основным признакам[146].

Таблица 2

Метод	Точность	Скорость работы	Ложнополо-жительные ответы	Ложноотри-цательные ответы	Особенности метода
Наивный байесовский классификатор	Средняя	Высокая	Много	много	Простой, быстрый, но не улавливает сложные зависимости; подходит для задач классификации и анализа тональности
Логистическая регрессия	Средняя/ высокая	Высокая	Средне	Средне	Эффективен для задач классификации, хорошо интерпретируется
Метод опорных векторов (*SVM*)	Высокая	Средняя/ низкая	Мало	Мало	Отлично для классификации, но сложность работы с большими данными
Случайный лес (*Random Forest*)	Высокая (до 98 %)	высокая	Мало	Мало	Фильтрация шума, при этом сохранение чувствительности к реальным угрозам; устойчив к переобучению, хорошо работает с разными признаками; ресурсоемкий для больших объемов данных
Градиентный бустинг (*XGBoost*)	Очень высокая (до 99 %)	Средняя	Мало	Очень мало	Высокая точность, гибкость; работа с большими данными; более долгое переобучение по сравнению с *RF*
Рекуррентные сети (*LSTM, GRU*)	Высокая (до 98 %)	Низкая	Средне/мало	Мало	Эффективен для длинных последовательностей более сложные архитектуры увеличивают число параметров и время обучения; хорошо понимают контекст, но требует много данных и ресурсов
Transformer (*BERT* и др.)	очень высокая	очень низкая	мало	очень мало	Максимальная точность и адаптивность к новым техникам; но медленный и ресурсоемкий; для обучения требует большие объемы размеченных данных

Таким образом, для быстрой проверки писем в режиме реального времени можно использовать ансамблиевые методы (*RF, XGBoost*), которые показывают хорошую точность и малое количество ошибок. Для детальной проверки подозрительных писем можно использовать глубокое обучение (*LSTM, BERT*), чтобы минимизировать ошибки. Классические методы (*Байес, регрессия*) сейчас применяются реже из-за высокой доли ошибок, но могут быть полезны как первый этап фильтрации.

В реальных системах часто используют каскад методов: сначала быстро отсеивают очевидный спам простыми методами, а сложные случаи отправляют на анализ более мощным моделям.

Анализ методов машинного обучения, используемых для противодействия AI-фишингу

Особо следует рассмотреть методы машинного обучения для противодействия AI-фишингу (письмам/сообщениям, созданным с помощью *LLM*). Традиционные признаки фишинга – грамматические ошибки, странные ссылки, неформальный стиль в таких письмах отсутствуют. Они написаны безупречно, используют деловой стиль и часто персонализированы.

Эффективность классических методов машинного обучения против AI-фишинга низкая. Письма от *LLM* не содержат типичных маркеров (ошибок, подозрительных ссылок в тексте), на которые эти модели «заточены». Они могут ошибочно классифицировать такое письмо, как легитимное.

Глубокое обучение (*DL*) и ***NLP*-модели** – это основное оружие борьбы с AI-фишингом. Модели-трансформеры (например, на основе *BERT*) в этом случае также показывают высокую эффективность, что подтверждается рядом аналитических и практических исследований[147, 148, 149, 150].

---

[146] Беспалова Н. В., Корчагин С. А., Сердечный Д. В. Анализ алгоритмов машинного обучения используемых для обработки текстовых документов [Электронный ресурс] // ИВД. 2025. № 5 (125). URL: https://cyberleninka.ru/article/n/analiz-algoritmov-mashinnogo-obucheniya-ispolzuemyh-dlya-obrabotki-tekstovyh-dokumentov (дата обращения: 06.05.2026).

[147] Vaswani, Ashish; Shazeer, Noam; Parmar, Niki; Uszkoreit, Jakob; Jones, Llion; Gomez, Aidan N; Kaiser, Łukasz; Polosukhin, Illia (Декабрь 2017). Attention is All you Need. In I. Guyon and U. Von Luxburg and S. Bengio and H. Wallach and R. Fergus and S. Vishwanathan and R. Garnett (ed.). 31st Conference on Neural Information Processing Systems (NIPS). Advances in Neural Information Processing Systems.Vol. 30. Curran Associates, Inc. arXiv:1706.03762.

[148] Эпоха ИИ-трансформеров: что это за архитектура и как работает механизм внимания [Электронный ресурс]. URL: https://serverflow.ru/blog/stati/epokha-ii-transformerov-chto-eto-za-arkhitektura-i-kak-rabotaet-mekhanizm-vnimaniya

[149] Смирнов А. В., Петров К. Д. Современные методы обнаружения фишинговых атак с использованием машинного обучения // Кибербезопасность и защита информации. 2023. № 4. С. 45–60.

[150] Соколов Д. В. Глубокое обучение для анализа текстов. СПб. : Питер, 2023. 256 с.

Они анализируют контекст всего предложения или письма целиком, улавливают семантические связи и тонкие стилистические нюансы. LLM склоны писать слишком гладко, безлично и использовать стандартные фразы-клише. Модель *BERT* может заметить неестественно высокую «плавность» текста или отсутствие индивидуального стиля автора. С точки зрения анализа семантики, эта модель может выявить логические «несостыковки» или неуместный контекст, который человек мог бы пропустить. Кроме того, *BERT* проводит сравнение стилей (*Writing Style DNA*) и показывает максимальную эффективность. Модель обучается на реальной переписке сотрудника или компании. Когда приходит письмо (даже идеальное по содержанию), система сравнивает его стиль (использование слов, длина предложений, пунктуация) с эталоном. Любое отклонение – сигнал тревоги.

Другим важным решением данной задачи являются **детекторы**, специально созданные **для распознавания ИИ-контента**. Они представляют собой бинарные классификаторы, обученные отличать тексты, написанные человеком, от текста, сгенерированного машиной. Чаще всего они также строятся на базе глубокого обучения и, в частности, на архитектуре трансформеров. Слабым их звеном является то, что как только появляется новый детектор, разработчики *LLM* находят способы сделать текст более «человечным» (например: добавление намеренных опечаток, варьирование стиля). Другим недостатком является достаточное количество ложноположительных срабатываний. Хороший человеческий текст может быть ошибочно принят за работу ИИ. Для повышения точности и надежности используются и другие техники – ансамблевые методы (часто один детектор не дает высокой гарантии, поэтому системы могут использовать ансамбль моделей, например несколько разных трансформеров, а итоговое решение принимается путем голосования или усреднения вероятностей). Кроме того, может проводиться анализ «водяных знаков» (разработчики ИИ, например Open AI, могут внедрять в сгенерированный текст невидимые статистические метки – «водяные знаки»; модель генерирует текст таким образом, чтобы в последовательности слов или их хэшах прослеживался определенный паттерн, незаметный для человека), при этом специальный алгоритм-детектор ищет этот паттерн.

Для распознавания AI-фишинга используют **гибридные** и **комплексные подходы**[151], которые сочетают анализ текста, метаданных и поведенческого контекста и показывают высокую надежность и эффективность. Поскольку одного анализа текста недостаточно, современные системы проводят анализ текста (*NLP*) и анализ контекста поведения (соответствует ли запрос обычной деловой практике), и анализ метаданных (проверка заголовков, времени отправки, IP-адреса отправителя). Фишинговое письмо может быть идеально по тексту, но прийти с подозрительного сервера.

Кроме того, применяется каскадная фильтрация. Сначала письмо проверяется легкими моделями на наличие явных признаков угрозы. Если они проходят проверку, то подключается более тяжеловесная *BERT*-модель.

Таким образом, противостоять письмам, созданным *LLM*, можно только с помощью продвинутых моделей ИИ (в основном *Transformer*-архитектур), которые анализируют не отдельные слова, а контекст, стиль и соответствие обычному поведению отправителя.

Методы машинного обучения для классификации и анализа URL-адресов

Для распознавания фишинговых ссылок также используются различные методы машинного обучения. «Все они условно делятся на несколько категорий: методы анализа характеристик URL, методы анализа содержимого веб-страницы, методы анализа сетевого трафика и гибридные методы»[152].

1. Методы на основе анализа характеристик URL. Эти методы «являются наиболее быстрыми, так как оперируют только строкой URL»153 и не требуют загрузки веб-страницы. Они направлены на выявление аномалий в структуре и синтаксисе адреса. Основные признаки этих методов:

- **Длина URL.** Фишинговые URL часто имеют экстремальные значения длины. С одной стороны, злоумышленники используют очень длинные, запутанные URL со множеством вложенных каталогов и параметров, чтобы скрыть истинный домен. С другой стороны, они используют сервисы сокращения ссылок (bit.ly, goo.gl), чтобы скрыть истинный адрес за коротким, безобидным на вид URL.
- **Количество и глубина поддоменов.** Легитимные сайты обычно используют 1–2 поддомена. Фишинговые сайты часто создают множество вложенных поддоменов, чтобы создать иллюзию принадлежности к известному бренду.

---

[151] Горбачев Ю. Узнайте, как Stacking Transformers с BERT и ансамблевой архитектурой может революционизировать ваш AI-проект! [Электронный ресурс]. URL: https://dzen.ru/a/Z9ROzoQnBwBkHVQQ (дата обращения: 18.04.26).

[152] Лукманова К. А., Картак В. М. Распознавание фишинговых ссылок с использованием методов машинного обучения // Безопасность цифровых технологий. 2024. № 3 (114). С. 9–20.

[153] Лукманова К. А., Картак В. М. Указ. соч. С. 9–20.

- **Наличие подозрительных ключевых слов.** Анализируется строка URL на наличие слов, часто ассоциируемых с действиями по безопасности или социальной инженерией: login, signin, secure, account, verify, update, confirm, banking, paypal, password, credential.
- **Наличие специальных символов.** Некоторые символы в URL используются для маскировки или перенаправления и редко встречаются в адресах легитимных сайтов:
  - символ @ используется для указания имени пользователя и пароля. Современные браузеры часто блокируют такие URL, но они могут использоваться в ссылках;
  - – (дефис) и подчеркивание (_) применяются злоумышленниками для регистрации доменов, похожих на настоящие, где точки заменяются дефисами;
  - % используется для URL-кодирования, причем чрезмерное количество закодированных символов может скрывать истинную структуру URL;
  - // (двойной слеш) после домена может указывать на попытку перенаправления.

Достоинства метода:
- высокая скорость обработки;
- не требует сетевых запросов, что безопасно и не раскрывает аналитику;
- прост в реализации и интерпретации.

Недостатки метода:
- уязвим к запутыванию URL, например, с использованием числовых IP-адресов вместо доменов или методов кодирования;
- низкая эффективность против «нулевых дней» – новых фишинговых сайтов, использующих нестандартные техники;
- высокий уровень ложных срабатываний.

2. Методы на основе анализа содержимого веб-страницы. Эти методы требуют загрузки страницы и анализа ее HTML-кода, текста, изображений и сетевых запросов. Они значительно точнее, но работают медленнее. Основные признаки для анализа:
- **Анализ SSL/TLS-сертификата.** «Проверяется наличие и подлинность сертификата, на какой домен он выдан и как долго действует. Фишинговые сайты часто используют самоподписанные сертификаты или бесплатные сертификаты (Let's Encrypt), выданные на недавно зарегистрированный домен. Если сертификат выдан на IP-адрес, а не на домен – это явный признак фишинга»[154].
- **Анализ соответствия домена содержимому.** Сравнивается домен из URL с брендами, упоминаемыми на странице.
- **Анализ количества и типов внешних ссылок.** Анализируется отношение внутренних ссылок (ведущих на тот же домен) к внешним. Легитимные сайты обычно ссылаются на самих себя. Фишинговые страницы часто являются подделкой и содержат много внешних ссылок на ресурсы злоумышленника.
- **Анализ текста страницы (NLP).** Применяются методы обработки естественного языка (*Natural Language Processing, NLP*) для анализа тональности, тематики и стиля текста. Например, фишинговые страницы, созданные непрофессионалами, часто содержат множество орфографических и грамматических ошибок. **Также может создаваться чувство срочности через** фразы типа «Ваш аккаунт будет заблокирован через 24 часа», «Немедленно подтвердите платеж».

Достоинства метода:
- высокая точность (до 95–99 %);
- устойчивость к запутыванию URL;
- возможность обнаружить фишинговую страницу, даже если ссылка выглядит безопасно.

Недостатки метода:
- требует времени на загрузку и парсинг страницы;
- высокие вычислительные затраты (CPU, память, сетевой трафик);
- уязвим к атакам, когда фишинговая страница динамически подменяется для ботов (боты видят легитимную страницу, а люди – фишинговую).

3. Методы на основе анализа трафика и поведения пользователя. Эти методы не анализируют отдельную ссылку, а изучают взаимодействие пользователя с сайтом или характеристики сетевого потока. Они учитывают ключевые аспекты:
- **Анализ частоты и времени посещений.** Строится профиль обычного поведения пользователя. Если пользователь внезапно начинает часто заходить на неизвестные домены или проводит на них нехарактерно много времени – это аномалия.

[154] Лукманова К. А., Картак В. М. Указ. соч. С. 9–20.

- **Анализ DNS-запросов.** Изучаются запросы к DNS-серверам. Фишинговые домены часто имеют недавнюю дату регистрации (менее 30 дней), короткий TTL (время жизни записи) и ведут на IP-адреса, расположенные в необычных географических регионах.
- **Поведенческая биометрия.** Анализируется то, как пользователь взаимодействует со страницей: скорость движения мыши, нажатия клавиш, скроллинг.

Достоинства метода:

- обнаруживает сложные, медленные атаки;
- может работать в фоновом режиме.

Недостатки метода:

- требует сбора больших объемов данных, что нарушает конфиденциальность;
- высокий уровень ложных срабатываний (изменение поведения пользователя не всегда связано с фишингом);
- не работает для первого посещения сайта.

4. Гибридные и глубокие методы (современный стандарт). Гибридные методы объединяют все вышеперечисленные подходы, а нейросети позволяют автоматически извлекать наиболее релевантные признаки.

- **CNN для анализа URL и HTML.** Сверточные сети «видят» URL как последовательность символов и автоматически выделяют паттерны, которые эксперт может не заметить (например характерные сочетания цифр или букв).
- **RNN/LSTM для анализа последовательности действий.** Рекуррентные сети анализируют последовательность переходов пользователя, историю запросов, временные ряды трафика.
- **Комбинированные модели.** На вход подаются и «ручные» признаки (длина URL, SSL), и «автоматические» признаки (эмбеддинги из CNN). Модель учится взвешивать их значимость.

Таблица 3

Итоговое сравнение методов машинного обучения для классификации и анализа URL-адресов[155, 156,157, 158, 159]

Характеристика	Анализ URL	Анализ контента	Анализ трафика	Гибридные (CNN/RNN)
Скорость	Очень высокая	Низкая	Средняя	Средняя (на GPU)
Точность	Средняя (80–90 %)	Высокая (95–99 %)	Средняя (85–90 %)	Очень высокая (97–99 %)
Обнаружение «нулевых дней»	Плохо	Хорошо	Средне	Отлично
Конфиденциальность	Полная (не загружает страницу)	Низкая (загружает страницу)	Очень низкая (следит за пользователем)	Низкая
Пример применения	Браузерное расширение, прокси-сервер	Корпоративный шлюз безопасности	SIEM-система, UBA	Исследования, облачные антивирусы

Таким образом, на фоне общего роста числа и сложности кибератак, превращения киберпреступности в особую экономическую отрасль, массовом использовании злоумышленниками технологий искусственного интеллекта продолжает наблюдаться устойчивый рост инцидентов с использование методов социальной инженерии и, в частности, фишинга. В настоящей статье были исследованы ключевые характеристики и векторы развития современных целевых фишинговых атак. Было показано, что сегодня фишинг зачастую выступает начальным звеном сложных составных кибератак.

Для обнаружения и предотвращения целевых фишинговых угроз наиболее эффективным инструментом на сегодняшний день становятся методы машинного обучения. Для решения задач противодействия фишингу они используются по нескольким направлениям. В настоящей статье был проведен общий разбор наиболее важных из этих направлений: анализ контента электронных сообщений, анализ URL-адресов, методы борьбы с AI-фишингом. Для решения подобных задач могут применяться различные алгоритмы машинного обучения (*ML* и *DL*). Проведенный сравнительный анализ этих методов показал, что методы на основе трансформеров (модели по типу *BERT*) являются

[155] Classifying phishing URLs using recurrent neural networks / A. C. Bahnsen, I. D. Torroledo, J. Camacho, S. Villegas // 2017 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2017.

[156] Machine learning based phishing detection from URLs / O. K. Sahingoz, E. Buber, O. Demir, B. Diri // Expert Systems with Applications. 2019. Vol. 117. P. 345–357.

[157] Лукманова К. А., Картак В. М. Векторное представление слов в задачеанализа текстовых сообщений // Мавлютовские чтения : XIV Всероссийская молодежная научная конференция. Уфа, 2020. Т. 5, Ч. 2. Ст. 25.

[158] Артюшкина Е. С., Андирякова О. О., Тюрина Д. А. Использование методов машинного обучения при анализе сетевого трафика и вредоносного программного обеспечения // Индустриальная экономика. 2023. № 4. С. 12–15.

[159] Мухамадиева К. Б., Муминов Б. Б. Обзор методов обнаружения фишинговых атак на основе искусственного интеллекта // Вестник Донецкого национального университета. Серия Г: Технические науки. 2021. № 4. С. 37–45.

универсальными (способны решать разнообразные задачи в борьбе с фишингом), демонстрируют максимальную точность и адаптивность к постоянно меняющимся угрозам, но при этом более ресурсоемки и медлительны.

В статье показано, что целесообразным является интеграция различных методов машинного обучения и использование гибридных методов для обнаружения и предупреждения фишинговых угроз, в том числе созданных с помощью технологий искусственного интеллекта. В связи с этим необходимо акцентировать внимание на системном подходе к выбору признаков для обнаружения целевого фишинга, что позволяет увеличить эффективность систем защиты, уменьшить их стоимость и время работы.

П. В. Лушников,
старший преподаватель кафедры теории и истории государства и права
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Герменевтический аспект информационной безопасности

Герменевтика является одним из первых древнейших философских и научных направлений, изучающих понимание, интерпретацию, контексты информации, получаемой человеком.

С древности понимание и толкование правовой действительности является одним из базовых направлений деятельности юристов. Поэтому герменевтические знания и методология используется в юриспруденции достаточно давно.

Понимание рассматривается в герменевтике и как процесс постижения смысла, заложенного в тексте автором, и как результат (состояние), достигнутый читателем после интерпретации.

В герменевтике выделяют три роли участников общения – автор, текст и читатель. В теории коммуникации и теории информации используются схожие категории – адресант, послание, адресат. Отличие заключается в том, что в теории коммуникации речь идет в первую очередь о путях, способах и средствах передачи информации, а в герменевтике речь идет о содержании передаваемой информации, о ее восприятии, интерпретации и понимании.

Движение информации между этими участниками образует коммуникативную модель, которую называют «герменевтический треугольник[160]». Автором статьи на основе этой модели было осуществлено дальнейшее моделирование коммуникативного взаимодействия. В результате изменения структуры герменевтического треугольника и рассмотрения происходящих в нем процессов в динамике автор открыл такое явление, как «герменевтическое сообщество»[161].

Такое сообщество рассматривается и как среда, в которой действуют единые для всех членов конвенции понимания, и как самостоятельный участник коммуникации.

В качестве элементов ГСО автор статьи выделяет: коллективность, информацию, коммуникативное взаимодействие. Для сравнения: в теории системы в качестве элементов системы выделяют также три элемента: массу, информацию, энергию. Совпадение элементов позволяет говорить о системности герменевтического сообщества.

Коллективность предполагает существование группы людей, которые объединены между собой необходимостью и потребностью в общении и взаимодействии. Причастность к сообществу проявляется через самоидентификацию членов.

Информация – это не просто данные (сведения), а смыслы, которые заложены в текст автором и возникают в процессе взаимодействия читателя с текстом. Информацию, циркулирующую в сообществе, можно разделить на базовую и текущую. Базовая – включает в себя картину мира (знания, мудрость, ценности и традиции) и создаваемую на ее основе культуру (в широком смысле). Текущая – это информация, необходимая для постоянного общения между участниками либо передаваемая между участниками в ходе обычного общения.

Коммуникативное взаимодействие (взаимосвязи) – это пути, средства, правила коммуникации (модели коммуникации). Основным средством общения являются языки, которые выступают

[160] См.: Лушников П. В. Правовая коммуникация и её участники: теоретический аспект // Вестник Удмуртского университета. Серия «Экономика и право». 2019. Т. 29, № 3. С. 369–378.

[161] См.: Лушников П. В. Герменевтическое сообщество в правовой коммуникации // Государство и право России в современном мире : сб. докладов XII Московской юридической недели : в 5 ч. М., 2023. С. 92–97.

не только средством общения, они также являются базой картины мира сообщества. В сообществе существуют правила взаимодействия.

Герменевтическое сообщество может не совпадать с границами государства, выходить за них, либо в пределах одного государства может быть несколько герменевтических сообществ. Одно большое сообщество может делиться на подсообщества.

Существование людей связано с конфликтами, которые имеют различные причины, ход протекания и результаты. Конфликты изучаются разными науками.

В герменевтике также рассматриваются конфликты между участниками коммуникации: конфликт между автором и читателем о первоначальном смысле текста, конфликт между разными читателями о правильности интерпретации и понимании текста.

Полагаем, что конфликты в коммуникативном и герменевтическом аспекте могут быть направлены на понимание (как состояние) – на навязывание определенных интерпретаций, на формирование картины мира. И на понимание (как процесс) – на передачу смыслов, на определение моделей коммуникации. Конфликты, связанные с существованием коммуникации, нацелены на прерывание коммуникации или изменение коммуникации. Прерывание может быть осуществлено путем исключения участника из коммуникативного взаимодействия. А изменение возможно путем замены участников или изменение движения информации.

Рассмотрение конфликтов в герменевтическом аспекте наталкивает на мысль о применении герменевтических знаний при изучении проблематики информационной безопасности. Так как существование герменевтического сообщества сопряжено с движением информации, то можно говорить об информационной безопасности такого сообщества.

Герменевтическое сообщество стремится к сохранению себя (своей целостности и самобытности) и к воспроизводству (сохранению количества членов и увеличению численности). Отсюда можно увидеть основные конфликты, связанные с сохранением самостоятельности (суверенности) и с определением численности членов сообщества. Такие конфликты могут быть внешними – между герменевтическими сообществами, и внутренними – между членами сообщества.

Конфликт в герменевтическом сообществе протекает с задействованием всех его элементов (коллектива, информации и взаимосвязей).

Коллективность и границы сообщества обеспечиваются за счет идентичности членов, она создается через формирование и навязывание культурных кодов, через механизм разграничения «свой-чужой».

Картина мира сообщества позволяет оптимально существовать и эффективно реализовывать свои интересы, в том числе за счет вытеснения «чужой» информации и навязывания своей.

Коммуникативное взаимодействие, формируя общую среду общения, позволяет за счет создания устойчивых коммуникативных моделей качественно обмениваться необходимой информацией, сохранять целостность сообщества, исключать недостоверные и чужие источники информации.

Из сказанного можно увидеть существование в сообществе механизмов сохранения (поддержание единства и целостности) и противоборства (защиты и нападения).

В научной литературе широко используется термин «информационная война». При этом единого определения этого понятия нет, это говорит о многоплановости и многомерности данного феномена.

А. А. Мушта, А. В. Баранов определяют ее как «противоборство между двумя государствами или группами государств в информационном пространстве в целях нанесения ущерба государственным информационным системам, процессам и ресурсам, критически важным и другим объектам; подрыва политической, экономической и социальной систем; массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны». Они также указывают, что эта война «представляет собой совокупность мероприятий, проводимых в информационном пространстве в интересах достижения информационного превосходства»[162].

В последнее время в военной науке выделился еще один термин «Ментальная война». Такая война направлена на уничтожение/изменение самосознания членов общества противника, изменение ментальной (цивилизационной) основы этого общества. Это определение интегрирует несколько понятий (прокси-война, гибридная и информационная война) и наиболее близко к понятию когнитивной войны (война ценностей, мировоззрения, идеологии). «Ментальная война – это скоординированная совокупность разномасштабных действий и операций, направленных на «оккупацию» сознания противника в целях паралича его воли, изменения индивидуального и массового сознания населения

[162] Мушта А. А., Баранов А. В. Информационная война // Большая энциклопедия [Электронный ресурс]. URL: https://bigenc.ru/c/informatsionnaia-voina-2b7815 (дата обращения: 12.01.2026).

для деморализации армии и общества, уничтожения духовно-нравственных ценностей, традиций и культурно-исторических основ государства, «стирания» национальной идентичности народа[163]».

Российский исследователь С. Б. Переслегин вводит понятие «Герменевтическое управление» – управление пониманием. Оно включает в себя несколько типов управления: семантическое, онтологическое, эпистемологическое. Семантическое – управление семантикой, языком, контроль над информационным пространством. Онтологическое управление – управление картиной мира. И эпистемологическое управление как управление представлениями об истинности[164].

Такое управление направлено на поддержание своей организованности и разрушение чужих организованностей путем поддержания своего состояния понимания, контроля за ним и разрушения чужих идентичности и культурных кодов. Такое информационное воздействие можно рассматривать как оружие массового поражения. Оно осуществляется через монополизацию информационного пространства и установление контроля над ним[165].

Таким образом можно говорить о герменевтическом воздействии на сообщество. Оно может быть направлено на уничтожение герменевтического сообщества или изменение его элементов с целью исключения сопротивления его членов и их дальнейшего подчинения (включения) своему сообществу. Достигается это за счет монополизации информационного пространства – возможность быть первичным (достоверным) источником информации, и путем установления контроля за коммуникациями – средствами и каналами распространения информации.

Воздействие может быть направлено на структуру герменевтического треугольника через изменение или исключение базовых авторов, базовых текстов, основных читателей. В герменевтическом сообществе направлением воздействия будут элементы сообщества – коллектив, информация, коммуникации.

Обеспечение информационной безопасности в герменевтическом аспекте имеет несколько направлений:

- сохранение самостоятельности и целостности сообщества;
- сохранение и увеличение количества членов сообщества;
- защита идентичности его членов;
- защита картины мира;
- защита текущей информации от избыточности;
- сохранение структуры коммуникаций;
- защита средств и каналов коммуникации.

Средства нападения и средства защиты во многом совпадают. Классическими инструментами информационной войны являются дезинформация, шифрование нужной информации, информационные ловушки, создание информационного шума и др.

Средствами герменевтического противоборства будут создание «ложных» авторитетов, внушение информационного, морального превосходства; умаление достоинств сообщества, преувеличение его недостатков; упрощение информации или подмена сложной более легкой информации; изменение средств интерпретации текстов; замусоривание информационного пространства ненужной информацией; отрицание, запрет, умаление опасной информации; активное замалчивание вредной или важной информации; использование альтернативных моделей коммуникации.

Оппоненты нашей страны хорошо знакомы с данным видом социального противоборства и активно используют его инструментарий. Они начали разрабатывать и применять эти знания во времена колонизации при взаимодействии с местными жителями и рабами. Используя военное и экономическое могущество, оппоненты навязывали свое информационное, моральное, культурное превосходство и внушали неполноценность и второсортность.

Эти же приемы были применены в отношении нашей страны. Положительно то, что в последние годы в руководстве нашего государства возникло понимание важности защиты ментальной сферы (сферы базовых смыслов) для сохранения и развития нашей страны. Были приняты нормативные акты, направленные на сохранение традиционных ценностей и защиту нашего герменевтического сообщества[166].

---

[163] Ментальная война // Рувики [Электронный ресурс]. URL: https://ru.ruwiki.ru/wiki/Ментальная_война (дата обращения: 12.01.2026).

[164] Переслегин С. Б. Диктатор и революция. Семантическое управление [Электронный ресурс]. URL: https://vk.com/wall-11898452_5559 (дата обращения: 12.11.2022).

[165] Переслегин С. Б. Лингвоинженерия. Семантическое оружие. [Электронный ресурс]. URL: https://yandex.ru/video/preview/1856846405958638996 (дата обращения: 12.11.2022).

[166] О государственном языке Российской Федерации : Федеральный закон от 01.06.2005 № 53-ФЗ (ред. от 22.04.2024) // Парламентская газета. 2005. № 100; Об утверждении Основ государственной политики по сохранению и укреплению тради-

В последние несколько десятилетий идет глобализация мира, которая связана в том числе с тем, что английский язык стал языком международного общения. При этом в нашей стране появилось уродливое явление, которое нами было названо «рунглиш»[167].

По иронии язык, как и воздух, не воспринимается как ценность или что-то важное. Лингвисты говорят, что ничего плохого в англоизации нет, что русский язык все переплавит и переварит. Но проблема не плавительных и переварительных способностях нашего языка. Язык – это не только средство коммуникации, это ключ к картине мира нашего сообщества, к его культурному наследию и истории. Использование чужого языка там, где можно использовать свой, разрушает картину мира нашего герменевтического сообщества, умаляет ценность своей культуры, нарушает коммуникативные модели. У членов сообщества происходит утрата идентификации с сообществом и примитивизация мыслительных и коммуникативных процессов.

Все это ведет к появлению колониальной психологии второсортных людей. Оно исключает стимул для социального развития и самосовершенствования. Автор статьи наблюдает, как у определенной части нашего сообщества сформировалась ложная установка – «наш ментальный, интеллектуальный уровень невысокий, наша культура неполноценна и второсортна, зачем что-то придумывать и делать самим, если есть те, кто нас превосходят, мы никогда не сможем их превзойти, они сделают все нужное, мы потом возьмем (купим, скопируем) у них». Очевидно, что общество, не говорящее на своем языке и не имеющее своей картины мира, обречено на исчезновение.

Современный мир становится сложнее, появляется множество новых явлений, событий и вещей. Поэтому следующим шагом для сохранения ментального суверенитета должно стать внутреннее развитие языка. Полагаем, что происходящее в настоящее время изменение страны должно сопровождаться изменением языка и появлением слов и словосочетаний, которые бы нашим языком описывали новые явления, события и вещи.

Средством юридической защиты языка является упорядочение и ограничение употребления иностранных слов и выражений в официальной и деловой речи, ограничение заимствований, создание механизмов формирования и «узаконивания» новых русских слов.

Подводя итог сказанному, укажем, что одним из существенных направлений информационной безопасности должно стать сохранение герменевтического сообщества нашей страны и российской цивилизации и противодействие информационному колониализму. С одной стороны, нужно дать возможность развиваться герменевтическому сообществу, с другой стороны, нужно защитить его самобытность, картину мира и средства коммуникации.

Д. М. Хурамшин,
начальник связи и автоматизированных систем Управления ФКУ «Военный комиссариат Удмуртской Республики», г. Ижевск

Правовые механизмы обеспечения информационной безопасности в условиях цифровой трансформации государства

В настоящее время цифровая трансформация государства выступает не просто направлением обновления публичного управления, а самостоятельным фактором изменения правового режима информационных отношений. Расширение электронного взаимодействия между органами власти, внедрение государственных информационных систем, платформенных решений, технологий больших данных и отдельных инструментов искусственного интеллекта повышают оперативность управленческих процессов, но одновременно создают новые риски в сфере информационной безопасности. В Доктрине информационной безопасности Российской Федерации прямо указано, что внедрение информационных технологий без их надлежащего сопряжения с мерами защиты повышает вероятность реализации информационных угроз.

ционных российских духовно-нравственных ценностей : Указ Президента РФ от 9 ноября 2022 г. № 809 [Электронный ресурс]. URL: pravo.gov.ru.

[167] По аналогии с возникшими в Британии с ироничными терминами «пакиш» и «индиш» – исковерканная, уродливая форма английского языка, на которой говорят малограмотные выходцы из Пакистана и Индии.

Актуальность темы определяется тем, что в условиях цифровизации государство одновременно выступает крупнейшим оператором данных, владельцем социально значимых информационных систем и субъектом публично-правовой обязанности по обеспечению защиты информации, прав граждан и устойчивости цифровой инфраструктуры. Вместе с тем действующее законодательство, несмотря на значительный объём нормативных предписаний, не всегда успевает адаптироваться к темпам технологических изменений, что приводит к пробелам, коллизиям и несогласованности отдельных регулятивных решений.

Цель статьи состоит в анализе правовых механизмов обеспечения информационной безопасности в процессе цифровой трансформации государства, выявлении проблем действующего регулирования и выработке предложений по его совершенствованию. Научная новизна исследования заключается в обосновании необходимости перехода от разрозненного отраслевого регулирования к комплексной риск-ориентированной модели правового обеспечения информационной безопасности в системе государственного управления.

Цифровая трансформация государства представляет собой комплексный процесс изменения форм, методов и технологий реализации публичной власти на основе применения цифровых решений. По существу, речь идет не только о переводе государственных услуг в электронный вид, но и о реорганизации всей системы публичного администрирования, включая межведомственное взаимодействие, принятие управленческих решений, хранение и обработку данных, идентификацию субъектов и контрольные процедуры. Базовые правовые категории информации, информационных технологий и защиты информации закреплены в Федеральном законе «Об информации, информационных технологиях и о защите информации»[168].

Правовое значение цифровой трансформации состоит в том, что она меняет сам предмет регулирования. Если ранее основное внимание уделялось документу, архиву, локальной системе и должностному лицу, то в цифровой среде в центр правового воздействия выходят данные, алгоритмы, распределенные системы, платформы и цифровые следы. В результате информационная безопасность перестает рассматриваться исключительно как техническая функция и приобретает значение самостоятельного элемента правового обеспечения устойчивости государственного управления.

Одновременно цифровая трансформация усиливает зависимость государственного управления от устойчивости информационных систем. Нарушение функционирования государственных цифровых сервисов способно повлечь не только технический сбой, но и дестабилизацию реализации публичных полномочий, ограничение прав граждан, срыв административных процедур и снижение доверия к институтам власти. Указанное обстоятельство особенно значимо применительно к объектам критической информационной инфраструктуры[169].

В условиях цифровой трансформации государства расширяется спектр угроз информационной безопасности. Их особенностью является сочетание технологического и правового содержания: практически любая современная информационная угроза одновременно затрагивает вопросы режима информации, ответственности, компетенции органов власти, допустимости обработки данных и соблюдения прав граждан.

К числу наиболее значимых угроз относятся несанкционированный доступ к государственным информационным ресурсам, утечки персональных данных, вредоносное воздействие на информационные системы, нарушение доступности государственных цифровых сервисов, а также компрометация значимых объектов критической информационной инфраструктуры. Правовое значение таких угроз определяется тем, что они посягают не только на сведения как объект защиты, но и на законные интересы личности, общества и государства. Федеральный закон «О персональных данных» прямо ориентирован на защиту прав и свобод человека при обработке персональных данных[170].

Особую опасность представляют многоуровневые инциденты, возникающие вследствие сочетания организационных, программных и правовых просчетов. Современная угроза информационной безопасности нередко проявляется не в форме единичного неправомерного доступа, а как системный результат недостаточной правовой координации, размытости компетенций, несогласованности режимов доступа и отсутствия единых требований к межведомственному обмену данными.

Система правового регулирования обеспечения информационной безопасности в Российской Федерации носит комплексный характер и включает нормы конституционного, информационного,

---

[168] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

[169] О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ // Собрание законодательства РФ. 2017. № 31 (ч. 1). Ст. 4736.

[170] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

административного, уголовного и иных отраслей права. Ее основу составляют положения Конституции Российской Федерации о защите прав и свобод человека, неприкосновенности частной жизни, свободе поиска, получения, передачи и распространения информации законным способом, а также об обязанности государства обеспечивать безопасность личности, общества и государства.

Отраслевую основу регулирования формируют Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон № 152-ФЗ «О персональных данных», Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также Доктрина информационной безопасности Российской Федерации. Указанные акты регулируют, соответственно, общие отношения в информационной сфере, порядок и принципы обработки персональных данных, обеспечение безопасности значимых объектов критической информационной инфраструктуры и стратегические ориентиры государственной политики в информационной сфере.

Вместе с тем действующее регулирование во многом сохраняет секторальный характер. Нормы о защите информации, персональных данных, государственной тайне, критической инфраструктуре, связи, электронном документообороте и государственных информационных системах развиваются параллельно, не всегда образуя единый и внутренне согласованный механизм. На практике это приводит к ситуации, когда формально правовые требования существуют, но их применение осложняется множественностью источников и различием правовых режимов.

Существенным недостатком современного законодательства остаётся его фрагментарность. Несмотря на наличие значительного массива нормативного материала, единый концептуально согласованный механизм правового обеспечения информационной безопасности в условиях цифрового государства пока не сложился. Отдельные акты регулируют самостоятельные сегменты информационной сферы, но не всегда образуют между собой устойчивую и логически завершённую систему.

Не менее заметна и другая проблема: технологическое развитие идёт быстрее, чем формируется адекватное правовое регулирование. Законодательство объективно не всегда успевает учитывать последствия внедрения больших данных, алгоритмических систем принятия решений, распределённого хранения информации, облачной инфраструктуры и иных цифровых решений. В результате правоприменительная практика либо расширительно толкует уже действующие нормы, либо сталкивается с состоянием регуляторной неопределённости.

Отдельного внимания требует недостаточная разработанность механизмов распределения ответственности между участниками цифрового взаимодействия. В современных условиях в процессы обработки и передачи информации могут одновременно быть вовлечены государственный орган, подведомственная организация, оператор информационной системы, внешний разработчик, центр обработки данных и иные субъекты. Однако законодательство не всегда достаточно ясно определяет пределы их обязанностей и основания юридической ответственности при возникновении инцидентов информационной безопасности.

Проблемным остаётся и вопрос институциональной увязки информационной безопасности с процессами цифровой трансформации. На практике цифровое развитие нередко воспринимается прежде всего как задача ускоренного внедрения технологий, тогда как правовое сопровождение и обеспечение безопасности рассматриваются как вторичное направление. Подобный подход снижает устойчивость цифровых решений и повышает риск системных сбоев при реализации публичных функций.

Совершенствование правовых механизмов обеспечения информационной безопасности в условиях цифровой трансформации государства целесообразно выстраивать по нескольким взаимосвязанным направлениям.

Во-первых, требуется переход к риск-ориентированной модели регулирования, при которой требования к защите информации будут определяться не только формальной принадлежностью системы к той или иной категории, но и характером обрабатываемых данных, масштабом потенциального ущерба, уровнем межведомственной интеграции и степенью влияния конкретной системы на реализацию публичных функций.

Во-вторых, необходима более последовательная систематизация нормативной базы в сфере информационной безопасности. Речь не обязательно должна идти о принятии единого кодекса, однако требуется сформировать согласованную законодательную конструкцию, объединяющую требования к государственным информационным системам, защите персональных данных, межведомственному обмену сведениями, критической инфраструктуре и юридической ответственности за нарушения в цифровой среде. Кроме того, представляется оправданным нормативно закрепить принцип «безопасность по проекту», при котором требования информационной безопасности учитываются уже на стадиях разработки, закупки, модернизации и ввода цифрового решения в эксплуатацию.

В-третьих, необходима более чёткая регламентация распределения компетенции и ответственности между государственными органами, операторами систем, подрядчиками и иными участниками цифровой инфраструктуры. Это позволит сократить зоны правовой неопределённости и сделать юридическую ответственность более адресной.

В-четвёртых, следует развивать обязательные процедуры правовой и организационной оценки цифровых решений, включая экспертизу проектов нормативных актов и государственных информационных систем с точки зрения их влияния на права граждан, режим защищаемой информации и устойчивость государственного управления.

Таким образом, развитие правовых механизмов обеспечения информационной безопасности должно быть ориентировано не только на усиление охранительных мер, но и на формирование целостной модели безопасного функционирования цифрового государства. В этом заключается основной научно-практический вывод проведённого исследования.

С. Д. Рубинович,
ведущий специалист по защите информации
АУ «Центр Цифровых технологий Удмуртской Республики»,
магистрант, «Экономика (Учетные технологии в сфере управления бизнесом)»,
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Оптимизация работы SIEM-систем на базе ИИ: методы снижения ложноположительных срабатываний

Программное обеспечение, которое в реальном времени собирает, агрегирует, нормализует и анализирует данные (логи и события) от множества различных источников в инфраструктуре компании (серверы, сетевые устройства, базы данных, приложения, антивирусы, межсетевые экраны) – так упрощенно можно описать работу SIEM-системы[171] (Security Information and Event Management).

Все чаще технологии искусственного интеллекта (ИИ) и машинного обучения (МО) применяются для обработки большого количества событий информационной безопасности (ИБ), которое в крупной корпоративной сети может достигать нескольких миллионов в сутки. Обработать такой объем данных вручную невозможно. ИИ обладает уникальными возможностями для анализа больших данных, выявления закономерностей и адаптации к изменяющимся условиям, что делает его идеальным инструментом для оптимизации SIEM-систем. Современные SIEM-системы работают не просто по жестким, заранее заданным правилам, а используют поведенческий анализ. ИИ пытается самостоятельно понять, что является «нормальным» поведением для сотрудников и системы в целом, и срабатывает, когда видит значимые отклонения от этой нормы.

Однако у такого подхода есть серьезный недостаток. Система достаточно часто ошибается, принимая обычные рабочие действия за нарушение. Эти ошибки называют «ложноположительными срабатываниями» (от англ. False Positive, FP) или просто ложными тревогами. Масштаб проблемы впечатляет: по некоторым оценкам аналитики центров мониторинга (SOC) вынуждены тратить примерно до 70–80 % своего рабочего времени на расследование алертов (тревог), которые в итоге оказываются ложными.

1. *Природа ложноположительных срабатываний в системах с ИИ.* Для того чтобы понять, как бороться с ложными срабатываниями нужно ввести и объяснить несколько ключевых понятий, лежащих в основе работы систем защиты.

1.1. *«Брутфорс» и другие угрозы, которые выявляет SIEM.* Одна из самых распространенных и известных атак называется «брутфорс» (от англ. brute force – «грубая сила»). Это метод взлома, при котором злоумышленник пытается подобрать пароль к учетной записи, перебирая все возможные комбинации символов. Для SIEM-системы признаком брутфорс-атаки является огромное количество неудачных попыток входа в систему за очень короткий промежуток времени.

Однако существуют и гораздо более сложные и скрытные атаки, для обнаружения которых ИИ как раз и предназначен. Например, атака через «смежные доверенные связи». Злоумышленник,

[171] SIEM-системы: построение эффективной защиты информации в корпоративных сетях [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/razrabotka-modeli-zaschity-informatsii-korporativnoy-seti-na-osnove-vnedreniya-siem-sistemy

взломав один незначительный компьютер (например, в бухгалтерском отделе), начинает незаметно перемещаться по корпоративной сети, выдавая себя за легитимного сотрудника, чтобы добраться до ценных данных в финансовом отделе. Человек-аналитик отследить такое многоходовое поведение в миллионах событий практически не в силах, а вот ИИ, проанализировав нетипичные сетевые связи между компьютерами, может заподозрить неладное.

1.2. *Что такое «ложноположительное срабатывание» и почему это не просто «ошибка»*. Ложноположительное срабатывание (False Positive, FP) – ситуация, когда система защиты ошибочно классифицирует легитимное, разрешенное действие пользователя или процесса как вредоносное и создает тревогу (инцидент). Проще говоря, это «ложный вызов».

Даже самая совершенная SIEM-система остается уязвимой перед «человеческим фактором» и форс-мажорными обстоятельствами. Рассмотрим пример типовой ситуации, которая способна приостановить работу целого центра мониторинга безопасности (SOC).

Представим обычную организацию, в которой внезапно произошло аварийное отключение электропитания. После восстановления подачи электроэнергии запускается стандартный процесс восстановления инфраструктуры: серверы, сетевое оборудование и рабочие станции сотрудников начинают одновременную перезагрузку. С точки зрения SIEM-системы происходящее выглядит как классическая скоординированная брутфорс-атака (подбор паролей):

1) сотни устройств одновременно генерируют события входа в систему;
2) пользователи, не помнящие пароли наизусть, совершают несколько неудачных попыток ввода;
3) почтовые клиенты, мессенджеры и внутренние сервисы также пытаются переподключиться, создавая лавину неудачных запросов на авторизацию.

Правила корреляции SIEM, настроенные на выявление перебора паролей, срабатывают множество раз. Система в таком случае генерирует тысячи ложных тревог высшего приоритета. Аналитики центра мониторинга (SOC) оказываются полностью загружены, потому что они вынуждены вручную разбирать поток инцидентов, пытаясь отличить реальную атаку от последствий технического сбоя.

Пока команда реагирования перегружена обработкой ложных срабатываний, вызванных отключением света, реальная, тщательно спланированная атака профессиональных хакеров имеет все шансы остаться незамеченной.

1.3. *Три основные причины ложных тревог.* Проанализировав работу центров мониторинга (SOC) и изучив практику эксплуатации таких популярных систем, как MaxPatrol SIEM[172] и KUMA[173], можно выделить три главные группы причин возникновения ложных срабатываний.

1) *«Живой человек – не робот».* Поведенческий анализ, лежащий в основе ИИ, строит так называемый «профиль нормальности» для каждого пользователя, хоста или приложения. Система запоминает, что сотрудник обычно работает с 8 до 17 часов и никогда не копирует большие объемы данных на внешние носители, но однажды сотруднику нужно сдать годовой отчет. Он приходит на работу в 7 утра, чтобы никто не отвлекал, и скачивает на флешку огромную таблицу с сервера. ИИ фиксирует, что время нерабочее, действие (копирование) нехарактерное для данного пользователя, а значит, это явная аномалия.

Отсюда следует причинно-следственная связь: Система генерирует тревогу высшего приоритета «Потенциальная кража данных», но сотрудник просто выполняет свою работу.

2) *«Мир меняется, а ИИ – нет».* В среде ИБ-специалистов это называется «дрейф концепт» (Concept Drift)[174]. Это изменение статистических свойств данных и самого понятия «нормы» с течением времени. Проще говоря, то, что считалось однозначной аномалией вчера, сегодня может стать абсолютной нормой и наоборот.

Один из примеров показывает, «дрейф концепт» – это пандемия COVID-19. До 2020 года массовые подключения к корпоративной сети из домашних сетей в вечернее и ночное время были практически стопроцентным признаком компрометации учетной записи. С 2020 года это стало нормой. Если модель ИИ не переучить на новые условия, то система будет выдавать ошибки и блокировать пользователей на начальных этапах работы.

3) *«Система не знает всего».* Очень часто ложное срабатывание возникает из-за отсутствия контекста. SIEM-система видит отдельное событие, но не понимает общей картины. Например, зафиксирован успешный вход в корпоративную систему из другой страны. Для SIEM, настроенной

[172] Документация MaxPatrol SIEM [Электронный ресурс]. URL: https://ptsecurity.com/about/docs/

[173] Документация Kaspersky Unified Monitoring and Analysis Platform [Электронный ресурс]. URL: https://support.kaspersky.com/kuma

[174] Дрейф концепт [Электронный ресурс]. URL: https://www.itsec.ru/

на работу в России, это критическое событие и явный признак взлома учетной записи, но в системе не прописано, что сотрудник находится за границей и подключился удаленно для работы.

2. *Методы снижения ложных срабатываний: как сделать так, чтобы ИИ работало точнее*. Для решения проблем, возникающих с ложноположительными срабатываниями, предлагается использовать системный подход, сочетающий в себе как технические решения, так и организационные меры. Такой поход является гибридным, поскольку объединяет в себе конкретные, но гибкие алерты (правила) и алгоритмы машинного обучения.

2.1. *Предварительная фильтрация и нормализация правил (Pre-filtering).* Первый и самый базовый этап – обработка событий, ведь цель данной задачи отсеять заведомо «шумовые» события, которые не несут никакой смысловой нагрузки с точки зрения безопасности, еще до того, как они попадут в раздел срабатывания. Это позволит кардинально снизить общую нагрузку на систему на самом раннем этапе.

К основным методам предварительной фильтрации относятся:

1) *Агрегация повторяющихся событий.* Тысячи абсолютно одинаковых событий от одного источника за секунду (например служебная проверка доступности сетевого порта) «сворачиваются» в одно событие, но с информацией о количестве повторений. Вместо 10 000 срабатываний система видит одно.

2) *Фильтрация по «белым спискам».* Целенаправленное исключение из анализа событий от доверенных и заведомо безопасных источников или событий определенных типов (например легитимное сканирование уязвимостей отделом ИБ).

3) *Пороговая фильтрация.* Игнорирование событий, чьи параметры не превышают заранее установленный, безопасный порог (например, загрузка процессора выше 95 % в течение менее 30 секунд не считается аномалией, так как это может быть кратковременным событием).

2.2. *Обогащение контекстом.* На первых этапах необходимо научить SIEM понимать «организационный контекст», то есть получать и обрабатывать данные из кадровой системы и систем документооборота: график работы сотрудников, приказы на командировки, графики отпусков. Если SIEM будет знать, что сотрудник находится в командировке и работает в нестандартное для системы время, его вход не вызовет ложной тревоги. Если система будет знать, что у бухгалтера сегодня отчет, то его работа допоздна и скачивание больших массивов данных будут расцениваться не как аномалия, а как бизнес-норма.

2.3. *Несколько ИИ в работе.* Вместо того чтобы полагаться на одну единственную модель ИИ для обнаружения всех типов угроз, предлагается использовать несколько. Каждая система смотрит на проблему со своей стороны, и только потом вся информация объединяется и выносится на дашборд. Такой подход кратно повышает точность диагностики и надежность системы в целом.

2.4. *Обратная связь: ИИ учится на ошибках аналитиков.* Самый важный и, пожалуй, ключевой метод для борьбы с дрейф концептом и постоянного повышения точности. ИИ должен непрерывно учиться на действиях человека-эксперта. В современных реалиях выстраивается следующий непрерывный цикл:

1) SIEM генерирует алерт (правило);

2) аналитик SOC берет этот алерт в работу и проводит тщательное расследование;

3) в результате расследования аналитик выносит однозначный вердикт и фиксирует его в системе: «Да, это реальный инцидент» (True Positive) или «Нет, это ложная тревога» (False Positive);

4) этот вердикт автоматически отправляется обратно в систему в качестве «правильного ответа», эталонной разметки;

5) модель ИИ периодически (например раз в неделю) переобучается заново, учитывая все новые, размеченные человеком данные.

Таким образом, система постоянно и динамично адаптируется к любым изменениям.

Проблема ложных срабатываний в системах информационной безопасности на базе искусственного интеллекта – фундаментальный фактор, напрямую и самым серьезным образом влияющий на способность организации защищать свои конфиденциальные данные, неукоснительно соблюдать требования закона и эффективно расследовать инциденты, привлекая виновных к ответственности.

Проблему высокого уровня ложноположительных срабатываний в SIEM-системах можно и нужно решать не отказом от поведенческого анализа, а его интеллектуальной «тонкой настройкой» и дополнением.

Перспективным направлением дальнейших исследований является разработка и внедрение методов искусственного интеллекта для SIEM-систем, чтобы аналитик всегда понимал, почему модель приняла то или иное решение. Это еще больше повысит доверие к системе, качество и скорость расследований инцидентов.

Е. А. Яковлева,
ассистент кафедры информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Формирование доверия к квантовым технологиям в контексте современных вызовов информационной безопасности

В условиях развития информационных технологий особое значение представляют квантовые технологии. Эта быстро развивающаяся отрасль, представляющая особый интерес не только в праве, но и в информационной безопасности. С помощью квантовых технологий сегодня при работе с большими данными можно решать многие задачи: сложные вычисления, создание защищенных каналов, защита больших данных от несанкционированного доступа, развитие инфраструктуры и многое другое. На сегодняшний день лидерами по использованию квантовых технологий являются США, Китай, Канада, а также Россия[175].

Под *квантовыми технологиями* стоит понимать «технологии, в основе которых лежит использование квантовых систем и их свойств»[176]. Межпарламентская Ассамблея государств – участников СНГ определяет квантовые технологии как технологии, в которых специфические свойства квантовой механики используются для создания сверхбыстрых компьютеров[177]. Вместе с тем ряд авторов понимают квантовые технологии как «квантовые технологии – это совокупность процессов, средств, методов сбора, обработки и передачи данных с использованием квантовых явлений (квантовых эффектов)»[178].

Квантовые технологии построены на квантовых явлениях, что позволяет обрабатывать информацию на высоком уровне. Как отметил Михаил Мишустин, «Квантовые коммуникации – это перспективное направление, и для его дальнейшего развития необходимо создать благоприятную регуляторную среду, исключить барьеры, которые тормозят такие процессы»[179]. В связи с этим Правительство РФ утвердило Концепцию регулирования отрасли квантовых коммуникаций в России до 2030 г., которая предлагает совершенствовать существующую регуляторную среду на основе баланса интересов человека, общества и государства, обеспечивая высокий уровень информационной безопасности[180].

Как отмечено в дорожной карте, «Квантовые коммуникации: технологии, направленные на устранение угрозы информационной безопасности, в том числе со стороны квантовых компьютеров, включают использование свойств квантовых систем для передачи ключей. Основная технология – квантовое распределение ключей (КРК). Главное преимущество КРК – защищенность информации, гарантированная законами физики»[181]. Квантовые технологии в себя включают[182]:

– Квантовые вычисления – это вычислительные системы, использующие для решения задач квантовые явления.

– Квантовые сенсоры и метрология – использование свойств квантовых систем для высокоточного измерения физических величин, миниатюризации или энергоэффективности.

---

[175] Россия вошла в топ-3 стран с передовыми квантовыми процессорами [Электронный ресурс] // АО «Росбизнесконсалтинг» (РБК). URL: https://trends.rbc.ru/trends/innovation/cmrm/68b007949a7947e3382e2758 (дата обращения: 25.03.2026).

[176] Об утверждении Программы фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021–2030 годы) : распоряжение Правительства РФ от 31 декабря 2020 г. № 3684-р (ред. от 25.12.2025) // СЗ РФ. 2021. № 3. Ст. 609.

[177] О Рекомендациях о сотрудничестве государств – участников СНГ в сфере цифрового развития : постановление № 53-12 Межпарламентской Ассамблеи государств – участников СНГ (Принято в г. Санкт-Петербурге 26.11.2021) // Информационный бюллетень. Межпарламентская Ассамблея государств – участников Содружества Независимых Государств. 2021. № 75.

[178] Холодная Е. В. Квантовые технологии как объект права [Электронный ресурс] // Вестник Университета имени О. Е. Кутафина (МГЮА). 2022. № 4 (92). С. 38–45. URL: https://www.elibrary.ru/item.asp?id=49027096 (дата обращения: 25.03.2026).

[179] [Электронный ресурс]. URL: https://www.rst.gov.ru/portal/gost/home/presscenter/news?portal:componentId=88beae40-0e16-414c-b176-d0ab5de82e16&navigationalstate=JBPNS_rO0ABXczAAZhY3Rpb24AAAABAA5zaW5nbGVOZXdzVmlldwACaWQAAAABAAQ5MDc2AAdfX0VPRl9f (дата обращения: 25.03.2026).

[180] Об утверждении Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года : распоряжение Правительства РФ от 11 июля 2023 г. № 1856-р // СЗ РФ. 2023. № 30. Ст. 5712.

[181] Евсиков К. С. Правовое регулирование поддержки отечественных производителей квантовых коммуникаций // Право и цифровая экономика. 2023. № 3. С. 11–19.

[182] Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии» [Электронный ресурс]. URL: https://digital.gov.ru/ (дата обращения: 25.03.2026).

– Квантовые коммуникации – технологии, направленные на устранение угрозы информационной безопасности, в том числе со стороны квантовых компьютеров, включают использование свойств квантовых систем для передачи ключей.

Квантовые коммуникации являются перспективной областью развития информационной безопасности, позволяющие усилить надежность и защищенность канала передачи информации. В состав которых входят[183]:

– доверенный промежуточный узел;
– квантовый датчик (генератор) случайных чисел;
– квантовозащищенный ключ;
– квантовозащищенная сеть связи;
– квантовый ключ;
– квантовое распределение ключей;
– модуль управления ключами;
– протокол квантовой передачи;
– средство криптографической защиты информации;
– система управления ключами;
– и другое.

Структура доверенных квантовых технологий направлена на создание безопасного пространства и эффективности развития квантовых технологий. Среди приоритетных направлений являются доверенные квантовые технологии, основанные на коммуникации по защищенным каналам связи, квантовых сетях с доверенными промежуточными узлами, с квантовым распределением ключей, доверенного и защищенного системного и прикладного программного обеспечения и так далее. Методы обеспечения доверия квантовых технологий необходимо применять на каждом этапе жизненного цикла, поскольку доверие формируется как на этапе создания квантовых технологий, так и на этапах функционирования и их эксплуатации (см. рис. 1).

Рис. 1. Формирование доверия к квантовым технологиям

Среди основных методов обеспечения доверия к квантовым технологиям стоит выделить следующие:

1) использование квантового распределения ключей, позволяющий обеспечить безопасность связи по каналу передачи данных;

2) построение сетей с доверенными промежуточными узлами, обеспечивающий защиту передачи ключей соединенных сегментов;

[183] ПНСТ 829-2023. Предварительный национальный стандарт Российской Федерации. Квантовые коммуникации. Общие положения (утв. и введен в действие приказом Росстандарта от 11.07.2023 № 22-пнст). М. : ФГБУ «Институт стандартизации», 2023. С. 14.

3) формирование квантовозащищенных ключей, необходимое для создания общего ключа с помощью квантовых криптографических протоколов с целью невозможности перехвата ключа злоумышленником;

4) использование доверенного программного обеспечения. Правительство Российской Федерации утвердило правила доверенных российских программ для ЭВМ, согласно которому программа должна быть включена в перечень доверенного программного обеспечения[184]. Вместе с этим необходимо реализовать ведение Реестра доверенного программного обеспечения квантовых технологий;

5) использование доверенных криптографических приложений необходимо для формирования доверенной электронной подписи, недоступная для третьих лиц и не позволяющая осуществить подписание документов без подтверждения авторства и дополнительных идентификаторов;

6) использование уникальных идентификаторов – это одно из главных решений формирования доверия, поскольку предполагает квантовое шифрование с целью обеспечения точности, надежности и безопасности идентификации субъекта;

7) тотальный контроль за действиями субъектов предполагает использование высокоточных передовых систем мониторинга и управления субъектами и объектами, обеспечивающее прозрачность их действий.

В результате доверие к квантовым технологиям формируется путем соблюдения нормативным требованиям, стандартам безопасности, защищенности каналов связи, регулированию деятельности в области разработки и внедрения квантовых технологий. Внедрение квантовых технологий ведет к научно-технологическому прогрессу на мировом уровне в сфере информационной безопасности, что является стратегической важностью для России.

Несмотря на отличные возможности применения квантовых технологий, наблюдаются отсутствие полного правового и технического регулирования квантовых технологий, не говоря уже о доверенных квантовых технологиях, которые представляют особый интерес сегодня. И как отмечает ряд авторов: «Наблюдается недостаток регулирования в области квантовых технологий, в этой сфере пока нет ни стратегической базы, ни конкретных подходов к правовому регулированию, что необходимо проработать»[185].

Тем не менее перед государством поставлены задачи для внедрения квантовых технологий. Ежегодное послание Президента Российской Федерации В. В. Путина Федеральному собранию: «Нам нужны собственные передовые разработки и научные решения. Цифровые технологии, другие так называемые сквозные технологии, которые сегодня определяют облик всех сфер жизни. Страны, которые смогут их генерировать, будут иметь долгосрочное преимущество. Другие окажутся в зависимом, уязвимом положении. Это цифровые, квантовые технологии, робототехника, нейротехнология и т. д. В цифровых технологиях кроются и риски. Необходимо укреплять киберзащиту. Развитие цифровой экономики, в ее реализации будем опираться именно на российские компании»[186].

[184] Об утверждении Правил формирования и ведения перечня доверенных российских программ для электронных вычислительных машин и баз данных : постановление Правительства РФ от 28 ноября 2025 г. № 1931 // СЗ РФ. 2025. № 48 (ч. IV). Ст. 7378.

[185] Минбалеев А. В., Петровская О. В. Основные направления регулирования квантовых технологий // Цифровые технологии и право : сб. науч. тр. III Междунар. науч.-практ. конф. : в 6 т., Казань, 20 сентября 2024 года. Казань : Познание, 2024. С. 27–29.

[186] Послание Президента Российской Федерации Федеральному Собранию от 01.12.2016.

Д. Д. Тумачев,
студент, кафедра информационной безопасности
ФГБОУ ВО «Астраханский государственный университет им. В. Н. Татищева»,
В. А. Корякова,
ассистент кафедры информационной безопасности
ФГБОУ ВО «Астраханский государственный университет им. В. Н. Татищева»,
г. Астрахань

Разработка системы автоматического тестирования безопасности веб-приложений на основе общедоступных банков уязвимостей

Веб-приложения используются в самых различных сферах, таких как финтех, государственные информационные системы или страховые компании. Такое распространение веб-приложений приводит к увеличению числа атак на них. Согласно данным, опубликованным компанией WMX, только с января по сентябрь 2025 года число таких кибератак выросло в 4 раза[187]. Разработанные на данный момент методы обеспечения безопасности имеют серьезные ограничения, например, ручной аудит кода[188] и пентест[189] требуют достаточно больших затрат по времени и постоянного присутствия специалиста, а сканеры[190], работающие отдельно друг от друга, находят не все уязвимости.

Таким образом, становится актуальной автоматизация комплексной проверки безопасности с использованием данных из открытых банков уязвимостей[191], таких как CVE, NVD, MITRE и OWASP. В них информация об уязвимостях уже структурирована и её удобно использовать.

Цель исследования – разработать систему комплексного автоматического тестирования безопасности веб-приложений, в которую будет добавлена синхронизация данных с общедоступными банками уязвимостей. Это поможет своевременно выявить потенциальные уязвимости и сформировать отчет с рекомендациями по их устранению.

Научная новизна работы заключается в создании подхода, который будет объединять возможности автоматизированного сканирования с динамической загрузкой данных из открытых источников. Это позволит повысить оперативность и полноту обнаружения угроз по сравнению с существующими методами.

Для проведения исследования были определены и выбраны наиболее распространённые средства для анализа безопасности веб-приложений: Burp Suite[192], OWASP ZAP[193], Nessus[194], Acunetix[195], Netsparker[196], Sqlmap[197], Metasploit[198] и Wfuzz[199]. Эти продукты охватывают достаточно широкий спектр задач ИБ, начиная с обычного комплексного анализа HTTP-трафика (Burp Suite) и сканирова-

[187] Промышленность столкнулась с кратным ростом веб-атак [Электронный ресурс] // webmonitorx. URL: https://webmonitorx.ru/news/novosti-kompanii/promyshlennost-stolknulas-s-kratnym-rostom-vebatak/ (дата обращения: 04.12.2025)

[188] Поиск уязвимостей в исходном коде с помощью ручного статического анализа [Электронный ресурс] // Хабр. URL: https://habr.com/ru/companies/ussc/articles/805031/ (дата обращения: 05.12.2025).

[189] Penetration Testing: российские системы тестирования на проникновение [Электронный ресурс] // SecurityLab.ru. URL: https://www.securitylab.ru/blog/personal/paragraph/354513.php (дата обращения: 05.12.2025).

[190] Методы и инструменты для поиска уязвимостей в системах [Электронный ресурс] // РУЦЕНТР. URL: https://www.nic.ru/help/metody-i-instrumenty-dlya-poiska-uyazvimostej-v-sistemah_13752.html (дата обращения: 05.12.2025).

[191] Making Sense of Open-Source Vulnerability Databases: NVD, OSV, etc. [Электронный ресурс] // DEV Community. URL: https://dev.to/gitguardian/making-sense-of-open-source-vulnerability-databases-nvd-osv-etc-4g9f (дата обращения: 05.12.2025).

[192] Как использовать Burp Suite для проверки сайтов на уязвимости – журнал «Код» [Электронный ресурс] // thecode. URL: https://thecode.media/burp-suite-2/ (дата обращения: 06.12.2025).

[193] ZAP – Getting Started [Электронный ресурс] // zaproxy. URL: https://www.zaproxy.org/getting-started/ (дата обращения: 06.12.2025).

[194] Nessus Vulnerability Scanner: Network Security Solution | Tenable® [Электронный ресурс] // tenable. URL: https://www.tenable.com/products/nessus (дата обращения: 06.12.2025).

[195] Acunetix | Web Application Security Scanner [Электронный ресурс] // acunetix. URL: https://www.acunetix.com/ (дата обращения: 07.12.2025).

[196] Netsparker 2025: Pricing, Features, Details and Comparison [Электронный ресурс] // akto. URL: https://www.akto.io/blog/netsparker (дата обращения: 07.12.2025).

[197] Sqlmap: automatic SQL injection and database takeover tool [Электронный ресурс] // sqlmap. URL: https://sqlmap.org/ (дата обращения: 07.12.2025).

[198] Что такое Metasploit? Руководство для начинающих [Электронный ресурс] // Хабр. URL: https://habr.com/ru/companies/varonis/articles/528578/?ysclid=miy9tu31ak294808221 (дата обращения: 07.12.2025).

[199] WFuzz – фреймворк для атак на веб-приложения через подстановку (fuzzing) [Электронный ресурс] // securitylab. URL: https://www.securitylab.ru/blog/personal/SimlpeHacker/355285.php?ysclid=miy9v0wckq675834279 (дата обращения: 07.12.2025).

ния инфраструктуры сети (Nessus) и заканчивая узкоспециализированным поиском SQL-инъекций (Sqlmap) или имитации атак (Metasploit).

По типу лицензии инструменты делятся на две группы. Первая – это коммерческие (Burp Suite, Nessus, Acunetix, Netsparker). Эта группа предлагает развитую, продуманную отчётность и высокий уровень автоматизации, но ограничены большой стоимостью и ресурсоёмкостью. А вторая группа – это программы с открытым исходным кодом (OWASP ZAP, Sqlmap, Metasploit, Wfuzz). Эта группа отличается бесплатностью, и программы, относящиеся к ней, обладают гибкой настройкой, но при этом требуют того, чтобы пользователь обладал достаточной квалификацией. Также эти программы могут уступать по удобству и дружелюбности интерфейса и полноте проверок.

Проведя сравнительный анализ, были выявлены некоторые ограничения, которые являются общими для этих решений. Например, Burp Suite и Metasploit[200] являются сложными в освоении. У Acunetix и OWASP ZAP достаточно большое количество ложных срабатываний. Sqlmap, Wfuzz имеют очень узкий профиль работы, буквально один вектор уязвимостей. Кроме всех этих недостатков можно отметить, что некоторые решения не своевременно обновляют свои базы уязвимостей.

Таким образом, становится необходимым создание программы, которая сочетала бы в себе функционал обычных сканеров с автоматической синхронизацией данных их открытых банков уязвимостей. Такая система расширила бы возможности по обнаружению уязвимостей в веб-приложениях.

Для проектирования системы был выбран подход, который включает в себя использование методологий функционального моделирования. Для этого применяются стандартные нотации IDEF0, и IDEF3. Они позволяют наглядно, а главное, комплексно описать функционирование всей системы на различных уровнях детализации.

Нотация IDEF0, которая представлена на рисунке 1, раскрывает систему автоматического тестирования безопасности веб-приложений на самом верхнем уровне абстракции.

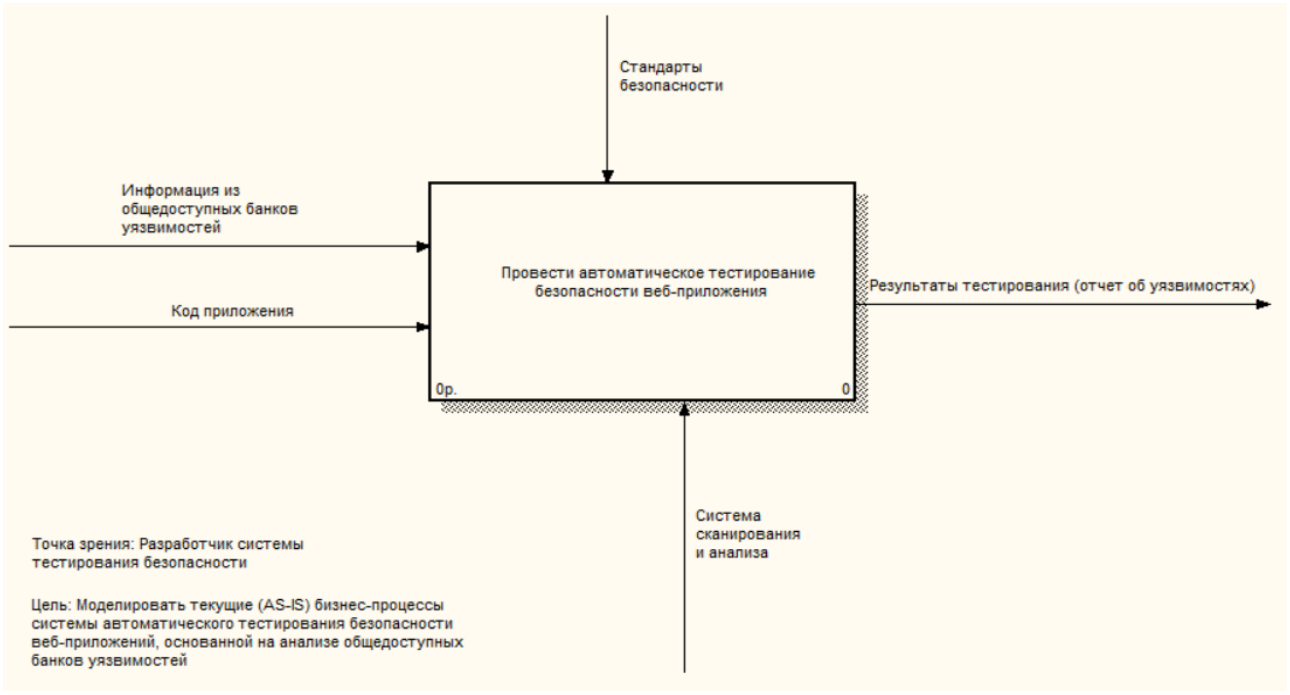

Рис. 1. Контекстная диаграмма IDEF0 процесса автоматического тестирования безопасности веб-приложения

В качестве основной функции системы на диаграмме был выбран процесс «Провести автоматическое тестирование безопасности веб-приложения». Он объединяет в себя совокупность действий, которые направлены на обнаружение уязвимостей и формирование итоговых результатов после анализа. На вход этому процессу подается код веб-приложения, который выступает объектом для анализа, а также информация из общедоступных банков уязвимостей, она содержит сведения об известных уязвимостях, их подробные описания, классификации и оценку уровня критичности. Процесс четко регулируется различными существующими стандартами безопасности, включающими в себя методические рекомендации, классификацию уязвимостей и требования к обеспечению безопасности веб-приложений. В качестве механизма реализации используется мощная система сканирования и анализа. Она

[200] Burp Suite для тестирования безопасности веб-приложений – журнал «Код» [Электронный ресурс] // thecode. URL: https://thecode.media/burp-suite/ (дата обращения: 09.12.2025).

выполняет различные автоматизированные процедуры для тестирования. Итогом выполнения всего этого процесса является результат тестирования, который сформирован в отчёт об уязвимостях веб-приложения.

Таким образом, эта контекстная диаграмма наглядно демонстрирует обобщённую структуру проектируемой системы для автоматического тестирования и определяет основные границы её функционирования.

Для более детального описания всей логики функционирования системы автоматического тестирования безопасности веб-приложений произведена декомпозиция основной функции верхнего уровня на взаимосвязанные подпроцессы. Диаграмма декомпозиции представлена на рисунке 2.

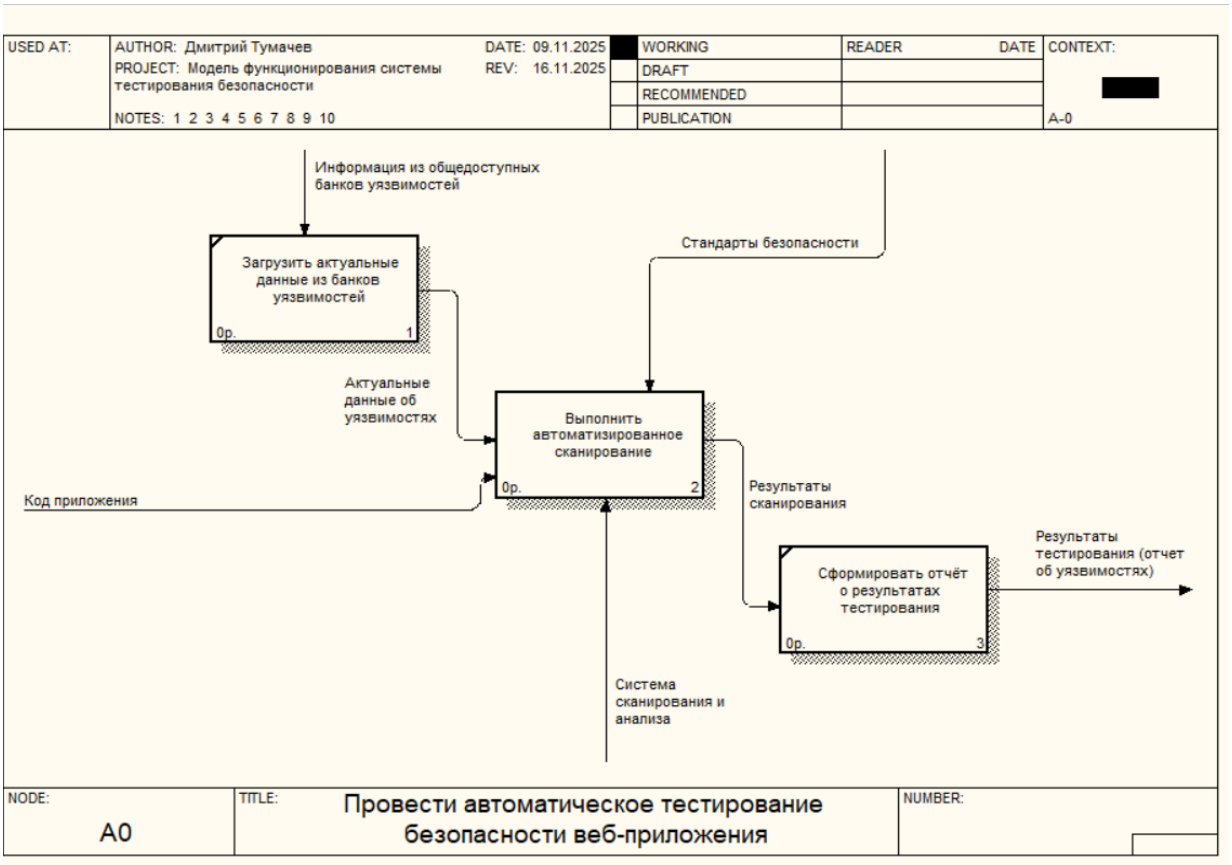

Рис. 2. Декомпозиция функции «Провести автоматическое тестирование безопасности веб-приложения»

В рамках данной декомпозиции основная функция была разделена на три ключевых подпроцесса. Они проходят последовательно, друг за другом. Каждый из них выполняет свою важную роль в процессе тестирования безопасности.

Первый подпроцесс необходим для того, чтобы сформировать информационную базу для анализа, второй уже непосредственно отвечает за выполнение сканирования веб-приложения, а третий обрабатывает и компонует все эти результаты тестирования в удобную для восприятия форму, чтобы результат был понятен даже тем людям, которые не являются профессионалами в сфере информационной безопасности.

Первый подпроцесс направлен на то, чтобы загрузить данные из открытых банков уязвимостей (или синхронизировать, обновить их в том случае, если они уже были загружены). Взаимодействие с банками проходит по средствам обращения к их API. Результатом этого подпроцесса является качественный, структурированный набор данных с актуальными уязвимостями.

Во время второго подпроцесса происходит тестирование и анализ безопасности веб-приложения, а именно его исходного кода и логики взаимодействия с пользователем. Анализ включает в себя три этапа. Первый – это сканирование зависимостей, второй – это статический анализ SAST. А третий – динамический анализ DAST. На всех этапах будут использоваться данные, загруженные во время первого подпроцесса.

Результатом второго подпроцесса является перечень найденных уязвимостей и проблем безопасности. Эти данные передаются в третий подпроцесс.

Основной задачей последнего подпроцесса является обработка и структурирование полученных данных для создания итогового отчета. Готовый, сформированный отчёт уже может спокойно использоваться специалистами по информационной безопасности для дальнейшего принятия решений по устранению найденных уязвимостей.

Данный подход позволит быстро получать знания о возможных угрозах. Также он расширит спектр обнаруживаемых уязвимостей из-за того, что всё сканирование основано на данных, которые синхронизируются с банками уязвимостей.

Разработанная система способна преодолеть основные ограничения текущих методов тестирования веб-приложений, а её внедрение повысит уровень их защищённости в очень быстро изменяющейся среде угроз кибербезопасности.

Я. Н. Шевченко,
студент, кафедра информационной безопасности
ФГБОУ ВО «Астраханский государственный университет им. В. Н. Татищева»,
В. А. Корякова,
ассистент кафедры информационной безопасности
ФГБОУ ВО «Астраханский государственный университет им. В. Н. Татищева»,
г. Астрахань

Выявление фишинговых доменов с помощью методов машинного обучения в режиме реального времени

В современном мире, направленном на повсеместную цифровизацию и перенос различных аспектов жизни в онлайн, информационная безопасность стала критически важным аспектом для пользователей и организаций по всему миру. Одной из наиболее распространённых и критических угроз является фишинг[201], при котором злоумышленники создают поддельные веб-сайты для кражи конфиденциальных данных, таких как учетные записи, пароли и банковская информация. Рост сложности и распространённости фишинговых атак, а также их относительная простота создания благодаря генеративному искусственному интеллекту требуют внедрения решений, способных бороться с данным видом угрозы. Современные бизнес процессы и простые пользователи ожидают не только высокую степень защиты, но и своевременную реакцию на всё возрастающие риски.

Тем не менее традиционные методы обеспечения кибербезопасности, такие как применение чёрных списков и оценочные системы репутации доменов, демонстрируют ограниченную эффективность либо требуют существенных трудозатрат на проведение анализа данных.

Следовательно, возникает потребность в новом методе обнаружения фишинговых доменов, который будет лишён недостатков традиционных решений[202]. Таким методом является машинное обучение, которое привносит проактивный подход в защиту от фишинговых угроз.

Существует несколько основных традиционных методов защиты. Самым простым из них является метод чёрных списков URL, работает путём простого сравнения с базой данных, содержащей список уже известных фишинговых адресов. Данный подход эффективен против уже выявленных фишинговых URL, однако совершенно бесполезен против новых и остаётся уязвимым к динамическим атакам.

Статические сигнатурные методы[203] и анализ правил. В данном методе выявляются заранее подготовленные сигнатуры. Сама сигнатура может быть разной и являть собой структуру файла, уникальную комбинацию битов или иные значения.

Принцип действия схож с «чёрными списками», но проверяются не названия доменов, а вышеупомянутые сигнатуры. Часто этот метод используется совместно с эвристическими правилами. Это повышает результативность традиционных подходов, однако ограничивает их эффективность против современных фишинговых атак – особенно на фоне развития генеративного ИИ, позволяющего создавать, на первый взгляд, идеальные копии легитимных сайтов.

Это приводит к тому, что сигнатура угрозы может постоянно меняться, буквально при создании каждого нового фишингового сайта, а сложные в настройке эвристические правила потребуют доработки. Что, в свою очередь, снижает эффективность традиционных методов.

---

[201] ВикиЗнание [Электронный ресурс]. URL: https://znanierussia.ru/articles/Фишинг (дата обращения: 02.03.2026).

[202] Knowbe4 [Электронный ресурс]. URL: https://www.knowbe4.com/resource-center/phishing (дата обращения: 02.03.2026).

[203] Anti-malware.ru.ru [Электронный ресурс]. https://www.anti-malware.ru/analytics/Technology_Analysis/All-About-Antiviruses-Part-II (дата обращения: 02.03.2026).

Методы защиты от фишинга, рассмотренные ранее, такие как использование черных списков, сигнатурного анализа, применение эвристических правил, обладают рядом существенных недостатков, ограничивающих их эффективность в современных условиях[204].

Ключевое ограничение традиционных подходов заключается в их реактивности. Они основаны исключительно на выявленных угрозах, включенных в заранее подготовленные базы данных. Следовательно, защита срабатывает лишь тогда, когда угроза уже известна и зарегистрирована. Между моментом появления нового вредоносного сайта и его внесением в черный список проходит определенный интервал времени, который является достаточно большим для злоумышленников, чтобы нанести значительный ущерб своим жертвам.

Машинное обучение является совершенно иным, проактивным подходом. Вместо обнаружения известных шаблонов модель машинного обучения выявляет более абстрактные признаки, что с высокой долей вероятности можно отнести к фишингу. В процессе обучения модель анализирует множество разнородных параметров, которые можно разделить на несколько основных групп.

Лексические признаки домена, т. е. использование специальных или похожих символов из другого алфавита, а также IP-адрес вместо домена. Признаки безопасности домена, такие как возраст, наличие SSL-сертификата, его тип и иные данные WHOIS. HTML контент, который включает в себя проверку количества внешних ссылок, наличие скриптов, выполняющих редирект, скачивание и т. д. А также иные признаки из внешних источников.

Модель анализирует весь комплекс этих параметров и выявляет неочевидные для человека паттерны фишинговых угроз. Это позволяет классифицировать угрозы на основе их поведения и характеристик, а не на основе статической сигнатуры, что делает метод чрезвычайно эффективным против совершенно новых, ранее не встречавшихся (zero-day) фишинговых ресурсов.

Среди классических алгоритмов, доказавших свою эффективность, выделяются метод k-ближайших соседей (KNN), наивный байесовский классификатор (NB), дерево решений (DT) и случайный лес (RF).

Ярким примером эффективности методов мащинного обучения служит работа «Real-Time Phishing URL Detection Using Machine Learning»[205], в которой проводилось сравнительное тестирование ряда алгоритмов, включая k-nearest neighbor (KNN), naive Bayes (NB), decision trees (DT) и random forest (RF), на крупном наборе данных из 235 795 экземпляров.

Согласно представленным в статье результатам вышеуказанные алгоритмы продемонстрировали высокие показатели на указанном наборе данных (рис. 1).

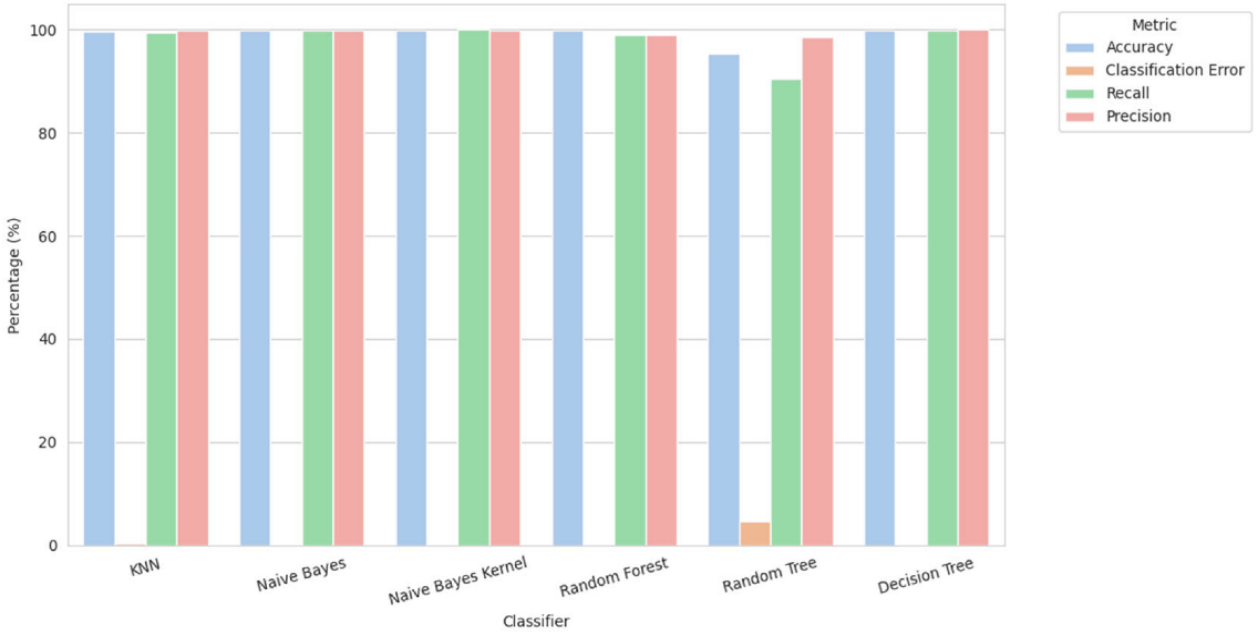

Рис. 1. Метрики производительности классификаторов

[204] Назаров А. А., Губенков А. А. Использование машинного обучения для защиты от фишинговых атак: сравнение с традиционными механизмами // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2025. № 2. (дата обращения: 02.03.2026).

[205] Рехман А. У., Имтиаз И., Джаваид С., Муслих М. Обнаружение фишинговых URL-адресов в реальном времени с использованием машинного обучения. Инженерные труды. 2025. 107 (1) : 108 [Электронный ресурс]. URL: https://doi.org/10.3390/engproc2025107108 (дата обращения: 02.03.2026).

Отдельно стоит отметить такой классификатор, как Random Forest, он является самым часто используемым в различных исследованиях и достигает высоких показателей точности от 94,36 до 99,99%. Столь высокий результат объясняется природой самого алгоритма: как ансамблевый метод Random Forest агрегирует прогнозы множества отдельных деревьев решений, что позволяет значительно снизить дисперсию и минимизировать риск переобучения, обеспечивая высокую обобщающую способность на новых данных.

Предлагаемая методика направлена на создание эффективного проактивного механизма выявления фишинговых доменов в режиме реального времени с использованием методов машинного обучения.

Входные данные алгоритма:

а) поток новых/подозрительных доменных имён;

б) актуальные белые и чёрные списки, датасеты;

в) архивы WHOIS.

Выходные данные:

а) для каждого проверяемого домена: бинарная метка (фишинг/легитимный) и вероятностная оценка (score phishing probability, 0–1);

б) обновлённая версия модели;

в) логи и объяснимые признаки, полезные для аналитиков.

Для формализации и структурированного описания методики выявления фишинговых доменов используется модель IDEF0. На контекстной диаграмме (A-0) единственной функцией является «Осуществить проверку безопасности веб-сайта при помощи ИИ» (рис. 2).

Рис. 2. Схема A-0 IDEF0

Входными данными выступают трафик новых доменных имен для проверки, белые/черные списки, архивы WHOIS и датасеты фишинговых сайтов. Управляющими воздействиями являются методики и стандарты безопасности, а также регламенты реагирования на инциденты. Механизмами – система обучения и анализа модели, ML-платформа и база данных. Выходом будут являться отметка о домене (фишинг/легитимный) и обновленная в процессе обучения модель ИИ.

Далее в рамках IDEF0 проводим декомпозицию, чтобы проиллюстрировать основные процессы реализации проверки (рис. 3 на след. стр.).

В рамках декомпозиции было принято решение разделить процесс на 4 основных блока: извлечение признаков, анализ и принятие решения, обучение ML-модели, а также вспомогательные процессы загрузки данных и верификации. Такое разделение соответствует стандартной практике и обеспечивает оптимизацию процесса анализа в реальном времени.

В представленной работе проанализированы недостатки традиционных подходов к защите от фишинга, а также аргументирована необходимость внедрения проактивной стратегии, основанной на методах машинного обучения, позволяющей выявлять фишинговые домены в режиме реального времени.

Рис. 3. Декомпозиционная диаграмма A0 IDEF0

Использование разработанной методики позволяет оперативно обрабатывать новые и неизвестные угрозы за счёт комплексного анализа различных показателей с последующей классификацией с помощью ИИ.

Г. А. Сегизбаев,
студент, кафедра информационной безопасности
ФГБОУ ВО «Астраханский государственный университет им. В. Н. Татищева»,
В. А. Корякова,
ассистент кафедры информационной безопасности
ФГБОУ ВО «Астраханский государственный университет им. В. Н. Татищева»,
г. Астрахань

Программный комплекс для защиты больших языковых моделей от извлечения обучающего набора данных

Большие языковые модели – одна из наиболее быстроразвивающихся сфер в области искусственного интеллекта. Проблемы возникают с тем, что в силу специфики своей работы они должны наиболее точно выдавать пользователю данные, заложенные в них в процессе обучения[206]. Свойство «запоминать» записи из обучающего набора данных является как достоинством, так и уязвимостью больших языковых моделей[207]. Злоумышленники могут попытаться воспользоваться данной уязвимостью с целью получить из модели конфиденциальные сведения посредством простых текстовых атак[208]. По данным опроса компании «Информзащиты» за 2025 год 70 % российских компаний, внедривших большие языковые модели в свою работу, сталкиваются с атаками на модели, 40 % из атак направлены на извлечение данных, помимо этого, 67 % российских компаний не тестируют внедренные решения на подверженность существующим атакам[209].

Цель данной работы – разработка программного комплекса для защиты больших языковых моделей от угроз извлечения данных. Научная новизна работы заключается в применении гибридной системы защиты на основе фильтрации запросов/ответов, мониторинга и накапливания данных

[206] The Landscape of Memorization in LLMs: Mechanisms, Measurement, and Mitigation. 2025 [Электронный ресурс]. URL: https://arxiv.org/pdf/2507.05578 (дата обращения: 20.12.25).
[207] Deduplicating Training Data Mitigates Privacy Risks in Language Models [Электронный ресурс]. URL: https://arxiv.org/pdf/2202.06539 (дата обращения: 25.12.25).
[208] Extracting Training Data from Large Language Models. 2021. URL: https://arxiv.org/pdf/ (дата обращения: 21.12.25).
[209] Злоумышленники усиливают атаки на корпоративные LLM-модели [Электронный ресурс] // infosec.ru. URL: https://www.infosec.ru/press-center/news/zloumyshlenniki-usilivayut-ataki-na-korporativnye-llm-modeli/ (дата обращения: 07.02.26).

для дальнейшего совершенствования системы, а также наличия инструмента для тестирования безопасности модели до и после промышленного внедрения программного комплекса.

Сперва следует рассмотреть уже существующие способы обеспечения безопасности и разобрать их ограничения: дифференциальная приватность, ансамблевый подход, методы на основе дообучения, guardrails.

При дифференциальной приватности влияние данных во время обучения снижается через их зашумление[210]. Однако при большой степени шума итоговая работа модели ухудшается, а при слишком малой – снижается эффект от защиты[211]. К тому же трудность представляет и необходимость полного переобучения большой модели.

Иной подход предлагает использовать ансамбль моделей. Обучающий набор разбивается на части, и на каждой части обучается отдельная модель. На запрос пользователя собирается агрегированный ответ всех моделей, что снижает риск дословного воспроизведения фрагментов данных[212]. При этом подходе возрастает нагрузка на систему, так как необходимо поддерживать несколько экземпляров большой языковой модели и все так же нужно проводить полное переобучение.

Методы на основе дообучения задают дополнительные инструкции безопасности модели вида «опасный запрос – безопасный ответ» и учат правильно реагировать на опасные запросы[213]. Если система встречает знакомый вариант опасного запроса, то выдает пользователю безопасный ответ. Тем не менее хоть объем вносимых данных при дообучения снижен, метод все равно требует модификации существующей модели.

Алгоритм Guardrails представляет собой комбинацию двух фильтров: входной проверяет запросы пользователей, выходной – ответы модели[214]. Сначала проверяется запрос пользователя. Если он выглядит подозрительно, его можно заблокировать. Аналогично с ответом модели. Guardrails – довольно простой и действенный способ защиты больших языковых моделей, не требующий изменения самих моделей. Именно он положен в основу разработки данного программного комплекса.

Большинство указанных методов не обеспечивают контроль безопасности на этапе эксплуатации модели, когда пользовательские запросы могут быть направлены на целенаправленное извлечение обучающих данных. В существующих системах механизмы фильтрации входных и выходных данных применяются ограниченно и, как правило, не сопровождаются инструментами оценки устойчивости модели к атакам. В связи с этим возникает необходимость разработки комплексной системы защиты, которая сочетает анализ пользовательских запросов, контроль генерируемых ответов и возможность тестирования модели на устойчивость к атакам извлечения данных. Предлагаемая в данной работе методика направлена на решение указанной задачи и применение на этапе промышленной эксплуатации больших языковых моделей.

Архитектура программного комплекса защиты больших языковых моделей представлена на рис. 1.

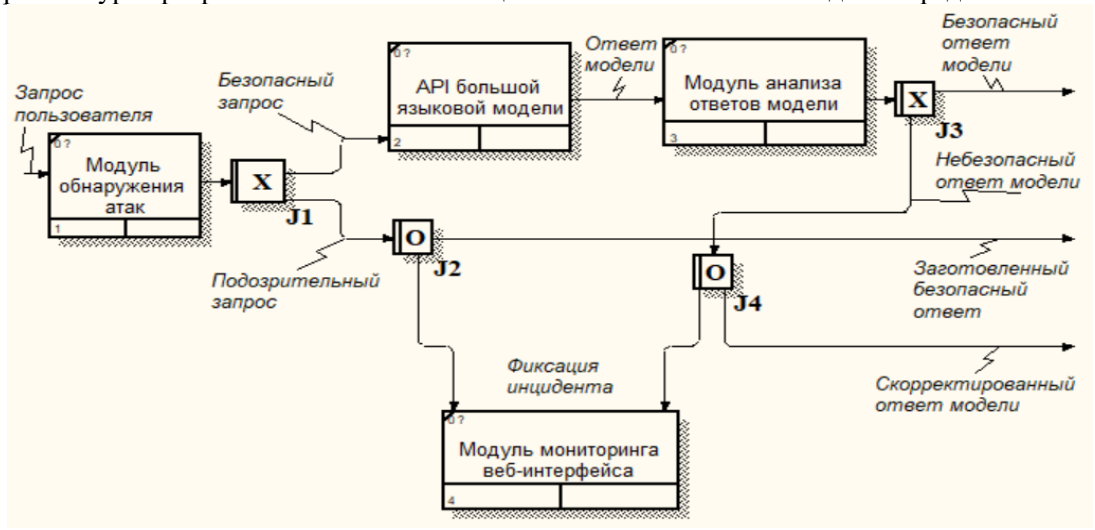

Рис. 1. Архитектура программного комплекса

[210] Дифференциальная приватность – анализ данных с сохранением конфиденциальности [Электронный ресурс] // Хабр. URL: https://habr.com/ru/companies/domclick/articles/526724/?ysclid=miexa4sfbl927197657 (дата обращения: 21.12.25).

[211] Differentially Private Learning with Adaptive Clipping. 2022. URL: https://arxiv.org/pdf/ (дата обращения: 22.12.25).

[212] SubMix: Practical Private Prediction for Large-Scale Language Models. 2022 [Электронный ресурс]. URL: https://arxiv.org/pdf/2201.00971 (дата обращения: 28.12.25).

[213] Parameter-Efficient Fine-Tuning (PEFT): методы LoRA, Prefix tuning, Prompt tuning и Adapters [Электронный ресурс] // Хабр. URL: https://habr.com/ru/articles/791966 (дата обращения: 21.12.25).

[214] Building Guardrails for Large Language Models. 2024 [Электронный ресурс]. URL: https://arxiv.org/html/2402.01822v1 (дата обращения: 02.02.26).

Перед развёртыванием системы защиты целесообразно провести тестирование модели на подверженность уязвимостям. Это позволит заранее выявить слабые места на чувствительность к встраиванию вредоносных инструкций и иных видов манипуляций. Инструмент тестирования будет интегрирован как интерфейсный модуль системы с возможностью в любой момент запустить проверку уязвимости модели к типичным атакам.

На этапе эксплуатации каждый запрос пользователей проходит проверку во входном фильтре. Фильтрация с использованием регулярных выражений определит наличие строго структурированных данных (например: номер телефона, ФИО, email) и заменит их безопасной маской, что не позволит модели установить соответствие с реальными данными. Далее классификатор на основе машинного обучения определит вероятность принадлежности пользовательского запроса к шаблонам атак извлечения данных. В случае преодоления определенного порога, задаваемого в веб-интерфейсе модуля мониторинга администратором безопасности, регистрируется инцидент безопасности, а пользователю выдается заготовленный безопасный ответ. В ином случае в запрос встраиваются дополнительные инструкции для защиты от манипуляций, и запрос передается в большую языковую модель.

Отфильтрованные запросы все равно могут приводить к непреднамеренным утечкам уже со стороны модели[215]. Поэтому в дополнение к входной фильтрации существует и проверка ответов, сгенерированных на этапе инференса. Валидаторы, на основе правил, просигнализируют об утечке конфиденциальной информации, а механизм повторной генерации запросит у модели вторично сгенерировать ответ, но уже с дополнительными ограничениями. Если и эти действия приведут к непреднамеренной утечке данных, регистрируется инцидент безопасности, а пользователю выдается безопасный ответ.

Важным элементом предлагаемой системы станет панель мониторинга. Все логи, подозрительные запросы и ответы будут направляться сюда. Накопление инцидентов безопасности позволит динамически совершенствовать работу фильтров. Здесь же администратор сможет настраивать чувствительность фильтров и запускать инструмент тестирования безопасности.

Разработанный программный комплекс для защиты больших языковых моделей от извлечения обучающего набора данных имплементируется над уже существующей системой и снимает необходимость в каких-либо модификациях. Накапливаемые логи и инциденты безопасности позволят поддерживать актуальный уровень защиты, а отчеты тестирования до и после полноценного внедрения комплекса помогут компаниям определиться, целесообразны ли существующие риски.

Г. Д. Псарев,
аспирант кафедры информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Применение искусственного интеллекта и иных инновационных цифровых технологий в целях защиты информации: организационные, правовые, технические и иные аспекты

Современный этап развития общества характеризуется глубинной цифровой трансформацией всех сфер жизни, что неизбежно влечет за собой эскалацию угроз в области информационной безопасности. Мы сталкиваемся не просто с увеличением числа кибератак, но и с качественной эволюцией методов злоумышленников, которые все активнее используют потенциал систем искусственного интеллекта (далее – ИИ). В этих условиях ИИ становится «палкой о двух концах»: мощнейшим инструментом для атакующих и незаменимым помощником для защитников. Целью данной работы является анализ многогранного применения инновационных цифровых технологий, прежде всего ИИ, для защиты информации с акцентом на организационные, технологические и правовые аспекты, а также систематизация взглядов российских исследователей на эту проблему.

Прежде всего необходимо определиться с понятийным аппаратом. Согласно Национальной стратегии развития искусственного интеллекта[216] под искусственным интеллектом понимается ком-

[215] SafeGPT: Preventing Data Leakage and Unethical Outputs in Enterprise LLMUse. 2026 [Электронный ресурс]. URL: https://arxiv.org/pdf/2601.06366 (дата обращения: 06.02.26).

[216] О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») : Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) [Электронный ресурс] // СПС «КонсультантПлюс». 2026.

плекс технологических решений, позволяющий имитировать когнитивные функции человека и получать результаты, сопоставимые или превосходящие результаты его интеллектуальной деятельности. Важно подчеркнуть, что эта же Стратегия в редакции 2024 года вводит понятие «доверенные технологии ИИ», акцентируя внимание на безопасности и исключении возможности нанесения ущерба интересам личности, общества и государства. Это задает вектор развития: безопасность должна быть вшита в технологии ИИ изначально, а не прилагаться постфактум. Профессор Н. И. Дорохов в своей работе расширяет контекст, связывая развитие ИИ с достижением технологического суверенитета и технологического лидерства России. Он подчеркивает, что технологическое лидерство – это не просто замещение импорта, а создание конкурентоспособных продуктов, в том числе в сфере ИТ, доля которого в валовой добавленной стоимости должна расти[217]. Таким образом, развитие защитных механизмов на базе ИИ становится не просто технической, но и стратегической государственной задачей.

Анализ научных исследований позволяет выделить два основных вектора применения ИИ в информационной безопасности: защита от угроз, реализуемых с помощью ИИ, и использование ИИ для усиления существующих систем защиты.

Рассматривая первый вектор, нельзя не согласиться с классификацией угроз, предложенной Р. В. Мещеряковым и его коллегами. Авторы систематизируют такие опасности, как «подделка» биометрических данных (deepfake голоса и видео), создание ложных текстов, имитирующих стиль конкретного человека, и формирование фальшивых речевых сообщений[218]. Эти угрозы направлены не только на конфиденциальность, но и на целостность информации, подрывая доверие к данным и системам. С. Ю. Мельников, Р. В. Мещеряков и В. А. Пересыпкин в своем обзоре убедительно демонстрируют, насколько серьезными могут быть последствия. Они приводят примеры атак на биометрические системы, а также описывают технологию использования акустического канала утечки от клавиатуры, где современные нейросети позволяют с высокой точностью распознавать нажатые клавиши по спектрограммам звуков. Более того, они указывают на использование больших языковых моделей (LLM) типа ChatGPT для создания убедительных фишинговых писем в невиданных ранее масштабах[219]. Позиция авторов представляется абсолютно обоснованной: генеративный ИИ становится мощнейшим оружием социальной инженерии. Разделяя их обеспокоенность, стоит отметить, что эта проблема усугубляется возможностью создания «умных» вирусов, которые, как пишут Р. Ф. Мансуров и И. А. Матющенко, могут адаптироваться и изменять свой код для обхода систем защиты[220].

Второй вектор – применение ИИ для защиты. Здесь все исследователи единодушны во мнении, что традиционные сигнатурные методы (основанные на поиске совпадений с базами известных угроз) перестают быть эффективными против адаптивных и полиморфных атак. Главное преимущество ИИ, как справедливо указывают большинство ученых, – это способность к анализу аномалий. Методы машинного обучения (кластеризация, классификация) позволяют системам (например класса UEBA – User and Entity Behavior Analytics) выявлять отклонения в поведении пользователей или сетевом трафике, которые могут сигнализировать о начале атаки, даже если ее сигнатура неизвестна.

В этом контексте особенно важным представляется замечание С. Ю. Мельникова с соавторами о необходимости использования не только классических метрик (ложная тревога/пропуск цели), но и более сложных, таких как F-мера, для оценки качества работы таких систем. Соглашаясь с этим, можно добавить, что разработка и внедрение адаптивных систем безопасности и «умных» фаерволов на базе ИИ является безальтернативным путем повышения киберустойчивости критической инфраструктуры.

Важное место в дискуссии об использовании ИИ занимают правовые и организационные вопросы. Исследователи, в частности Н. И. Дорохов, а также Е. В. Шевченко и В. М. Смирнов, обращают внимание на то, что право пока не успевает за развитием технологий[221]. По сути, они ставят вопрос о том, как именно законодательство должно реагировать на вызовы цифровой эпохи.

---

[217] Дорохов Н. И. Технологический суверенитет России, цифровые технологии и искусственный интеллект: публично-правовые аспекты функционирования // Искусственный и естественный интеллект: алгоритмы, мышление и образовательные технологии : материалы XXI междунар. конгресса с элементами научной школы для молодых ученых. М., 2025. С. 1084–1101.

[218] Перспективные направления применения технологий искусственного интеллекта при защите информации / Р. В. Мещеряков, С. Ю. Мельников, В. А. Пересыпкин, А. А. Хорев // Вопросы кибербезопасности. 2024. № 4 (62). С. 2–12.

[219] Мельников С. Ю., Мещряков Р. В., Пересыпкин В. А. Некоторые аспекты применения технологий искусственного интеллекта в задачах защиты информации (обзор) // Известия ЮФУ. Технические науки. 2024. № 5 (241). С. 58–68.

[220] Мансуров Р. Ф., Матющенко И. А. Искусственный интеллект в кибербезопасности: новые угрозы и способы защиты // International Journal of Advanced Studies in Computer Engineering. 2025. Т. 8, № 1. С. 12–22.

[221] Шевченко Е. В., Смирнов В. М. Правовые аспекты регулирования применения технологий искусственного интеллекта в целях защиты информации // Обеспечение информационной безопасности: вопросы теории и практики : сб. ст. Всерос. науч.-практ. конф. Ижевск, 2025. С. 38–44.

Н. И. Дорохов обоснованно отмечает, что в современных условиях необходима глубокая трансформация системы государственного и муниципального управления, достижение так называемой «цифровой зрелости». Однако ключевой проблемой, по его мнению, остается разрозненность нормативных актов в информационной сфере. Сегодня регулирование осуществляется множеством отдельных законов, что затрудняет правоприменение. В связи с этим автор выдвигает идею о необходимости систематизации законодательства вплоть до разработки и принятия единого Цифрового кодекса. Представляется, что такое решение действительно могло бы устранить существующие противоречия и создать целостную правовую основу для цифрового развития.

Е. В. Шевченко и В. М. Смирнов в своем исследовании идут еще дальше и затрагивают более сложный вопрос – о правосубъектности искусственного интеллекта и ответственности за его действия. Их логика понятна: если рекомендация, выданная системой ИИ в контуре защиты информации, приведет к ошибочной блокировке легитимного пользователя или, что еще опаснее, к пропуску реальной атаки, кто именно должен нести за это ответственность? Разработчик, владелец системы или эксплуатирующая организация? Авторы справедливо указывают, что сегодня этот вопрос проработан слабо и не имеет однозначного законодательного решения.

При этом оба исследования позитивно оценивают уже существующие шаги государства в данном направлении. В частности, отмечается роль ГОСТ Р 59277-2020[222], который вводит классификацию систем искусственного интеллекта, и Федерального закона № 258-ФЗ об экспериментальных правовых режимах[223]. Последний документ представляет особый интерес, поскольку он позволяет апробировать новые технологии в контролируемых условиях, временно отступая от общих требований законодательства.

С такой оценкой трудно не согласиться. Так, в условиях столь динамично развивающейся сферы, как искусственный интеллект, жесткое и излишне детализированное регулирование может, скорее, навредить, затормозив внедрение полезных разработок. Гибкий подход, основанный на «регуляторных песочницах», выглядит наиболее разумным компромиссом: он позволяет не останавливать инновации, но при этом сохраняет необходимый уровень безопасности и контроля со стороны государства.

Однако, как неоднократно подчеркивается во всех работах, применение ИИ создает и новые уязвимости. Сами системы ИИ (особенно модели машинного обучения) становятся объектом атак. Р. В. Мещеряков, С. Ю. Мельников, В. А. Пересыпкин, А. А. Хорев подробно описывают такие угрозы, как отравление данных (искажение обучающей выборки), атаки с использованием состязательных примеров (когда минимальные, незаметные для человека искажения входных данных заставляют модель ошибаться), а также возможность извлечения данных из обученной модели. Обеспечение безопасности самих систем ИИ (интерпретируемость результатов, контроль процессов обучения) становится отдельным важнейшим направлением. Разделяя эту точку зрения, хочется добавить, что без решения этой задачи невозможно построение «доверенного искусственного интеллекта», о котором говорит и А. И. Аветисян в своих работах[224]. Особенно тревожным выглядит описанный в обзоре С. Ю. Мельникова новый тип атаки на LLM-ассистентов через анализ длины токенов в зашифрованном трафике, что позволяет восстановить содержание конфиденциального диалога. Это наглядно демонстрирует, что угрозы становятся все более изощренными и неочевидными.

Проведенный анализ позволяет обобщить полученные результаты и сформулировать ряд ключевых выводов и практических предложений.

1. В современном киберпространстве наблюдается настоящая технологическая гонка, в которой средства нападения и защиты развиваются параллельно. В этих условиях отказ от использования искусственного интеллекта в системах защиты информации фактически означает заведомое проигрышное положение. Анализ рассмотренных исследований показывает, что их авторы единодушны во мнении: применение алгоритмов машинного обучения для выявления аномалий, прогнозирования возможных атак и автоматического реагирования на инциденты становится не просто желательным, а критически необходимым условием обеспечения безопасности.

2. Важно понимать, что простое внедрение технологий ИИ само по себе не решает всех проблем. Более того, оно порождает новые риски. В связи с этим необходимо сместить акцент с количественных показателей внедрения на качественные характеристики безопасности и доверия. Развитие

---

[222] Об утверждении национального стандарта Российской Федерации : приказ Росстандарта от 23.12.2020 № 1372-ст [Электронный ресурс] // СПС «КонсультантПлюс». 2026.

[223] Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации : Федеральный закон от 31.07.2020 № 258-ФЗ (ред. от 31.07.2025) [Электронный ресурс] // СПС «КонсультантПлюс». 2026.

[224] Аветисян А. И. Доверенный искусственный интеллект // Вестник Российской академии наук. 2024. Т. 94, № 3. С. 200–209.

систем так называемого «доверенного искусственного интеллекта» должно стать одним из приоритетных направлений. Это предполагает не только создание технических средств защиты самих моделей машинного обучения (например, от отравления данных или так называемых состязательных атак), но и внедрение стандартов, обеспечивающих понятность и объяснимость решений, которые принимают интеллектуальные системы. Пользователь и общество в целом должны понимать, почему система приняла то или иное решение, особенно когда речь идет о безопасности.

3. Правовое регулирование должно успевать за технологическим развитием, а в идеале – создавать условия для него, минимизируя при этом риски. В этом контексте заслуживает поддержки идея о необходимости систематизации информационного законодательства. Существующий сегодня массив разрозненных нормативных актов действительно нуждается в упорядочивании. Разработка и принятие Цифрового кодекса могли бы стать решением этой проблемы. Такой документ мог бы объединить нормы, регулирующие электронную подпись, оборот персональных данных, использование информационных систем, а также закрепить базовые принципы ответственности при применении технологий искусственного интеллекта, в том числе в сфере информационной безопасности.

Кроме того, перспективным представляется подход, связанный с созданием специализированного программного обеспечения на базе ИИ для задач защиты информации и его апробацией в рамках экспериментальных правовых режимов, так называемых «регуляторных песочницах». Это позволило бы в контролируемых условиях отработать механизмы взаимодействия человека и интеллектуальной системы, выявить возможные проблемы и на практике определить, каким образом должна распределяться ответственность разработчиков, операторов и пользователей таких систем.

4. Нельзя забывать об организационных и человеческих факторах. Технологии сами по себе не создают культуру безопасности. Как показывает практика, достижение «цифровой зрелости» органов власти и организаций, а также системное повышение осведомленности и обучение персонала являются не менее важными элементами защиты, чем самые современные программно-аппаратные комплексы. Сотрудник, который понимает риски фишинга и методов социальной инженерии, включая угрозы, генерируемые с помощью искусственного интеллекта, становится не слабым звеном, а дополнительным рубежом обороны.

Подводя итог, можно сказать, что будущее кибербезопасности видится не в противостоянии человека и машины, а в их эффективном взаимодействии, в симбиозе. Задача научного сообщества, разработчиков и государства заключается в том, чтобы сделать этот симбиоз максимально продуктивным и безопасным, превратив искусственный интеллект из источника новых угроз в надежного помощника и защитника информационного суверенитета.

Д. И. Рыжков,

аспирант кафедры информационного права и цифровых технологий
ФГАОУ ВО «Московский государственный юридический университет имени О. Е. Кутафина»,
г. Москва

Нормативно-правовое регулирование безопасности устройств интернета вещей как инструмент профилактики ботнет-активности

Стремительное развитие технологий интернета вещей (англ. Internet of Things, далее – IoT) привело к фундаментальному изменению ландшафта информационной безопасности. Количество подключённых к сети устройств уже превысило 20 миллиардов, и, по прогнозам исследователей, к 2030 году их число возрастёт многократно[225]. При этом IoT охватывает не только бытовые «умные» устройства – лампочки, колонки и роботы-пылесосы, – но и промышленные системы, энергетические сети, медицинские приборы и транспортную инфраструктуру.

Одновременно с ростом экосистемы IoT экспоненциально растёт и количество кибератак, использующих уязвимости данных устройств. Злоумышленники формируют масштабные ботнеты – сети из десятков и сотен тысяч скомпрометированных устройств, способных генерировать DDoS-атаки беспрецедентной мощности. По данным аналитического центра StormWall, с января по октябрь 2025 года количество DDoS-атак с использованием IoT-устройств в России увеличилось в пять раз,

[225] См.: State of IoT 2025: Number of connected IoT devices growing 14 % to 21.1 billion globally [Электронный ресурс] // IoT Analytics. URL: https://iot-analytics.com/number-connected-iot-devices/ (дата обращения: 10.11.2025).

а доля таких инцидентов возросла с 7 до 35 %[226]. Специалисты компании Curator зафиксировали ботнет, состоящий из 1,33 млн устройств, – почти в шесть раз больше, чем крупнейший ботнет 2024 г.[227].

Ботнет представляет собой распределённую сеть скомпрометированных устройств, управляемых из единого центра. IoT-ботнеты эксплуатируют уязвимости «умных» устройств: использование стандартных учётных данных (admin/admin, root/12345), отсутствие шифрования трафика, а также невозможность обновления программного обеспечения.

Объективные данные свидетельствуют о стремительном нарастании угрозы IoT-ботнетов. В октябре 2024 г. компания Cloudflare зафиксировала рекордную DDoS-атаку мощностью 5,6 Тбит/с, осуществлённую ботнетом на базе Mirai с использованием более 13 000 IoT-устройств. За весь 2024 г. Cloudflare заблокировала 21,3 млн DDoS-атак – на 53 % больше по сравнению с 2023 годом, при этом ежечасно предотвращалось в среднем 4 870 атак[228].

В России ситуация не менее тревожна. Хакеры формируют ботнеты из домашних роутеров, камер видеонаблюдения и умных гаджетов, создавая сети из десятков тысяч заражённых устройств. Мощность отдельных атак достигала 1–1,5 Тбит/с, а крупнейший обнаруженный ботнет на территории России включал 118 тысяч IoT-устройств[229]. Больше всего пострадали финансовые организации (32 %), ритейл (26 %), телеком (14 %), индустрия развлечений (12 %) и логистика (9 %)[230].

Роскомнадзор в своём отчёте за 2025 г. зафиксировал 100-процентный рост DDoS-атак и указал, что «в подавляющем большинстве случаев речь идёт об использовании распределённых ботнетов, сформированных из скомпрометированных серверов, облачных виртуальных машин и конечных устройств»[231].

Правовое регулирование безопасности IoT в России носит фрагментарный характер и не представлено в виде единого специализированного закона. Регулирование осуществляется комплексом нормативных правовых актов общего характера.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает общие требования к обеспечению защиты информации, включая обязанность обладателя информации и оператора информационной системы обеспечивать предотвращение несанкционированного доступа к информации и своевременное обнаружение фактов несанкционированного доступа[232]. Данные нормы применимы к IoT-устройствам, однако не учитывают их специфику.

Стратегическое значение IoT закреплено в Указе Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», который определяет интернет вещей как «концепцию вычислительной сети, соединяющей вещи (физические предметы), оснащённые встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека»[233].

Существенный вклад в формирование правового обеспечения информационной безопасности интернета вещей вносит деятельность Технического комитета по стандартизации № 194 «Киберфизические системы». Так, в 2024 году Росстандарт утвердил ГОСТ для интернета вещей – национальный стандарт протокола NB-IoT, устанавливающий требования для оборудования и устройств беспроводной передачи данных, режимы энергосбережения и архитектуру сети передачи пакетов[234].

---

[226] См.: StormWall: с января по октябрь 2025 года количество DDoS-атак с умных устройств в России выросло в 5 раз [Электронный ресурс] // CNews. URL: https://safe.cnews.ru/news/line/2025-12-01_stormwall_s_yanvarya_po_oktyabr (дата обращения: 11.01.2026).

[227] См.: DDoS-атаки, боты и BGP-инциденты в 1 квартале 2025 года: статистика и тренды [Электронный ресурс] // QruatorLabs. URL: https://blog.qrator.net/ru/ddos-ataki-boty-i-bgp-incidenty-v-1-kvartale-2025_213/ (дата обращения: 01.12.2025).

[228] См.: Восстание машин началось с кухни: IoT-ботнет установил рекорд DDoS-атаки [Электронный ресурс] // SecurityLab.ru. URL: https://www.securitylab.ru/news/555715.php (дата обращения: 12.12.2025).

[229] См.: StormWall: с января по октябрь 2025 года количество DDoS-атак с умных устройств в России выросло в 5 раз [Электронный ресурс] // CNews. URL: https://safe.cnews.ru/news/line/2025-12-01_stormwall_s_yanvarya_po_oktyabr (дата обращения: 11.01.2026).

[230] Там же.

[231] Роскомнадзор зафиксировал 100 %-й рост DDoS-атак за 2025 год [Электронный ресурс] // Коммерсант. URL: https://www.kommersant.ru/doc/8361498 (дата обращения: 01.02.2026).

[232] См. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

[233] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента РФ от 9 мая 2017 г. № 203 // Собрание законодательства РФ. 2017. № 20. ст. 2901.

[234] ГОСТ Р 59026-2024. Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных NB-IoT. Основные параметры (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 07 октября 2024 г. № 1399-ст. М. : Рос. ин-т стандартизации, 2024.

Между тем наиболее существенным пробелом российского законодательства в контексте профилактики ботнет-активности является полное отсутствие обязательных минимальных требований безопасности, предъявляемых к потребительским IoT-устройствам. Именно данная категория устройств – домашние роутеры, IP-камеры, «умные» колонки, бытовые приборы с Wi-Fi-модулем – составляет подавляющее большинство «узлов» в современных ботнетах.

Кроме того, отсутствие законодательного запрета на выпуск IoT-устройств со стандартными заводскими паролями является, пожалуй, наиболее прямой правовой причиной формирования ботнетов. Ботнет Mirai, ставший «эталонным» инструментом для DDoS-атак, был построен именно на эксплуатации стандартных учётных данных, содержащих не более 62 комбинаций логинов и паролей типа «admin/admin», «root/root», «default/default»[235]. Несмотря на очевидность данной уязвимости, российское законодательство не содержит ни запрета на использование стандартных паролей, ни требования к производителям генерировать уникальные учётные данные для каждого устройства, ни обязанности предусмотреть принудительную смену пароля при первом включении.

Великобритания, напротив, стала первой страной в мире, законодательно запретившей продажу IoT-устройств со стандартными паролями. PSTI Act, вступивший в силу 29 апреля 2024 года, устанавливает требование о том, что производитель не должен поставлять устройства, которые используют пароли по умолчанию, которые могут быть легко обнаружены в сети и являются общими для всех устройств. Если используется пароль по умолчанию, злоумышленник может войти в умное устройство и использовать его для доступа к локальной сети или проведения кибератак[236].

Другой критической проблемой является отсутствие в российском праве нормативных требований к обеспечению обновления программного обеспечения IoT-устройств. Значительная часть устройств, представленных на российском рынке, либо не имеет механизма обновления прошивки, либо содержит уязвимости, которые производитель никогда не устраняет после поставки.

Так, Директива Европейского союза 2022/2025 от 14 декабря 2022 года расширяет требования к кибербезопасности на критическую инфраструктуру, включая энергетику, транспорт, здравоохранение и цифровую инфраструктуру, в том числе IoT-устройства, используемые в этих секторах, обязывая обеспечивать регулярные обновления программного обеспечения и установку патчей[237].

Специфической проблемой, связанной с IoT-ботнетами, является «скрытая» обработка данных, при которой незаявленный сбор и использование информации происходит без явного согласия пользователей. Многие IoT-устройства собирают данные, которые не обязательно необходимы для их заявленной функциональности, например анализ местоположения для рекламных целей без уведомления пользователя.

Следовательно, одним из пробелов российского законодательства является отсутствие юридических санкций за выпуск на рынок небезопасных устройств интернета вещей. Действующий механизм правового регулирования предусматривает ответственность для субъектов критической информационной инфраструктуры и операторов персональных данных, но практически не затрагивает производителей соответствующих категорий устройств.

Таким образом, следует отметить, что стремительный рост экосистемы интернета вещей при отсутствии требований к их безопасности превращает потребительские устройства интернета вещей в один из ключевых источников ботнет-активности и масштабных DDoS-атак. В системе российского законодательства необходимо обеспечить переход от общего и рекомендательного регулирования к специализированной системе правовых норм, устанавливающих минимальные стандарты кибербезопасности устройств интернета вещей, и обеспечить обязательную интеграцию требований безопасности на стадиях проектирования, производства и эксплуатации устройств.

---

[235] См.: Weak default IoT passwords targeted by new UK law [Электронный ресурс] // TechHive. URL: https://www.techhive.com/article/2318294/weak-default-iot-passwords-targeted-uk-law.html (дата обращения: 01.12.2025).

[236] Там же.

[237] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [Электронный ресурс] // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555 (дата обращения: 01.02.2026).

А. Н. Сабуров,
аспирант 3 года обучения, «Уголовно-правовые науки»,
ИПСУБ ФГБОУ ВО «Удмуртский государственный университет».
Научный руководитель: В. Е. Зварыгин, к.ю.н., доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Международный опыт противодействия «фейковизации» общественно значимой информации уголовно-правовыми средствами на примере государств – участников и партнеров объединения БРИКС

В последние годы объединение государств БРИКС играет все большую роль на мировой арене, поскольку количество участников объединения увеличивается за счет новых членов из среды наиболее стремительно развивающихся экономик мира и крупнейших стран по численности населения. Укрепляются их взаимоотношения не только на почве решения общих вопросов и проблем экономического развития, внешней торговли, развития высоких технологий, культурных связей, но и в правовом поле и вопросам информационной безопасности. В особенности это проявляется на фоне происходящих в мире военных конфликтов, террористических актов, стихийных бедствий и эпидемий, когда «фейковизация» новостей, распространение ложных сведений способны нанести непоправимый ущерб как отдельным гражданам, так и обществу и государству в целом.

Российская Федерация как один из ведущих членов объединения БРИКС может заимствовать некоторые положения из уголовного законодательства других стран в целях международного уголовно-правового сотрудничества в общей борьбе с тотальной «фейковизацией» информационного пространства, не имеющего границ и пределов, и возможной гармонизации законодательства в сфере противодействия распространению ложной общественно значимой информации уголовно-правовыми средствами.

Приверженность укреплению информационной безопасности граждан в государствах – участниках БРИКС международному сотрудничеству в данной области была неоднократно выражена в декларациях ежегодных саммитов БРИКС[238], проходивших в том числе и в России (2009, 2015, 2020, 2024 гг.). Так, в п. 41 Московской декларации XII саммита БРИКС от 17.11.2020 подчеркивается важность разработки единой нормативно-правовой базы стран – участников БРИКС для противодействия растущему использованию в преступных целях информационно-коммуникационных технологий[239]. А в п. 40 декларации, принятой 23.10.2024 в г. Казани по итогам XVI саммита БРИКС, указана необходимость достижения взаимопонимания в области сотрудничества правоохранительных органов в сфере кибербезопасности[240].

Обратимся к опыту некоторых государств – участников и партнеров БРИКС в части уголовно-правового противодействия распространению ложных социально значимых сведений.

Китайская Народная Республика (КНР) по праву занимает одно из лидирующих мест в мире не только в области цифровизации и развития информационных технологий, но и в законодательном регулировании общественных отношений, связанных с распространением информации в обществе и использованием при этом искусственного интеллекта.

Еще в 2001 г. в Уголовный кодекс КНР была введена статья 291-1, предусматривающая уголовное наказание в виде лишения свободы на срок до 5 лет и более за создание ложной информации о радиоактивной или биохимической опасности либо за умышленное распространение заведомо ложной, как сказано в законе, «террористической информации», в результате чего произошло значительное нарушение общественного порядка или наступили некие «серьезные последствия». В 2015 г. была введена часть 2 в указанную статью, по которой за формирование или умышленное распространение на информационных платформах или в средствах массовой информации заведомо ложных слухов о стихийных бедствиях, эпидемиях, действиях правоохранительных органов, тем самым

[238] Муратшина К. Г. К вопросу о сотрудничестве в области информационной безопасности в рамках БРИКС // Гуманитарное знание и искусственный интеллект: стратегии и инновации : 4-й молодежный конвент УрФУ : материалы Междунар. конф., 26 марта 2020 года. Екатеринбург : Изд во Урал. ун та, 2020. С. 616.

[239] Декларация, принятая по итогам саммита БРИКС в г. Москва [Электронный ресурс] // Официальный сайт Президента РФ. 17.11.2020. URL: http://www.kremlin.ru/supplement/5581?ysclid=mmkpqfp2zb715810496 (дата обращения: 09.03.2026).

[240] Декларация, принятая по итогам саммита БРИКС в г. Казани [Электронный ресурс] // Совместный сайт министерств иностранных дел государств-участников БРИКС. БРИКС Документы. URL: https://infobrics.org/ru/documents/ (дата обращения: 09.03.2026).

повлекшее «серьезное нарушение общественного порядка» (в этом случае предусматривается лишение свободы до трех лет) или тяжкие последствия (лишение свободы от трех до семи лет)[241].

С 2020 г. вступили в силу поправки в законодательство КНР касательно распространения так называемого «синтетического контента», в частности дипфейков. Полного запрета на их создание и использование не последовало, однако теперь любой информационный и новостной «продукт» в текстовом, голосовом, биометрическом виде или видеоролик, созданный с использованием технологий искусственного интеллекта, «смены лица» или виртуальной реальности, должен в обязательном порядке иметь соответствующую пометку-предупреждение об этом. Публикация такого материала в информационно-коммуникационной сети «Интернет» без необходимого указания-маркировки о его «синтетическом» происхождении может повлечь за собой уголовную ответственность[242].

Республика Казахстан является государством – партнером объединения БРИКС с 2025 г. В данной стране по аналогии с законодательством Российской Федерации действует одновременно комплекс сразу из нескольких законов, направленных на противодействие распространению дезинформации и «фейковизации».

Базовым нормативным положением в данной области выступает статья 274 «Распространение заведомо ложной информации» Уголовного кодекса Республики Казахстан[243]. По части первой указанной статьи уголовная ответственность наступает при распространении заведомо ложной для субъекта преступления информации, которая способна создать опасность нарушения общественного порядка, а равно существенного нарушения прав и законных интересов граждан, организаций, общества и государства. В данном случае предполагается наказание до 1000 месячного расчетного показателя (фиксированная величина, использующаяся в Казахстане для расчетов социальных пособий, льгот, штрафов, налогов и так далее), исправительные либо общественные работы до 400 часов, или лишение либо ограничение свободы на срок до одного года.

Часть 2 статьи 274 предусматривает такие квалифицирующие признаки, как совершения деяния по части 1 группой лиц по предварительному сговору; с использованием лицом своего служебного положения; с использованием онлайн-платформ, телекоммуникационных сетей и массмедиа. Наказывается деяние штрафом в размере до 3000 месячных расчетных показателей либо исправительными или общественными работами на срок до 800 часов, либо ограничением или лишением свободы на срок до 3 лет.

В части 3 статьи 274 УК Республики Казахстан предусмотрен материальный состав преступления с последствиями совершения деяния по части 1-2 в виде причинения гражданину, организации или государству крупного ущерба, или наступления иных тяжких последствий, величины и характеристики которых определены в статье 3 УК Республики Казахстан «Разъяснение некоторых понятий, содержащихся в настоящем Кодексе» в пп. 4 и 38 соответственно. Наказание – штраф в размере до 5000 месячных расчетных показателей либо исправительные или общественные работы на срок до 1200 часов, либо ограничение или лишение свободы на срок до 5 лет.

В части 4 предусматривается еще более жесткое наказание – ограничение или лишение свободы на срок от 3 до 7 лет – за деяния по части 1-3, совершенные преступной группой; «в условиях чрезвычайного положения или в боевой обстановке, или в военное время, либо при проведении публичных мероприятий»[244].

В Казахстане также действует отдельный закон «Об онлайн-платформах и онлайн-рекламе» от 10.07.2023 № 18-VIII, где закреплено легальное определение понятия «ложная информация». По логике законодателя, которая в целом соотносится с логикой российского законодателя, изложенной в Федеральном законе «Об информации, информационных технологиях и о защите информации»[245], ложная информация представляет собой зафиксированную в любой форме информацию, не соответствующую действительности либо содержащую существенные искажения фактов, создающую ложное представление о лицах, предметах, событиях, процессах и явлениях.

---

[241] Уголовный кодекс Китайской Народной Республики / под общ. ред. проф. А. И. Чучаева и проф. А. И. Коробеева, пер. с китайского: проф. Хуан Даосю. 2-е изд. М. : ООО «Юридическая фирма «Контракт», 2021. С. 150–151.

[242] Дремлюга Р. И., Моисейцев В. В., Парин Д. В., Романова Л. И. Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (deepfake): опыт Китая // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. Т. 24, № 4. С. 98.

[243] Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V (с изм. и доп. по состоянию на 08.03.2026) [Электронный ресурс] // ИС Параграф. URL: https://prg.kz/document/?doc_id=31575252&pos=4538;84 (дата обращения: 09.03.2026).

[244] Там же.

[245] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 09.03.2026).

Республика Узбекистан с июля 2025 г. является государством – партнером БРИКС. Узбекское уголовное законодательство в сфере распространения социально значимой лжи сводится к двум статьям – ст. 244^5 и 244^6 УК Республики Узбекистан[246].

Первой из указанных выше статей установлена уголовная ответственность за распространение не соответствующих действительности сведений о распространении карантинных и других опасных для человека инфекций в условиях возникновения и распространения карантинных и других опасных для человека инфекций. Наказание за данные деяния – штраф до 200 базовых расчетных величин или обязательные общественные работы до 300 часов либо исправительные работы до 2 лет. Квалифицирующим признаком по части 2 статьи 244^5 является распространение сведений в печатном или иным способом размноженном тексте либо в СМИ, а также в Интернете, что влечет наказание вплоть до ограничения или лишения свободы до 3 лет.

По ч. 1 ст. 244^6 УК Республики Узбекистан за распространение ложной, унижающей достоинство личности или дискредитирующей ее информации, в том числе в СМИ и Интернете, при наличии административной преюдиции за подобное деяние, лицо может быть подвергнуто наказанию исправительными работами или ограничением свободы на срок до 2 лет. Аналогично наказывается по ч. 2 ст. 244^6 распространение ложных сведений, содержащих угрозу общественному порядку или безопасности, при отсутствии признаков преступлений экстремистской направленности.

Квалифицирующими признаками по ч. 3-4 указанной статьи, влекущие наказание вплоть до ограничения свободы до 3 лет, являются повторность или рецидив; причинение крупного или особо крупного ущерба; совершение означенных выше деяний во время массовых мероприятий или при чрезвычайной ситуации; наступление тяжких последствий; деяния, совершенные организованной группой или в ее интересах.

Малайзия, являясь с 2025 г. партнером БРИКС, стала одним из государств-пионеров, первыми предпринявшими попытку противодействия «фейковизации» информационного пространства уголовно-правовыми средствами.

В УК Малайзии присутствует ст. 124I, согласно которой тюремным заключением на срок до 5 лет наказывается лицо, распространившее ложные сообщения устно, письменно, электронными или любыми иными средствами или сделавшее ложное заявление, которое может вызвать тревогу в обществе[247].

Помимо данного положения с 2018 г. в Малайзии действует Anti-fake news Act 2018 (Act 803), где среди прочего законодатель закрепил понятия «публикация», «фейковые новости» и другие, установил юридическую ответственность, в том числе и уголовную, за их распространение[248].

В указанном выше нормативно-правовом акте «фейковые новости» понимаются как любые сведения, отчеты, новостные сводки в любой форме, способной передавать информацию, являющиеся частично или полностью ложными. «Публикация», согласно закону, подразумевает любую письменную публикацию либо обладающую аналогичными с письменной публикацией свойствами, созданной любым способом. Отдельно стоит упомянуть, что к публикации приравнивается любое ее копирование, полное или частичное воспроизведение не автором – так называемые «репосты»[249].

Малайзийский «Антифейковый закон» в статье 4 предусматривает уголовную ответственность для субъектов преступных деяний, выраженных в злонамеренном создании, опубликовании, предложении, финансировании, поставке, передаче или распространении любых фейк-новостей в любом формате или публикации, содержащие такие фейк-новости. Указанные деяния влекут за собой достаточно суровые уголовные наказания вплоть до лишения свободы на срок до 6 лет. При рецидиве преступления суд вправе назначить штраф в размере до 3 000 ринггитов за каждый день, следующий за днем вынесения обвинительного приговора. Кроме того, помимо указанных наказаний субъекта преступления могут обязать принести извинения лицам, пострадавшим от распространения ложных сведений.

При этом в статье 6 также закрепляется обязанность администраторов, модераторов информационных площадок незамедлительно удалять публикации, содержащие фейк-новости. В противном случае таким лицам грозит наказание в виде штрафа в размере до 100 000 ринггитов. Если даже после

---

[246] Уголовный кодекс Республики Узбекистан от 22.09.1994 № 2012-XII (с изм. и доп. по состоянию на 06.03.2026) [Электронный ресурс] // ИС Параграф. URL: https://prg.kz/document/?doc_id=30421110 (дата обращения: 09.03.2026).

[247] Уголовный кодекс Малайзии от 07.08.1994 № 574 (в ред. от 04.06.2015) [Электронный ресурс] // Библиотека Resilience. Ресурсы Юго-Восточной Азии. URL: https://www.rcrc-resilience-southeastasia.org/wp-content/uploads/2017/12/Penal-Code-Act-574 (дата обращения: 07.03.2026).

[248] Щербаков А. Д. Fake news как объект уголовно-правовой регуляции: опыт Малайзии // Международное уголовное право и международная юстиция. 2018. № 4. С. 20.

[249] Anti-Fake News Act 2018 [Act 803] [Электронный ресурс] // CYRILLA: Global Digital Rights Law. URL: https://cyrilla.org/en/document/i675szk3h8m?page=4 (дата обращения: 07.03.2026).

вынесения приговора фейковая публикация не удалена, то за каждый день нарушения начисляются штрафные санкции вплоть до 3 000 ринггитов[250].

Таким образом, рассмотрев уголовное законодательство некоторых государств – участников и партнеров объединения БРИКС, можно констатировать, что некоторые из них значительно продвинулись в регулировании противодействия распространению фейк-информации, имеющей социально важное значение. Целесообразным видится применение в Российской Федерации опыта КНР касаемо уголовно-правовой регламентации использования «синтетического контента» в создании и распространении информационных материалов. Кроме того, по аналогии с уголовными законами Казахстана и Узбекистана необходимо включить в соответствующие статьи УК РФ такой квалифицирующий признак, как распространение фейков при помощи СМИ и Интернета. Также представляется разумным перенять некоторые положения малайзийского «антифейкового законодательства», например ужесточение ответственности владельцев онлайн-платформ за нарушение судебного требования удалить фейк-сведения из общего доступа. Данные изменения могли бы повысить эффективность противодействия распространению ложной социально значимой информации в Российской Федерации.

М. С. Чернышов,

аспирант кафедры информационного права и цифровых технологий ФГАОУ ВО «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)», г. Москва

Актуальные проблемы легального определения понятия «искусственный интеллект» в отечественном законодательстве в контексте обеспечения информационной безопасности

Искусственный интеллект (**ИИ**) стремительно проникает в самые разные сферы жизни, вследствие чего задача формулирования корректного юридического определения этого явления приобретает принципиальное значение для обеспечения правовой определённости в целом. Данная проблема приобретает особую остроту в контексте угроз информационной безопасности: размытость и неопределенность термина может влечь за собой пробелы в регулировании и создавать «серые зоны», которые могут использоваться как недобросовестными участниками рынка, так и злоумышленниками, использующими системы ИИ.

Проблема формулирования корректного определения понятия «искусственный интеллект» имеет значение для обеспечения информационной безопасности Российской Федерации на законодательном уровне. Как отмечается в Доктрине информационной безопасности Российской Федерации, обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами[251].

В августе 2025 года Правительство Российской Федерации утвердило План мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий[252]. Помимо прочего, в Плане мероприятий предусмотрены меры, направленные на контроль за использованием искусственного интеллекта. Представляется, что для корректной и эффективной реализации таких мер понадобится разработка нормативно-правовых актов, содержащих адекватное и релевантное определение термина «искусственный интеллект».

Таким образом, вопрос выработки юридически корректного определения понятия «искусственный интеллект» является важнейшей предпосылкой для эффективного правового регулирования в сфере информационной безопасности Российской Федерации.

---

[250] Anti-Fake News Act 2018 [Act 803] // CYRILLA: Global Digital Rights Law [Электронный ресурс]. URL: https://cyrilla.org/en/document/i675szk3h8m?page=4 (дата обращения: 06.03.2026).

[251] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646 [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 08.03.2026).

[252] Об утверждении Плана мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий : распоряжение Правительства РФ от 14.08.2025 № 2207-р [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 08.03.2026).

В зависимости от контекста понятием «искусственный интеллект» можно охватить широкий набор технологических и программных компонентов, к которым, в частности, можно отнести алгоритмы машинного обучения, процессы обработки данных, алгоритмы компьютерного зрения, робототехнику (способ интеграции искусственного интеллекта с киберфизическими системами). Под искусственным интеллектом также может пониматься сфера науки. С точки зрения информационной безопасности особую значимость приобретают те компоненты ИИ, которые непосредственно взаимодействуют с информационными системами и телекоммуникационными сетями: именно такие элементы могут выступать как вектором атаки, так и объектом несанкционированного воздействия злоумышленников.

Если обратиться к отдельным российским ведомственным нормативно-правовым актам, можно обнаружить следующие варианты определений искусственного интеллекта:

1. Министерство связи и массовых коммуникаций в 2018 году определило технологии искусственного интеллекта как «свойства автоматических систем брать на себя отдельные функции интеллекта человека, выбирать и принимать оптимальные решения на основе ранее полученного опыта и рационального анализа внешних воздействий»[253].

2. Министерство просвещения в 2020 году определило искусственный интеллект как «науку и технологию создания интеллектуальных машин, особенно интеллектуальных компьютерных программ; свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека»[254].

3. Росздравнадзор в ведомственной программе цифровой трансформации на 2022–2024 годы определил искусственный интеллект как «способность цифрового компьютера или управляемого компьютером робота выполнять задачи, обычно связанные с разумными существами»[255].

Действующее легальное определение искусственного интеллекта, которое на данном этапе можно считать ключевым для российского правопорядка, содержится в Национальной стратегии развития искусственного интеллекта до 2030 года[256] и в Федеральном законе от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве… » [257]. Указанное определение можно разделить на следующие составные элементы:

Искусственный интеллект – это:

1) комплекс технологических решений;

2) позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма);

3) позволяющий получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их;

4) комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений;

5) технологиями искусственного интеллекта являются технологии, основанные на использовании искусственного интеллекта (включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта).

---

[253] Об утверждении Разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов национальной программы «Цифровая экономика Российской Федерации» : приказ Минкомсвязи России от 01.08.2018 № 428 [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 08.03.2026).

[254] Об утверждении методических рекомендаций для внедрения в основные общеобразовательные программы современных цифровых технологий : распоряжение Минпросвещения России от 18.05.2020 № Р-44 [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 08.03.2026).

[255] Ведомственная программа цифровой трансформации Федеральной службы по надзору в сфере здравоохранения на 2022–2024 годы [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 08.03.2026).

[256] О развитии искусственного интеллекта в Российской Федерации : Указ Президента РФ от 10.10.2019 № 490 [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 08.03.2026).

[257] О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве, об особенностях обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» : Федеральный закон от 24.04.2020 № 123-ФЗ (ред. от 08.08.2024) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 08.03.2026).

Приведенное определение содержит ряд проблемных аспектов, на которые важно обратить внимание.

Так, учеными не первый год отмечается, что ссылка на «когнитивные функции» человека и критерий «сопоставимости» с результатами человеческой интеллектуальной деятельности в определении искусственного интеллекта является спорной. Указанные признаки подробно не раскрываются ни в отраслевом законодательстве, ни в общей теории права[258]. Очевидно, что такой подход к определению проистекает из устоявшейся дихотомии понятий «естественный интеллект – искусственный интеллект»; однако ее корректное юридическое использование серьезно осложнено неопределенностью понятия «естественный интеллект».

Специалисты предлагают при определении искусственного интеллекта не обращаться к аналогиям с умственными способностями человека, а использовать признак способности системы к достижению результатов, непредсказуемых для человека[259]. Данный подход представляется более конструктивным с точки зрения информационной безопасности: непредсказуемость поведения системы искусственного интеллекта прямым образом связана с вероятностью наступления вреда вследствие ошибочных действий системы ИИ, совершенных непредсказуемым для человека образом.

В связи с тем, что на текущем этапе научно-технологического развития искусственный интеллект всегда реализуется внутри какой-либо аппаратно-программной (киберфизической) оболочки, можно обоснованно предположить, что искусственный интеллект является в первую очередь информационной системой[260]. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (**Закон об информации**) определяет информационную систему как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Представляется, что такой подход позволит встроить определение искусственного интеллекта в уже сложившийся понятийный аппарат информационного законодательства (в котором уже раскрыты понятия информационной системы и её оператора).

Также квалификация системы ИИ в качестве информационной системы в смысле Закона об информации позволяет распространить на такую систему требования по защите информации, предусмотренные статьёй 16 указанного закона.

Представляется важным также обратить внимание на соотношение понятий «технологии искусственного интеллекта» и «системы искусственного интеллекта». С теоретической точки зрения «технологию искусственного интеллекта» можно определить как совокупность компьютерных алгоритмов, математических моделей и способов обработки информации, а «систему искусственного интеллекта» – как конкретную информационную систему, представляющую собой программное обеспечение или программно-аппаратный комплекс, функционирующую полностью или частично с использованием технологии искусственного интеллекта.

Если обратиться к иностранному опыту, то можно обратить внимание на то, что объектом правового регулирования зачастую выступают именно системы искусственного интеллекта. Так, положения Регламента Европейского союза об искусственном интеллекте регулируют порядок разработки и эксплуатации систем искусственного интеллекта (AI systems)[261]. В недавно принятом Цифровом кодексе Кыргызской республики система искусственного интеллекта определяется как цифровая технологическая система, которая на основе цифровых данных и заданного человеком набора целей способна с определенной степенью автономности формировать прогнозы, рекомендации или принимать решения, оказывающие влияние на состояние субъектов или объектов внешней среды[262].

В. Б. Наумов и Г. Г. Камалова предлагают следующее концептуальное определение: система искусственного интеллекта – это информационная система, которая на основе данных и с помощью алгоритмов машинного обучения или других технологий искусственного интеллекта с определенной степенью автономности осуществляет формирование прогнозов, рекомендаций, принятие решений или генерацию контента, оказывающего воздействие на физическую или информационную среду[263].

---

[258] Наумов В. Б., Камалова Г. Г. Вопросы построения юридических дефиниций в сфере искусственного интеллекта // Труды Института государства и права Российской академии наук. 2020. Т. 15, № 1. С. 81–93.

[259] На пути к юридическому определению искусственного интеллекта / В. В. Архипов, А. Ю. Брагинец, А. В. Грачева, В. Б. Наумов // Информационное право. 2021. № 4. С. 22–26.

[260] Там же.

[261] Artificial Intelligence Act [Электронный ресурс]. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата обращения: 08.03.2026).

[262] Цифровой Кодекс Кыргызской Республики [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru (дата обращения: 08.03.2026).

[263] Naumov V. B., Kamalova G. G. On the discussion regarding the legal conceptual framework in the field of artificial intelligence // State and Law. 2025. № 10. P. 92–97.

Таким образом, проведенный анализ показывает, что существующие в российском законодательстве дефиниции понятия «искусственного интеллекта» носят преимущественно описательно-антропоморфный характер («имитация когнитивных функций», «сопоставимость с человеком» и т. д.). Такой подход может стать препятствием для правоприменения в условиях массового использования технологии в будущем, когда возникнет потребность однозначно определить субъектный и объектный состав правоотношений с использованием искусственного интеллекта. Применительно к сфере информационной безопасности указанный недостаток влечёт невозможность точного определения объекта защиты, обязанного субъекта и применимых требований по защите информации.

Также представляется целесообразным включить в законодательный корпус понятие «систем искусственного интеллекта» как особой разновидности информационных систем, которые будут выступать непосредственным объектом правового регулирования. Закрепление данного понятия позволит распространить на системы ИИ режим защиты информации в информационных системах, установленный Законом об информации.

В. В. Собинский,

аспирант кафедры информационного права и цифровых технологий ФГАОУ ВО «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)», г. Москва

Проблемы организационно-правового и технологического обеспечения информационной безопасности России в условиях формирования правового регулирования оборота цифровых валют и стейблкойнов

Современный этап цифровой трансформации финансового рынка объективно изменяет содержание задач, стоящих перед российским государством в сфере обеспечения информационной безопасности. Если ранее традиционный вектор правового регулирования в данной области был сосредоточен преимущественно на защите государственных информационных систем, персональных данных и информационной инфраструктуры, то сегодня к числу системообразующих вызовов относятся также цифровые валюты, токенизированные формы имущественных прав, а в перспективе и стейблкойны как особый феномен пересечения денежной единицы и ценной бумаги, существующий в трансграничной сетевой инфраструктуре. Значимость данной проблематики усиливается тем, что действующая Стратегия национальной безопасности Российской Федерации относит информационную безопасность, экономическую безопасность и научно-технологическое развитие к числу самостоятельных стратегических приоритетов, а Доктрина информационной безопасности Российской Федерации связывает обеспечение суверенитета с устойчивым функционированием информационной инфраструктуры и защитой от внешних и внутренних угроз[264]. Именно поэтому правовое регулирование оборота цифровых валют не может рассматриваться изолированно как частный вопрос финансового или гражданского права. По существу, мы должны говорить о формировании новой межотраслевой системы правового регулирования, финансового суверенитета, цифрового суверенитета и национальной безопасности.

Отправной точкой для российского законодательства выступает Федеральный закон от 31.07.2020 № 259-ФЗ, закрепивший базовые подходы к цифровым финансовым активам и цифровой валюте[265]. Законодатель признал цифровую валюту совокупностью электронных данных, содержащихся в информационной системе, которые могут быть приняты в качестве средства платежа, но при этом не являются денежной единицей Российской Федерации, иностранного государства или международной расчетной единицей. В самой конструкции закона уже заключено принципиальное противоречие: цифровая валюта фактически описывается в том числе через экономические функции, сходные с платежным средством и инвестиционным активом, однако выводится за пределы традиционного денежного подхода. Такая модель изначально задала высокий уровень регуляторной неопределенности,

[264] О стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 02.07.2021 № 400 [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 12.02.2025).

[265] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31.07.2020 № 259-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 12.02.2025).

поскольку оборот цифровой валюты оказался признанным, но ограниченным ввиду правовой неопределенности, а ее правовой режим – неоднозначным с позиций налогового контроля, валютного регулирования и информационной безопасности. В научной литературе обоснованно отмечается, что правовая природа цифровой валюты в российском праве остается смешанной и не укладывается полностью ни в вещно-правовую, ни в обязательственно-правовую модель, что затрудняет выработку единых требований к субъектам оборота, инфраструктуре и режиму защиты информации[266].

Ситуация изменилась в 2024 г., когда был принят Федеральный закон от 08.08.2024 № 221-ФЗ, установивший правовые основы майнинга цифровой валюты, требования к субъектам соответствующей деятельности и ограничения на совмещение отдельных видов деятельности[267]. Также ранее на законодательном уровне была открыта возможность использования криптовалют в трансграничных расчетах по внешнеторговым договорам, но только в рамках экспериментального правового режима. Тем самым российский законодатель де-факто признал, что в условиях внешнеэкономических ограничений цифровые валюты способны рассматриваться как инструмент повышения автономности трансграничных расчетов. Однако такой шаг одновременно порождает качественно новые риски: чем шире вовлечение распределенных реестров и криптоинфраструктуры в международные расчеты, тем выше зависимость от зарубежных программных решений, валидаторов, сетевой маршрутизации, иностранных провайдеров ликвидности и внешних площадок хранения цифровых активов. Следовательно, расширение оборота цифровых валют объективно повышает требования к технологическому суверенитету, прослеживаемости транзакций, устойчивости шлюзовой инфраструктуры и процедурам верификации контрагентов.

Особую сложность для российской правовой системы представляет вопрос о стейблкойнах. В действующем федеральном законодательстве Российской Федерации данное понятие не закреплено как самостоятельная правовая категория, тогда как Банк России в аналитическом докладе 2024 года прямо указывает, что в мире пока отсутствуют единое определение и единые подходы к регулированию стейблкойнов, а сами они нередко сочетают черты традиционных и цифровых финансовых инструментов в различных комбинациях[268]. Отсюда следует важный вывод: стейблкойн не может быть автоматически отнесен исключительно к цифровой валюте в смысле Закона № 259-ФЗ, поскольку конкретная квалификация зависит от его экономической модели, способа обеспечения, характера обязательств эмитента, механизма выкупа, наличия централизованного оператора и особенностей обращения. В основе наиболее часто встречающейся классификации стейблкойнов лежит механизм, используемый для поддержания стабильности стоимости стейблкойнов относительно стоимости актива (корзины активов), к которому он привязан. По этому критерию выделяют следующие основные виды стейблкойнов:

– обеспеченные стейблкойны (например: USDT, USDC, DAI, PAXG) предусматривают формирование специального обеспечения за счет выделения активов;

– необеспеченные алгоритмические стейблкойны (например: FRAX, FEI) не предполагают формирования обеспечения, стабилизация относительно стоимости актива (корзины активов) обеспечивается с помощью специальных алгоритмов;

– гибридные стейблкойны (например IRON) предусматривают совмещение обеспечительного и алгоритмического механизмов.

При отсутствии специальной классификации российское регулирование неизбежно сталкивается с риском подмены правовых режимов: один и тот же инструмент может описываться как цифровая валюта или иностранное цифровое право. В организационно-правовом смысле это означает неопределенность состава надзорных полномочий Банка России, Росфинмониторинга, ФНС России, Роскомнадзора и правоохранительных органов, а в технологическом смысле – отсутствие единых обязательных требований к инфраструктуре эмиссии, резервирования, информационной безопасности и раскрытию информации о таких активах.

Проблема организационно-правового обеспечения информационной безопасности в рассматриваемой сфере состоит прежде всего в межотраслевом характере регулирования. Оборот цифровых валют и потенциальное обращение стейблкойнов находятся на стыке гражданского, финансового, информационного, административного и уголовного права. Такой межотраслевой характер сам по себе

---

[266] Хамуков А. А. Формирование правовой модели регулирования обращения криптовалют в России // Юридическая наука. 2024. С. 307.

[267] О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 08.08.2024 № 221-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 12.02.2025).

[268] Стейблкойны: опыт использования и регулирования: Центральный банк России, Аналитический доклад. 2024.

не является недостатком, но в российской модели он пока не подкреплен достаточной институциональной согласованностью. Общие отношения в сфере информации, информационных технологий и защиты информации регулируются Федеральным законом от 27.07.2006 № 149-ФЗ; режим персональных данных – Федеральным законом от 27.07.2006 № 152-ФЗ; основы национальной платежной системы – Федеральным законом от 27.06.2011 № 161-ФЗ; защита критической информационной инфраструктуры – Федеральным законом от 26.07.2017 № 187-ФЗ; противодействие легализации преступных доходов и финансированию терроризма – Федеральным законом от 07.08.2001 № 115-ФЗ. Однако между указанными законами отсутствует специальная «связка», предназначенная именно для инфраструктуры оборота цифровых валют и стейблкойнов. В результате вопрос о том, какие именно платформы, шлюзы обмена, кастодиальные сервисы, узлы, центры хранения ключей и аналитические сервисы должны подпадать под специальные требования к значимым субъектам критической инфраструктуры, остается открытым. Между тем в условиях роста киберугроз такая неопределенность создает пространство для регуляторных пробелов и распределения рисков на самих участников рынка.

Не менее существенной является проблема идентификации субъектов и формирования цифровой среды доверия. В научной литературе справедливо подчеркивается, что цифровая среда доверия невозможна без устойчивых юридических механизмов идентификации, анонимность либо псевдонимность в распределенных системах должна компенсироваться правовыми и технологическими процедурами верификации, дифференцированными в зависимости от уровня риска[269]. Для цифровых валют и стейблкойнов это имеет особое значение, поскольку сама технологическая архитектура блокчейн-сетей допускает быстрый трансграничный оборот активов при затрудненной идентификации конечных бенефициаров и источников происхождения средств. Законодательные и надзорные механизмы в сфере ПОД/ФТ не могут быть механически перенесены на цифровые сети без учета особенностей функционирования смарт-контрактов, некастодиальных кошельков, миксеров, кроссчейн-мостов и алгоритмических систем эмиссии. Организационно-правовой вызов состоит в том, чтобы сохранить баланс между законными интересами участников оборота, защитой частной жизни и задачами государственного контроля. В противном случае либо будет создана чрезмерно репрессивная модель, вытесняющая оборот в нелегальный сегмент, либо сохранится избыточная анонимность, несовместимая с задачами финансовой и информационной безопасности.

Технологическое измерение рассматриваемой проблемы не менее значимо, чем нормативное. В действительности информационная безопасность оборота цифровых валют и стейблкойнов определяется не только защитой информации как таковой, но и безопасностью вычислительной среды, устойчивостью алгоритмов консенсуса, надежностью средств управления криптографическими ключами, защищенностью интерфейсов интеграции, качеством смарт-контрактов, способностью к непрерывному мониторингу аномальной активности и готовностью к инцидентному реагированию. Для национальной платежной системы Банк России прямо указывает на необходимость развития независимых от глобальной инфраструктуры решений[270]. Из этого следует, что в сфере цифровых валют и стейблкойнов технологическая зависимость от внешней инфраструктуры становится не только коммерческим, но и стратегическим риском. Если инфраструктура расчета, хранения резервов, аудита смарт-контрактов, размещения нод или аналитики транзакций остается критически завязанной на зарубежные программные, облачные или биржевые решения, то устойчивость всего правового режима оказывается условной.

Таким образом, проблемы организационно-правового и технологического обеспечения информационной безопасности России в условиях формирования правового регулирования оборота цифровых валют и стейблкойнов носят комплексный характер. Их сущность заключается не просто в отсутствии отдельных правовых норм, а в необходимости согласовать несколько уровней регулирования: стратегический, отраслевой, институциональный и технологический. Российское право уже сформировало базовый каркас регулирования цифровой валюты и приступило к апробации специальных режимов для трансграничных расчетов. Вместе с тем стейблкойны по-прежнему находятся в «серой зоне» между существующими правовыми конструкциями, а требования к информационной безопасности соответствующей инфраструктуры остаются недостаточно конкретизированными. В этих условиях наиболее перспективной представляется модель, в которой правовое регулирование

[269] Химченко А. И. Формирование цифровой среды доверия: динамика развития инфраструктуры идентификации при реализации цифровых услуг [Электронный ресурс] // Legal Concept = Правовая парадигма. 2023. Т. 22, № 4. С. 54–63. URL: https://cyberleninka.ru/ (дата обращения: 13.02.2026).

[270] Основные направления развития национальной платежной системы на период 2025–2027 годов [Электронный ресурс] // Банк России. 2025. URL: https://www.cbr.ru/ (дата обращения: 13.03.2026).

цифровых валют и стейблкойнов строится на принципах технологического суверенитета, прослеживаемости, дифференциации рисков, приоритета публичной платежной инфраструктуры и нормативной предсказуемости для добросовестных участников оборота. Только при таком подходе информационная безопасность сможет выполнять не вспомогательную, а системообразующую функцию в механизме регулирования цифровых финансовых отношений.

А. В. Касаткин,
аспирант 3 года обучения, «Публично-правовые науки»,
ИПСУБ ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Цифровой суверенитет Российской Федерации в сфере экологического мониторинга Северного морского пути: правовые аспекты обеспечения информационной безопасности

Северный морской путь в последние годы из спокойного сюжета для узких специалистов превратился в политический и экономический символ, в котором переплетаются транзитные амбиции России, климатические изменения и, что особенно важно для юриста, растущая роль цифровых технологий в управлении этой сложной системой. В фокусе внимания оказываются уже не только атомный ледокольный флот и пропускная способность маршрута, но и то, как именно государство собирает, обрабатывает и защищает данные об окружающей среде в арктической акватории, какой режим доступа к этим данным устанавливает, и кто в итоге реально контролирует цифровую инфраструктуру. При более глубоком рассмотрении вопроса мы приходим к выводу, что вопрос здесь не только в «технике», а в суверенитете в самом прямом, юридически нагруженном смысле.

Экологический мониторинг Северного морского пути постепенно переходит на новые технологические рельсы: датчики, спутниковые системы, автоматизированные посты наблюдений, большие массивы данных, алгоритмы обработки и визуализации[271]. С точки зрения экологического права это выглядит почти как мечта – непрерывное, детальное, пространственно распределённое наблюдение за состоянием морской среды. Но параллельно возникает другая, менее привычная для классического эколого-правового дискурса, тема: кто владеет этим массивом данных, через какие цифровые контуры он циркулирует, где географически и юрисдикционно находятся серверы и какие уязвимости заложены в этой инфраструктуре. Здесь на первый план выходят информационная безопасность и цифровой суверенитет.

Если следовать логике российских исследований в области информационного права и безопасности, цифровой суверенитет сегодня трактуется как способность государства сохранять контроль над ключевой цифровой инфраструктурой, критическими данными и правилами их обработки[272]. Вопрос однозначного определения понятия «цифровой суверенитет» является острым вопросом для исследователей[273]. В российской науке данное понятие используется часто, но исследователи не дают однозначного определения. Для абстрактных сфер это можно обсуждать годами, но когда речь идёт о конкретном проекте, таком как Северный морской путь, теория очень быстро сталкивается с практикой, ведь данные мониторинга в Арктике – это не только научный ресурс и основа природоохранных решений, это ещё и чувствительная информация о состоянии морской среды, о загрязнениях, об аварийных выбросах, о фактическом поведении судов, которая в руках недружественных акторов вполне может превратиться в инструмент давления. На наш взгляд, недооценивать это сейчас – значит добровольно закладывать мину замедленного действия под эколого-правовой режим СМП.

---

[271] Скорина А. А. Создание системы экологического мониторинга Северного морского пути [Электронный ресурс] // Сайт международного делового форума «Большая Сибирь и Арктика». URL: https://bolshaya-sibir-arctica.ru/wp-content/uploads/2023/12/Био-Создание-системы-экологического-мониторинга.pdf (дата обращения: 12.02.2026).

[272] Кочетков А. П., Маслов К. В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе [Электронный ресурс] // Вестник Московского университета. Серия 12. Политические науки. 2022. № 2. URL: https://cyberleninka.ru/article/n/tsifrovoy-suverenitet-kak-osnova-natsionalnoy-bezopasnosti-rossii-v-globalnom-tsifrovom-obschestve (дата обращения: 15.02.2026).

[273] Маргарита Р.-К. Суверенитет и цифровой суверенитет [Электронный ресурс] // Journal of Digital Technologies and Law. 2023. № 3. URL: https://cyberleninka.ru/article/n/suverenitet-i-tsifrovoy-suverenitet (дата обращения: 15.02.2026).

В этой статье предлагается рассмотреть экологический мониторинг акватории Северного морского пути через призму цифрового суверенитета Российской Федерации, исходя не только из классических экологических и международно-правовых подходов, но и из накопленной за последние годы доктрины информационного права, где уже активно обсуждаются информационный суверенитет, кибербезопасность и защита критической инфраструктуры. Нам важно, чтобы разговор не сводился к лозунгам о «цифровом национальном контроле», а обнажал реальные правовые проблемы: фрагментарность регулирования, отсутствие специальных режимов доступа к экологическим данным, недосформированность статуса цифровых систем мониторинга как объектов, требующих особого режима безопасности. История фактически про стык трёх режимов: экологического, информационного и арктического.

Цель исследования можно сформулировать вполне прагматично: выявить и описать правовые аспекты обеспечения информационной безопасности в системе цифрового экологического мониторинга Северного морского пути, показав, каким образом концепция цифрового суверенитета может и должна быть «встроена» в действующее регулирование и в предлагаемые направления его развития. Нам важно ответить на вопрос: что именно должен и может делать российский законодатель (и правоприменитель), чтобы экологический мониторинг СМП был не только «цифровым» и «современным», но и действительно подконтрольным российской юрисдикции, устойчивым к внешним воздействиям и внятно встроенным в систему обеспечения национальной безопасности.

Понятие цифрового суверенитета в российской юридической науке уже успело обрасти своей историей, набором авторских трактовок и, честно говоря, даже некоторой модой. Как уже отмечалось выше, под этим термином обычно понимают способность государства самостоятельно определять правила существования и развития цифровой среды, контролировать ключевую инфраструктуру (от каналов связи до платформ) и осуществлять приоритетное воздействие на информационные потоки в пределах своей юрисдикции. В ряде работ цифровой суверенитет прямо увязывается с национальной и информационной безопасностью[274]: государство, которое утрачивает контроль над своими цифровыми ресурсами и данными, фактически теряет часть реального суверенитета, как бы пафосно это ни звучало. В более «технически» ориентированных исследованиях предлагается говорить о компонентах цифрового суверенитета: национальные поисковые системы и платформы, собственная криптография, отечественные системы хранения и обработки данных, национальные платежные решения, навигационные сервисы, средства защиты информации[275]. Если смотреть на проблему глазами юриста эколога, эти компоненты вдруг приобретают довольно неочевидный, но совершенно конкретный смысл: от того, на каком программном обеспечении и «железе» работает система экологического мониторинга, через какие каналы и платформы передаются данные, где физически расположен центр обработки, зависит не только удобство работы специалистов, но и то, может ли государство в любой момент обеспечить их целостность, конфиденциальность и доступность.

Есть ещё один важный сюжет, который, на наш взгляд, пока не до конца осознан в экологическом праве. Информация об окружающей среде традиционно рассматривается как благо, которое должно быть по возможности открытым, доступным, циркулирующим для науки, общественности и всех заинтересованных сторон. В российской и международной доктрине эта открытость закреплена очень глубоко: вспомним и Орхусскую конвенцию[276], и статью 42 Конституции Российской Федерации. Но когда речь идёт об Арктике и Северном морском пути, эта информация одновременно начинает играть роль стратегического ресурса: данные о состоянии льда, о загрязнениях, о характере грузопотоков и аварийных событиях могут использоваться вовсе не только в экологических целях. В результате возникает напряжение между традиционной установкой на максимальную открытость экологической информации и необходимостью вводить особые правовые режимы для её защиты.

На этом стыке, на наш взгляд, и появляется пространство для применения категории цифрового суверенитета к экологическому мониторингу. Речь не о том, чтобы «закрыть» данные и спрятать информацию от общества и науки – это был бы прямой шаг назад. Речь о том, чтобы юридически зафиксировать ключевые полномочия государства по управлению цифровой инфраструктурой мониторинга, определению режимов доступа, разграничению открытой и ограниченной информации, контролю над трансграничной передачей данных, если речь идёт о чувствительных сегментах. По сути,

---

[274] Бухарин В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО. 2016. № 6 (51). URL: https://cyberleninka.ru/article/n/kom-ponenty-tsifrovogo-suvereniteta-rossiyskoy-federatsii-kak-tehnicheskaya-osnova-informatsionnoy-bezopasnosti (дата обращения: 15.03.2026).

[275] Там же.

[276] Конвенция о доступе к информации, участии общественности в процессе принятия решений и доступе к правосудию по вопросам, касающимся окружающей среды (Орхусская конвенция). Принята 25 июня 1998 г.

цифровой суверенитет в этой сфере должен проявляться как способность России устанавливать и реализовывать собственные правила игры в отношении цифровых данных о состоянии арктической морской среды.

Если чуть отойти от абстракций и посмотреть, как устроен экологический мониторинг в акватории СМП, сразу бросается в глаза его многослойность. С одной стороны, есть классические элементы: единая система государственного экологического мониторинга, ведомственные системы наблюдений[277], научные программы[278], наблюдения, связанные с хозяйственной деятельностью компаний. С другой – всё активнее внедряются цифровые решения: автоматизированные станции, спутниковые и аэрокосмические методы, специализированные программно-аппаратные комплексы[279]. И вот здесь начинается интересное для юриста: изменения технологического уровня почти автоматически тянут за собой необходимость обновления правовой рамки.

Традиционная модель правового регулирования мониторинга, построенная вокруг распределения полномочий между органами, порядка обмена информацией и отчётности, начинает буксовать, когда возникает единая цифровая платформа, собирающая данные из разных источников в режиме, близком к реальному времени. Существующие проблемы были признаны Правительством РФ в «Стратегическом направлении в области цифровой трансформации отрасли экологии и природопользования… »[280]. Такое «сшивание» данных порождает новые вопросы: кто является оператором этой системы, на каком основании осуществляется обработка данных, каков правовой статус агрегированных массивов информации, может ли один из участников потребовать ограничения доступа к тем данным, которые ранее считались в большей степени «ведомственными». По сути, цифровизация усиливает интеграцию, а право пока ещё во многом остаётся фрагментированным.

Для Арктики и СМП это усиливается экстремальными природными условиями и повышенной экологической чувствительностью региона. Тут нельзя позволить себе роскошь «подождать», пока правовое регулирование само догонит технологические инновации. Любой серьёзный проект по развитию СМП предполагает наращивание интенсивности судоходства, строительства инфраструктуры, добычи полезных ископаемых и т. д., а значит, повышает риск техногенных аварий и загрязнений. Надёжный, оперативный и точный экологический мониторинг становится не просто желательной опцией, а обязательным элементом эколого-правового режима. Но чем сложнее и «цифровизованней» этот мониторинг, тем больше он уязвим с точки зрения информационной безопасности, и тем актуальнее становится вопрос о том, кто реально контролирует его «цифровое сердце».

Сейчас можно заметить, что государственная политика и ведомственные инициативы в сфере цифрового мониторинга и развития СМП идут параллельными, а местами пересекающимися курсами. С одной стороны, есть общие документы, где декларируется необходимость создания национальных автоматизированных систем мониторинга окружающей среды, внедрения цифровых технологий, использования больших данных и искусственного интеллекта[281]. С другой – существуют проекты, которые прямо касаются Арктики и Северного морского пути, где упоминаются цифровые системы поддержки судоходства, навигации и мониторинга условий[282].

Перейдём к более неприятной части – угрозам и уязвимостям. Как только мы признаём, что экологический мониторинг в акватории СМП опирается на сложную цифровую инфраструктуру, становится невозможно игнорировать риски кибератак, несанкционированного доступа к данным, вмешательства в работу датчиков и коммуникационных каналов. Для «классического» экологического права это звучит непривычно: мы привыкли говорить об источниках повышенной опасности, об обязанностях природопользователей, о государственном контроле, но почти не обсуждали возможность того, что экологические решения могут быть приняты на основе сознательно искажённой информации в результате атаки на систему мониторинга.

---

[277] Единая платформа цифровых сервисов Северного морского пути (ЕПЦС СМП) [Электронный ресурс] // Атомфлот. URL: https://rosatomflot.ru/epcs/ (дата обращения: 18.02.2026).

[278] Программа экологического мониторинга акватории Северного морского пути [Электронный ресурс] // Атоммедиа. URL: https://atommedia.online/reference/programma-ekologicheskogo-monitoringa-akvatorii-severnogo-morskogo-puti/ (дата обращения: 18.02.2026).

[279] Экомониторинг: как работают новейшие технологии для сохранения природы [Электронный ресурс] // РБК. URL: https://trends.rbc.ru/trends/industry/cmrm/6103afce9a79476310f6ad4b (дата обращения: 18.02.2026).

[280] Об утверждении стратегического направления в области цифровой трансформации отрасли экологии и природопользования, относящейся к сфере деятельности Министерства природных ресурсов и экологии Российской Федерации : распоряжение Правительства РФ от 15.12.2023 № 3664-р // СЗ РФ. 01.01.2024. № 1 (Ч IV). Ст. 280.

[281] Там же.

[282] Единая платформа цифровых сервисов Северного морского пути (ЕПЦС СМП) [Электронный ресурс] // Атомфлот. URL: https://rosatomflot.ru/epcs/ (дата обращения: 18.02.2026).

Между тем, если представить себе, как формируется картина состояния морской среды в арктической акватории – через датчики, спутники, автоматизированные посты, передачу данных по каналам связи, обработку на серверах, – становится очевидно, что на каждом этапе существует угроза вмешательства. Причём необязательно грубого и очевидного: достаточно чуть-чуть «зашумить» данные, изменить параметры, задержать сигнал, чтобы в итоге управляющие решения строились на неверной картине. Добавим сюда возможность компрометации систем хранения и обработки – и получим уже не просто экологический, а комплексный риск национальной безопасности. В Арктике цена ошибки особенно высока: климат хрупкий, последствия аварий долгосрочные, а репутационные издержки для государства могут быть очень серьёзными.

Именно здесь, как нам кажется, концепция цифрового суверенитета перестаёт быть отвлечённым лозунгом и приобретает вполне прикладной смысл. Если государство декларирует, что оно обеспечивает суверенитет в цифровой сфере, логично ожидать, что ключевые системы экологического мониторинга в стратегических регионах, включая СМП, находятся под его непосредственным контролем, используют защищённые каналы связи, опираются на сертифицированные средства защиты информации и не критично зависят от зарубежных программно-аппаратных решений. В противном случае получается парадоксальная ситуация: формально экологический мониторинг вроде бы осуществляется, но фактически его результаты и сама инфраструктура могут быть уязвимы для внешнего воздействия.

Проблема, однако, в том, что действующее законодательство пока не выстроило специальный правовой режим для систем цифрового экологического мониторинга, сопоставимый по степени детализации и уровню защиты с тем, который установлен для объектов критической информационной инфраструктуры (далее – КИИ). Да, отдельные такие системы могут быть отнесены к объектам КИИ, в частности, когда они интегрированы в инфраструктуру государственных органов или крупных компаний и отвечают установленным критериям значимости. Вместе с тем действующая модель регулирования не исходит из особенностей экологической информации, специфики Арктики и стратегического значения Северного морского пути, не выделяя системы цифрового экологического мониторинга Арктики и СМП в самостоятельный вид объектов либо в особый режим их защиты. При этом, хотя при категорировании КИИ ст. 7 Федерального закона от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025) предусматривает учет «экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду», сфера охраны окружающей среды как таковая прямо не поименована в п. 8 ст. 2 названного закона, что дополнительно подчеркивает отсутствие отраслевого, экологически ориентированного подхода к регулированию цифровых систем мониторинга в Арктике и на СМП.

Если попытаться «перевести» идею цифрового суверенитета и потребности информационной безопасности на язык правовых конструкций, вырисовывается несколько направлений, которые как минимум заслуживают обсуждения. Первое – это признание систем цифрового экологического мониторинга в акватории СМП объектами, требующими особого режима защиты, с учётом их значения для национальной и экологической безопасности. Это не обязательно должно означать автоматическое отнесение ко всей критической информационной инфраструктуре, но потребность в дифференцированном, а не общем режиме представляется довольно очевидной.

Второе направление связано с правовым режимом данных. Возможно, настало время честно сказать, что не вся информация экологического мониторинга в Арктике может и должна регулироваться по тем же правилам, что и обычная экологическая информация. Мы не предлагаем ломать принцип открытости, но кажется рациональным юридически закрепить категории данных, которые имеют повышенное значение и в силу этого подлежат особой защите, в том числе при трансграничной передаче. Здесь напрашиваются решения уровня специальных процедур согласования, согласованного доступа, введения моделей совместного контроля над предоставлением информации.

Третье – нормативное осмысление роли больших данных и искусственного интеллекта в системах мониторинга. Сейчас это во многом «серая зона»: технологии внедряются, алгоритмы принимают участие в обработке и интерпретации данных, но юридическая ответственность за их работу размыта. При этом в контексте Арктики и СМП последствия ошибок могут быть критическими. Представляется, что в ближайшие годы нам всё равно придётся ответить на вопросы о том, кто отвечает за использование автоматизированных аналитических систем, как проверяется корректность их работы, какие требования предъявляются к программному обеспечению, применяемому в системах мониторинга.

Наконец, четвёртое – так или иначе придётся синхронизировать стратегические документы в области цифрового развития, информационной безопасности, освоения Арктики и охраны окружающей среды. Сейчас каждое из этих направлений живёт в своём нормативном и институциональном измерении, а юристы-экологи вынуждены «собирать» общую картину по кускам. Северный морской

путь здесь, как ни странно, может стать удобной «лабораторией»: он достаточно важен, чтобы оправдать серьёзные институциональные и нормативные усилия, но достаточно конкретен, чтобы увидеть результаты этого синтеза не только на бумаге, но и в реальных управленческих практиках.

Не хочется завершать эту работу привычным набором фраз о «необходимости дальнейших исследований» и «важности комплексного подхода». Гораздо честнее сказать так: цифровой суверенитет в сфере экологического мониторинга Северного морского пути – это пока больше вопрос, чем ответ. Мы только начинаем понимать, какие именно правовые решения нужны, чтобы цифровая инфраструктура мониторинга не превратилась в ахиллесову пяту эколого-правового режима СМП. И в этом смысле сегодняшние дискуссии о цифровом суверенитете, кибербезопасности, эколого-правовом статусе Арктики – это не параллельные разговоры в разных аудиториях, а элементы одной большой, пока ещё плохо собранной мозаики.

Если попытаться сформулировать главный вывод: цифровизация экологического мониторинга Северного морского пути неизбежна и, по сути, уже состоялась, а вот правовое обеспечение цифрового суверенитета и информационной безопасности в этой сфере пока остаётся в зачаточном состоянии. Значит, у нас, юристов, есть незавидная, но интеллектуально честная задача – не только фиксировать этот разрыв, но и предлагать конкретные механизмы его преодоления: от изменения статуса информационных систем до уточнения режима данных и ответственности за цифровые решения. Хочется верить, что обсуждение подобных вопросов на площадках, посвящённых информационной безопасности, поможет сделать этот разговор не только академическим, но и практически значимым.

Н. К. Ш. Кагмени,
магистрант 1 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Г. Г. Камалова, д.ю.н., доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Особенности защиты персональных данных в Камеруне

В условиях стремительно развивающейся экономики 23 декабря 2023 года[283] Республика Камерун сделала решительный шаг в защите цифровых прав своих граждан, приняв Закон № 2024/017 о защите персональных данных[284].

Прежде чем продолжить, необходимо определить ключевые термины темы. Понятие «персональные данные» обозначает любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу[285]. Лицо считается «идентифицируемым», если оно может быть определено прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении или факторы, специфичные для его физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности[286]. Таким образом, это широкое понятие, охватывающее как классическую идентифицирующую информацию (фамилия, имя, адрес), так и более современные данные (IP-адрес, данные геолокации, отпечатки пальцев).

Сбор и обработка этих данных, если они не регулируются, могут нанести ущерб основным правам человека, в частности его частной жизни и личной свободе[287]. Именно поэтому во многих правовых системах появилась отрасль права, посвященная защите персональных данных. Ее можно определить как совокупность правовых норм, направленных на обеспечение того, чтобы информация о лице собиралась, обрабатывалась и хранилась законно, добросовестно и прозрачно, с соблюдением его основных прав и свобод[288]. Эта защита основывается на нескольких принципах: согласие лица,

[283] Закон № 2024/017 от 23 декабря 2023 года о защите персональных данных // Официальный журнал Республики Камерун. декабрь 2023 года.

[284] Там же.

[285] Статья 4 Регламента (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года (GDPR). См. также статью 2 Закона № 2024/017.

[286] Там же.

[287] Статья 8 Европейской конвенции по правам человека; статья 22 Конституции Камеруна.

[288] CNIL «Что такое защита данных?», 2026.

предварительное информирование, ограничение целей обработки, безопасность данных и признание субъективных прав (доступ, исправление, возражение, удаление).

Действительно, в условиях, когда растущая цифровизация экономики подвергает население новым рискам – киберпреступность, злоупотребление данными, неконтролируемая слежка – камерунский закон делает Камерун 38-й африканской страной, принявшей законодательство в этой области[289]. В то время как Общий регламент по защите данных (GDPR) стал международным стандартом[290], африканские государства в целом, и Камерун в частности, были вынуждены адаптировать эту модель к своим социальным, экономическим и культурным реалиям. Новая камерунская правовая база, также вдохновлённая международными конвенциями (например Малабской конвенцией 2014 года)[291], имеет заметные особенности. Они отличают её не только от европейской модели, но и от законодательств других стран, в частности Российской Федерации[292]. На этих особенностях стоит остановиться подробнее.

Актуальность данного исследования объясняется несколькими причинами. Во-первых, с теоретической и юридической точки зрения оно обогащает сравнительное правоведение в области защиты данных. Анализ африканских законов остаётся малоизученной областью – большинство исследований посвящены GDPR или западным законодательствам[293]. Новый камерунский закон позволяет понять, как универсальные принципы защиты данных применяются в конкретных экономических и культурных условиях. Во-вторых, с практической стороны понимание этих особенностей крайне важно для экономических операторов – государственных и частных. Они должны привести свою практику сбора и обработки данных в соответствие с законом под угрозой санкций[294]. Напрямую это касается банков, операторов связи, цифровых платформ и государственных органов. В-третьих, данное исследование представляет особый интерес для российской научной аудитории. Сравнение с европейской моделью может дать пищу для размышлений об альтернативных способах принятия решений по примеру стран с формирующейся рыночной экономикой в том смысле, что в России, принявшей собственное законодательство о персональных данных (Федеральный закон № 152-ФЗ от 2006 г.), также ведутся дебаты о балансе между цифровым суверенитетом и защитой прав личности. Поэтому можно задаться вопросом, в какой степени камерунский законодательный орган адаптировал международные стандарты защиты данных к национальным реалиям. Таким образом, подход заключается, во-первых, в том, чтобы представить общие рамки камерунского законодательства в соответствии с международными стандартами, обеспечивая при этом стремление к защите (I), затем показать 4 выявленные особенности, сравнив их с GDPR (II) и, наконец, показать проблемы реализации этого текста (III).

Часть I. Правовая основа, соответствующая международным стандартам

Камерунский закон № 2024/017, как и другие современные законодательства о защите данных, опирается на три столпа. Это фундаментальные принципы обработки, усиленные права лиц, и независимый контрольный орган.

I-1. Фундаментальные принципы обработки

В соответствии с международными стандартами камерунский закон закрепляет ряд фундаментальных принципов обработки персональных данных[295]. Первый принцип, который, кстати, является краеугольным камнем системы, – это принцип согласия. Действительно, согласно статье 10 Закона № 2024/017 обработка может осуществляться только при условии, что заинтересованное лицо дало явное согласие. Следует подчеркнуть, что требование явного согласия является более строгим, чем простое согласие по GDPR, и будет подробно проанализировано во второй части.

Другим принципом является законность и целевое назначение. Изложенный в статье 8, он требует, чтобы данные собирались для определенных, явных и законных целей. Последующая обработка, несовместимая с этими первоначальными целями, запрещена.

---

[289] Африканский союз, «Состояние защиты данных в Африке», 2026.

[290] Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (GDPR).

[291] Конвенция Африканского союза о кибербезопасности и защите персональных данных, принятая в Малабо 27 июня 2014 года.

[292] Федеральный закон России № 152-ФЗ от 27 июля 2006 года о персональных данных.

[293] Зенге Л.-Ф. Системы и выбор в области защиты персональных данных (Камерун). Village de la Justice, 2026.

[294] Статья 71 вышеупомянутого Закона № 2024/017 (санкции могут достигать 50 миллионов франков КФА).

[295] См., в частности, Antoine RENUCCI и Jean-François RENUCCI, Droit et protection des données à caractère personnel, LGDJ, coll. Manuels, 2022, для подробного изложения принципов GDPR.

Также существует принцип прозрачности. Он предусмотрен статьей 14 и обязывает оператора предоставлять заинтересованному лицу четкую и доступную информацию о личности оператора, целях обработки, получателях данных, а также о существовании прав на доступ, исправление и возражение.

Наконец, принцип пропорциональности и минимизации данных. Исходя из статьи 9, он требует, чтобы собирались и обрабатывались только те данные, которые являются адекватными, релевантными и не чрезмерными по отношению к преследуемой цели.

Следует отметить, что вышеупомянутые принципы, общие для большинства современных законодательств и подвергающиеся глубокому анализу в специализированной доктрине[296], свидетельствуют о включении Камеруна в глобальное движение за защиту данных. И это движение продолжается признанием прав заинтересованных лиц.

I-2. Усиленные права лиц

Камерунский закон предоставляет лицам, чьи данные собираются, ряд прав, позволяющих им сохранять контроль над своей личной информацией. При прочтении положений этого закона можно выделить 6 закрепленных прав. Первое – это право на доступ, изложенное в статье 28. Оно позволяет любому лицу получить от оператора подтверждение того, обрабатываются ли данные, касающиеся его, а также получить их в доступной форме.

Далее, право на исправление, предусмотренное статьей 29, позволяет лицу требовать исправления неточных или неполных данных о себе.

Кроме того, право на возражение, изложенное в статье 30, позволяет лицу возражать по законным основаниям против обработки его данных.

Кроме того, при прочтении статьи 31 право на удаление, также называемое «правом на забвение», обязывает контролёров данных удалять данные в определённых случаях. Например: отзыв согласия, законное возражение, данные, собранные незаконным образом, и истечение срока хранения. Право на переносимость, предусмотренное в статье 32, на самом деле является важным нововведением, поскольку оно позволяет человеку получать предоставленные им данные в структурированном, обычно используемом и машиночитаемом формате и передавать их контролёру данных. С другой стороны, статья 33 гарантирует право не подвергаться индивидуальному решению, основанному исключительно на автоматизированной обработке, включая профилирование, имеющее юридические последствия для личности. Эти права, сравнимые с правами по GDPR, ставят человека в центр системы[297] и предоставляют ему конкретные инструменты для осуществления эффективного контроля над своими данными. И именно с этой целью создается независимый орган, ответственный за соблюдение или применение этих прав.

I-3. Создание независимого органа

Камерун, учреждая Орган по защите персональных данных (APDP), не отступил от правила, согласно которому любое современное законодательство о защите данных должно сопровождаться созданием независимого административного органа, ответственного за контроль за его применением.

Действительно, статус и состав APDP определены в статьях 48-55. Орган состоит из членов, выбранных за их юридическую и техническую компетентность, назначаемых на шестилетний непродлеваемый срок, что гарантирует их независимость.

Кроме того, задачи APDP многообразны. Он отвечает за контроль законности обработки, консультирование государственных и частных операторов по их обязательствам, прием жалоб от заинтересованных лиц и проведение информационно-просветительских мероприятий среди населения. Он также должен вести публичный реестр разрешенных видов обработки.

Полномочия APDP значительны. Он может проводить проверки на месте, выносить предупреждения и предписания, требовать прекращения незаконной обработки и налагать денежные штрафы в размере до 50 миллионов франков КФА (статья 71). Он также может предавать свои санкции гласности, что является эффективным средством сдерживания.

Эффективность APDP, однако, будет зависеть от его кадровых и финансовых ресурсов, а также от его способности стать известным гражданам[298]. Проблема его функционирования будет рассмотрена в третьей части.

---

[296] По совокупности этих принципов см. Guillaume DESGENS-PASANAU, La protection des données personnelles: le RGPD et la loi du 20 juin 2018. 2018. С. 45–78.

[297] Для подробного изучения прав лиц см. Laurane RAIMONDO, La protection des données personnelles. 2-е изд. Ellipses, 2023. С. 23–45.

[298] О проблемах создания органов по защите данных во франкоязычной Африке см. Bangali DEDIA и Modeste OUATTARA, La protection des données à caractère personnel en Afrique francophone: guide pratique, LGDJ, coll. Droits africains, 2020. С. 120–145.

Таким образом, своими фундаментальными принципами, правами, предоставляемыми лицам, и учреждением независимого органа камерунский закон полностью вписывается в международное движение за защиту данных. Однако именно в его отступлениях от доминирующей модели и заключается его оригинальность.

Часть II. Особенности камерунского закона

Вписываясь в глобальное движение за защиту данных, камерунский законодатель сделал выбор, отражающий адаптацию к национальным реалиям и стремление к усиленной защите граждан. В этом смысле четыре основные особенности заслуживают углубленного анализа.

II-1. Расширительная концепция чувствительных данных

Статья 5, пункт 13 Закона № 2024/017 определяет чувствительные данные как: «информацию, касающуюся, в частности, религиозных, философских, политических, профсоюзных взглядов и деятельности, банковских операций, расового или этнического, языкового или регионального происхождения, сексуальной жизни, генетики, биометрии, здоровья, судебных исков и уголовных наказаний». Основываясь на международных стандартах, из этого определения вытекают два важных новшества: включение языкового происхождения и возведение банковских данных в ранг чувствительных данных.

В связи с этим вышеупомянутая статья включает языковое происхождение лиц в число чувствительных данных. Это положение, отсутствующее в европейском GDPR, представляет собой замечательную адаптацию к социокультурным реалиям Камеруна. Имея более 280 национальных языков[299] и два официальных языка (французский и английский), страна обладает исключительным языковым разнообразием, которое может быть источником дискриминации.

Таким образом, законодатель хотел защитить граждан от любой формы дискриминации, основанной на разговорном языке, особенно при приеме на работу, доступе к государственным услугам или социальным пособиям. Как подчеркивает Лоран-Фабрис Зенге, это положение «отражает желание защитить граждан от потенциальной дискриминации, связанной с языком, в стране, где сосуществуют более 280 национальных языков»[300].

В том же ключе эта статья также включает данные о банковских операциях в категорию чувствительных данных. Это новшество является важным, поскольку в большинстве законодательств (включая GDPR) банковские данные считаются простыми финансовыми данными, не подпадающими под усиленный режим чувствительных данных.

Для финансовых организаций – банков, микрофинансовых учреждений, финтех-компаний – эта квалификация имеет практические последствия. Они обязаны обрабатывать банковские данные своих клиентов на том же уровне защиты, что и медицинские данные или политические взгляды. Это означает три главные обязанности: получать явное согласие клиента, применять усиленные меры безопасности и обеспечивать полную отслеживаемость всех операций с такими данными.

II-2. Усиленные обязательства обработчиков

Статья 22 камерунского закона устанавливает для подрядчиков (субподрядчиков) особенно строгий режим, который резко отличается от европейского подхода. В случае утечки данных подрядчик должен уведомить «немедленно» три стороны: во-первых, оператора данных, во-вторых, регулирующий орган (APDP), и в-третьих, самих пострадавших людей, если утечка создаёт высокий риск для их прав и свобод.

Эта тройная обязанность вместе с требованием немедленного уведомления – серьёзное отличие от GDPR. В европейской системе подрядчик обязан сообщить об утечке только оператору данных. А уже оператор решает, нужно ли уведомлять регулирующий орган и пострадавших граждан, и на это у него есть 72 часа.

Кроме того, в отношении солидарной ответственности статья 30 (2) закона уточняет, что оператор и обработчик связаны договором и несут солидарную ответственность в случае нарушения или незаконного разглашения данных без согласия затронутого лица.

Таким образом, практическое значение этого положения заключается в том, что такая прямая ответственность обработчиков отвечает растущей сложности цепочек обработки данных. В современной цифровой экономике данные часто обрабатываются несколькими последовательными обработчиками (хостинг-провайдеры, аналитические провайдеры, облачные сервисы). Устанавливая

[299] В Камеруне насчитывается около 280 национальных языков, разделенных на три основные филы: нило-сахарскую, афразийскую и конго-кордофанскую. Источник: Университет Лаваля, «Камерун: языковая ситуация», Языковое планирование в мире, обновлено в 2023 г. См. также Irène Aline MAFOU DABOULA и Amina GORDON, «Межкультурный подход в преподавании национальных языков и культур (LCN) на Крайнем Севере Камеруна», в сборнике Multilinguisme, multiculturalisme et représentations identitaires, 2023. С. 273–286, которые подтверждают цифру от 240 до 280 языков.

[300] Лоран-Фабрис Зенге. Указ. соч.

прямое обязательство по уведомлению, законодатель избегает рисков размывания ответственности и гарантирует максимальную оперативность реагирования на инциденты безопасности.

II-3. Беспрецедентный экстерриториальный охват

Статья 3 камерунского закона определяет территориальную сферу применения текста с замечательной широтой.

Действительно, учитывается критерий физического присутствия. Помимо классического критерия учреждения на территории, закон распространяет свою компетенцию на всю обработку, осуществляемую за пределами Камеруна, если она касается лиц, «находящихся на камерунской территории, включая транзит».

Иными словами, явное включение транзитных лиц является камерунской особенностью.

Камерунский законодатель сделал оригинальный выбор, прямо включив транзитных пассажиров в сферу действия закона. Что это значит на практике? иностранный турист, совершающий остановку в аэропорту Дуалы или путешествующий транзитом в другую страну Центральной Африки, пользуется защитой камерунского законодательства в отношении данных, которые иностранные компании могут обрабатывать о нем. Утверждение этого положения о цифровом суверенитете соответствует географической реальности в том смысле, что Камерун является важной транзитной платформой в Центральной Африке. Для этого она позволяет избежать правовой лазейки, позволяющей иностранным субъектам обрабатывать данные незащищенных путешественников под предлогом краткости их пребывания. С этого момента компании, базирующиеся за пределами Камеруна, но, следовательно, услуги, доступные с территории, теперь должны соответствовать камерунскому законодательству в соответствии со стандартами. К ним относятся: приложения для путешествий и бронирования, социальные сети, доступные в Камеруне, облачные сервисы, используемые лицами, присутствующими в Камеруне, и платформы электронной коммерции, доставляющие товары в Камерун.

II-4. Восемнадцатимесячный срок приведения в соответствие

Статья 73 закона предусматривает важное переходное положение: «Физические или юридические лица, ответственные за обработку персональных данных, имеют восемнадцатимесячный срок с даты обнародования настоящего закона для приведения своей деятельности в соответствие с его положениями». Обнародованный 23 декабря 2024 года, закон устанавливает предельный срок приведения в соответствие – 23 июня 2026 года. Этот относительно длительный срок свидетельствует о желании законодателя обеспечить постепенный переход, адаптированный к реалиям экономических операторов. Несколько причин оправдывают этот льготный период:

- Информирование операторов: компании и администрации должны быть обучены новым обязательствам.
- Затраты на приведение в соответствие: адаптация информационных систем, назначение сотрудников по защите данных (DPO), разработка политик защиты данных представляют собой значительные инвестиции, особенно для МСП.
- Создание органа: APDP должен быть создан, его процедуры функционирования определены нормативными актами, а его разрешительные процедуры должны стать операционными. Поэтому существует необходимость срочной подготовки.

Несмотря на этот срок, операторы не должны ждать последнего момента. Как подчеркивает сама статья 73, закон применяется с момента его обнародования, и основные обязательства существуют немедленно. 18-месячный срок касается фактического приведения в соответствие, но компании уже сейчас должны:

- провести аудит своей обработки данных;
- определить чувствительные данные;
- пересмотреть свои процедуры получения согласия;
- обеспечить безопасность своих архивов и носителей.

Эти четыре особенности очерчивают контуры оригинального, амбициозного и защитного закона, но их практическая реализация сталкивается со значительными препятствиями, особенно практическими, институциональными и культурными.

Часть III. Ограничения на конкретизацию законодательства Камеруна

Доказано, что закон № 2024/017 от 23 декабря 2024 года является законодательным шагом вперед, но его результат будет зависеть от его способности преодолевать препятствия практического, институционального и культурного характера.

III-1. Независимость органа защиты

Наиболее важной институциональной проблемой, влияющей на эффективность законодательства Камеруна, является независимость органа по защите персональных данных (APDP). Несмотря

на то, что законодательный орган создал независимый орган, вопросы возникают на уровне его состава и функционирования. Статья 53 закона действительно предусматривает, что члены APDP назначаются Главой государства – положение, которое, хотя и соответствует некоторым африканским моделям, исключает любой парламентский контроль или участие гражданского общества в процессе назначения. Это отсутствие сдержек и противовесов при назначении с самого начала подрывает доверие к институту, как подчеркивает панафриканская организация «Paradigm Initiative», для которой это исключительно президентское назначение «ставит вопрос о его способности действовать без политического влияния, что необходимо для беспристрастного применения закона». Критика, исходящая от камерунского гражданского общества, усиливает это беспокойство, осуждая «отсутствие достаточного судебного и парламентского контроля» в институциональном механизме.

Чтобы в полной мере оценить масштаб этой проблемы, поучительно сравнение с другими моделями. Европейская модель, закрепленная в GDPR, делает независимость контрольных органов абсолютным стандартом. Во Франции CNIL, таким образом, обладает статусом независимого административного органа, члены которого назначаются по смешанной процедуре с участием парламента, исполнительной власти и квалифицированных специалистов, в условиях, гарантирующих их несменяемость в течение срока полномочий. Более того, статья 52 GDPR обязывает государства-члены гарантировать этим органам «полную независимость» при выполнении своих задач, отсутствие указаний от кого бы то ни было, а также достаточные кадровые и финансовые ресурсы. Эта модель является эталоном настолько, что любое отступление от этих принципов подвергает соответствующее государство критике или судебным разбирательствам.

Российская модель представляет собой интересный контраст, поскольку она полностью основана на иной логике. Российский орган, Роскомнадзор, создан как федеральный орган исполнительной власти, находящийся в ведении Министерства цифрового развития. Его руководитель назначается правительством без участия парламента, а его бюджет включен в бюджет курирующего министерства. Россия, таким образом, не провозглашает независимость своего органа; она принимает модель исполнительного контроля, что имеет преимущество ясности. Каждый знает, что Роскомнадзор проводит политику правительства в области персональных данных. В этой связи интересно отметить, что в январе 2026 года российские депутаты предложили изменить существующую систему и ввести парламентский контроль за назначением главы органа по защите данных. Следствием этих дебатов является то, что вопрос о независимости органов обработки данных возникает во всех системах. Однако Камерун находится в противоречивой ситуации, поскольку закон подтверждает независимость APDP в соответствии с международными стандартами, но конкретные организационные формы приближают его больше к российской исполнительной модели, чем к европейской независимой модели. Мы видим: назначение только президентом, отсутствие парламентского контроля, отсутствие чётких законодательных гарантий несменяемости членов или бюджетной самостоятельности.

Это несоответствие между декларациями и фактическими гарантиями создает серьезный риск для доверия к институту. APDP действительно может колебаться в применении санкций к обработке данных, осуществляемой государством или приближенными к власти лицами, а его назначения могут подчиняться политическим соображениям, а не требованию технической компетентности. Без реальной бюджетной независимости он, кроме того, будет зависеть от доброй воли исполнительной власти в отношении ресурсов, что ограничивает его способность к действию.

Урок российских дебатов в этом отношении ценен: даже в системе, принимающей исполнительный контроль, раздаются голоса, требующие большей прозрачности и подотчетности. В Камеруне, где независимость провозглашена, но не гарантирована, проблема, следовательно, двойная. Во-первых, необходимо на практике доказать, что APDP может действовать независимо, несмотря на способ назначения, который к этому не располагает. Во-вторых, необходимо укрепить с помощью подзаконных актов или последующих пересмотров законодательные гарантии: несменяемость членов, автономный бюджет, парламентский контроль, участие гражданского общества. В противном случае APDP рискует оказаться независимым органом только на бумаге, а на деле – исполнительным органом, что предало бы защитные амбиции закона и породило бы недоверие как со стороны граждан, так и со стороны экономических операторов.

III-2. Практические проблемы для экономических операторов

С одной стороны, малые и средние предприятия (МСП), составляющие основу камерунской экономической ткани, сталкиваются со специфическими трудностями. Анализ CLG Global подчеркивает, что «приведение в соответствие с законом может быть особенно сложным для малых и средних предприятий, которые часто работают с ограниченными финансовыми ресурсами, ограниченной технической экспертизой и незнанием нормативных требований».

Затраты на приведение в соответствие включают:

- назначение сотрудника по защите данных (DPO);
- обучение персонала принципам защиты данных;
- адаптацию информационных систем;
- разработку политик конфиденциальности и внутренних процедур.

С другой стороны, трансграничная передача данных представляет собой практическую проблему, поскольку статья 30 закона устанавливает строгие условия для передачи данных в страны, не обеспечивающие адекватный уровень защиты. для камерунских компаний, которые используют или сотрудничают с иностранными партнерами, это требование затрудняет повседневные операции.

III-3. Культурные и социальные ограничения

Недостаточная осведомленность населения является одним из основных препятствий. Действительно, эффективность закона в определенной степени зависит от осведомленности о нем граждан. В этой связи недавний доклад показал, что было бы неоценимо повысить квалификацию лиц, ответственных за обработку, провести общенациональные информационные кампании, организовать семинары на уровне общин и наладить партнерские отношения с образовательными учреждениями. Это будет способствовать лучшему пониманию гражданами своих прав в области конфиденциальности данных и их эффективному осуществлению. Практика ясна, большинство граждан Камеруна не знают о существовании своих прав на личные данные. Кроме того, парламентские дебаты показали, что операторы связи, которые в массовом порядке собирают информацию о своих абонентах, в прошлом не всегда демонстрировали образцовую работу. Определенные категории населения особенно подвержены цифровому риску из-за своей уязвимости. Как отмечает камерунский судья, женщины и дети подвергаются непропорционально высокому риску в интернете. Примеры очевидны: мы можем привести случай студентки, фотографии которой были опубликованы в частном порядке бывшим одноклассником, или случай 13-летнего ребенка, который предоставил свои биометрические данные мошенническому интернет-сайту. Особая ситуация в англоязычных регионах и действующее там чрезвычайное положение создают дополнительные трудности. В этих районах, сталкивающихся с проблемами безопасности, применение текста сталкивается с особыми препятствиями. Кольбер Гвейн отмечает, что законопроект не отвечает на сложный вопрос об офицерах Сил обороны и безопасности. Последние под предлогом обеспечения национальной безопасности и общественного порядка незаконно и произвольно посягают на частную жизнь жителей. Это, по его словам, приведет к повторным обыскам телефонов, которые часто приводят к криминализации граждан.

III-4. Технологические и инфраструктурные трудности

Конкретная защита данных однозначно связана с наличием защищенной цифровой инфраструктуры. Но проблема национальной связности относится не только к телекоммуникационному сектору, как, кстати, отметил министр путей сообщения и телекоммуникаций. Это также зависит от других навыков, в частности от электроснабжения. На самом деле в Камеруне основной проблемой является нестабильность электросети. Кроме того, компании обязаны инвестировать в технические решения для обеспечения безопасности: шифрование данных, процессы анонимизации, системы обнаружения вторжений. Для многих из них эти инвестиции представляют собой значительное финансовое бремя. К этим трудностям добавляется развитие искусственного интеллекта, о котором говорилось в ходе парламентских дебатов. Алгоритмы, управляемые искусственным интеллектом, обрабатывают большие объемы персональных данных, иногда в условиях полной непрозрачности и без возможности какого-либо контроля со стороны субъектов данных.

В заключение, Закон № 2024/017 от 23 декабря 2024 года о защите персональных данных является решающим шагом в процессе построения правового государства в цифровом формате в Камеруне. Проведенное выше исследование было направлено на освещение особенностей этого текста, находящегося между международным вдохновением и местной адаптацией, чтобы определить, как камерунский законодатель смог применить глобальные стандарты к национальным реалиям.

Из этого анализа следует, что Камерун, как и тридцать восемь других африканских стран, создал комплексную правовую базу, которая воспроизводит фундаментальные принципы права на защиту данных: согласие, законность, прозрачность, права на доступ, исправление, возражение и переносимость. Создание независимого органа, APDP, также свидетельствует об этом стремлении соответствовать международным стандартам. Однако именно в своих отступлениях от доминирующей модели заключается оригинальность камерунского закона. Включение языкового происхождения и банковских операций в категорию чувствительных данных, обязательство обработчиков напрямую уведомлять орган и затронутых лиц о нарушениях, экстерриториальный охват, распространяющийся на транзитных лиц, и восемнадцатимесячный срок приведения в соответствие до июня

2026 года – вот те особенности, которые делают камерунский текст оригинальным вкладом в сравнительное правоведение.

Однако этот законодательный прогресс, сколь бы замечательным он ни был, сталкивается со значительными проблемами, которые обусловливают его эффективность. независимость надзорного органа, хотя и провозглашенная законом, ослаблена исключительно президентским способом назначения, а риск беспристрастности будущих решений отмечен отсутствием парламентского контроля. Таким образом, противоречие Камеруна выявляется путем сравнения с европейской моделью и российской моделью, то есть с предоставленной независимостью, но с такими организационными механизмами, которые выгодно приближают APDP к подведомственному органу, а не к реальному независимому органу. Кроме того, на практике малые и средние предприятия сталкиваются с трудностями, связанными с затратами на соблюдение нормативных требований, низкой осведомленностью граждан об их новых правах и недостатками цифровой инфраструктуры, которые затрудняют практическую защиту данных. Таким образом, законодательный орган Камеруна смог адаптировать международные стандарты к национальным реалиям, добавив проблемы, характерные для местного контекста, в частности языковое разнообразие или защита банковского сектора. Он также выбрал путь усиленной защиты граждан, возложив прямую ответственность на подрядчиков (субподрядчиков). Эти нововведения – ценный вклад в международный юридический диалог о регулировании цифровой среды.

Однако амбициозная защитная цель закона сможет стать реальностью только при условии, что будут преодолены институциональные, практические и культурные проблемы. Независимость APDP должна быть доказана на деле, а не только в текстах – для этого нужны усиленные законодательные гарантии и ресурсы, соответствующие его задачам. Просвещение граждан должно стать национальным приоритетом, чтобы провозглашённые права стали правами, которые люди реально могут осуществлять...

Предприятия, особенно малые, должны быть поддержаны в процессе приведения в соответствие.

Переходный период до 23 июня 2026 года дает ценную возможность для подготовки этого перехода. Все заинтересованные стороны – государство, независимый орган, предприятия, гражданское общество, граждане – должны воспользоваться этим шансом, чтобы сделать защиту персональных данных в Камеруне не просто законодательной амбицией, а конкретной и защитной реальностью для каждого. Камерун этим законом утверждает свой цифровой суверенитет и позиционирует себя как потенциально ведущего игрока в Центральной Африке. Остается превратить этот текстуальный прогресс в ощутимый прогресс для миллионов граждан, чьи данные, с каждым днем все более многочисленные, заслуживают защиты, соответствующей вызовам XXI века. Камерунский опыт, таким образом, демонстрирует, что развивающаяся страна может принять амбициозное законодательство, адаптированное к ее реалиям; он также напоминает, что право, сколь бы инновационным оно ни было, имеет силу только благодаря коллективной воле претворить его в жизнь.

Ю. А. Буторина,
обучающаяся 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: О. А. Сегал, к.ю.н., доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Проблемные аспекты безопасности и вопросы компетенции в цифровом нотариате

В условиях стремительного развития цифровой экономики и реализации национальной программы «Цифровая экономика Российской Федерации» требования к специалистам в сфере права претерпевают кардинальные изменения, затрагивая и нотариат. Современный нотариус не ограничивается работой исключительно с бумажными носителями информации; его профессиональная деятельность включает активное взаимодействие с Единой информационной системой нотариата (ЕИС), использование портала государственных услуг, а также осуществление удаленных нотариальных действий посредством усиленной квалифицированной электронной подписи (УКЭП) второго поколения[301].

[301] Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 № 4462-1) (ред. от 08.08.2024) [Электронный ресурс] // СПС «КонсультантПлюс».

В этих условиях обеспечение информационной безопасности приобретает первостепенное значение, а подготовка кадров, способных эффективно защищать конфиденциальную информацию и персональные данные в цифровом пространстве, становится одной из ключевых стратегических задач развития нотариальной системы. Опираясь на анализ законодательных норм, научных публикаций и практический опыт нотариальной деятельности, выявим основные проблемы подготовки специалистов в области информационной безопасности для нотариата и предложим возможные пути их решения.

Автоматизированную систему Федеральной нотариальной палаты представляет Единая информационная система нотариата (ЕИС). Данная программа предназначена для автоматизации процессов сбора, обработки и хранения данных о нотариальной деятельности. Непрерывное функционирование и соблюдение установленных требований обеспечивается оператором ЕИС, которым является Федеральная нотариальная палата. ЕИС включает сведения о нотариальных действиях и иную информацию, предусмотренную Основами законодательства Российской Федерации о нотариате.

Оператором ЕИС выполняются следующие функции:

1. Обеспечение ежедневного функционирования системы.
2. Предоставление пользователям доступа к реестрам ЕИС.
3. Осуществление создания резервных копий реестров и предоставление их федеральному органу юстиции ежеквартально, а также по запросам.
4. Осуществление проверки действительности усиленных электронных подписей нотариусов и отказ в приеме документов, подписанных недействительными подписями.
5. Обеспечение неизменности и целостности данных, хранящихся в ЕИС.

Сведения, передаваемые по средствам ЕИС, не рассматриваются как разглашение тайны совершения нотариальных действий, но при этом лица, допущенные к работе ЕИС, должны соблюдать конфиденциальность содержащихся в ней данных, исключениями являются случаи, предусмотренные Основами законодательства о нотариате Российской Федерации. При разглашении данной информации ответственность предусмотрена законодательством Российской Федерации. Информация, содержащаяся в ЕИС, защищена законодательством о персональных данных и информационных технологиях. Отчетность о функционировании реестров определяется федеральным органом юстиции[302].

Законодательство о нотариате, информационное право, законодательство о защите персональных данных представляют сочетание основных областей законодательства. Основные принципы регулирования, создания и функционирования ЕИС, а также принципы и требования к использованию электронных реестров определяют Основы законодательства о нотариате Российской Федерации.

Федеральным законом «Об информации, информационных технологиях и о защите информации», а также Федеральным законом «О персональных данных» регулируется защита информации в ЕИС. Еще один документ, регулирующий защиту информации, – «Политика в отношении обработки и защиты персональных данных», который утвержден Федеральной нотариальной палатой в июне 2025 года. Документ детализирует требования к хранению нотариальных документов в электронном виде. Также им установлен порядок хранения нотариальных документов, включая технические требования к форматам использования усиленной квалифицированной электронной подписи. Обеспечение безопасности определяется совместными усилиями федерального органа юстиции, Федеральной нотариальной палаты и федерального органа исполнительной власти[303].

А. В. Бегичев провел исследование, посвященное развитию трансформации профессиональных компетенций нотариусов в контексте цифровой эпохи. Автор отмечает, что несмотря на активное внедрение технологий, расширению предметной компетенции нотариата в законодательстве уделяется незначительное внимание, что демонстрирует, в частности, законопроект о нотариате, представленный Минюстом России 26 июля 2024 г.[304]. Данный факт создает риск отставания нормативной базы от темпов технологического развития и формирует так называемые «серые зоны» в вопросах ответственности и требуемых навыков. Исходя из этого, возникает необходимость в разработке новых нормативно-правовых актов, которые бы регулировали деятельность нотариусов в цифровой среде.

Практический взгляд на проблему подготовки кадров представлен в материалах заседания НОЦ «Цифровая образовательная среда» и Центра нотариального права «Путь к закону» МГУ (декабрь 2024 г.). В докладе М. В. Воронина «Профессия нотариуса в условиях нового типа конструирования

[302] Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 № 4462-1) (ред. от 08.08.2024) [Электронный ресурс] // СПС «КонсультантПлюс».

[303] Политика в отношении обработки и защиты персональных данных в Федеральной нотариальной палате (утв. ФНП 02.06.2025) [Электронный ресурс] // СПС «КонсультантПлюс».

[304] Бегичев А. В. Развитие предметной компетенции нотариата в цифровую эпоху как фактор, влияющий на укрепление правовой стабильности [Электронный ресурс] // Нотариальный вестник. 2024. № 10. С. 13–21. URL: https://repository.rudn.ru/

реальности: междисциплинарность и цифровизация» подчеркивается, что современный нотариус должен обладать междисциплинарными компетенциями, находящимися на стыке юриспруденции и информационных технологий[305]. Участники на заседании пришли к выводу о важности соблюдения баланса между внедрением цифровых технологий и сохранением интересов всех участников нотариального процесса, где технологии должны быть инструментом, служащим принципам гуманизма и справедливости.

В выступлениях руководства Федеральной нотариальной палаты (ФНП) можно выявить основные требования к современному нотариусу:

- Обладание навыками работы в ЕИС. Что позволит автоматизировать рутинные процессы и повысит эффективность.
- Знания в области информационной безопасности и цифровой инфраструктуры. Необходимы для понимания принципов электронного документооборота и правового статуса электронных документов.
- Умения владеть усиленной квалифицированной электронной подписью. Требуются для обеспечения высокого уровня защиты и аутентичности электронных документов.
- Готовность к обучению и профессиональному развитию в условиях технологического прогресса.

Трансформация компетенции нотариусов требует комплексного подхода. Такой подход обеспечит успешную адаптацию нотариусов к новым реалиям и сохранит высокий уровень профессионализма и доверия общества. Поэтому необходимо учесть не только технологические аспекты, но и правовые, этические, социальные последствия внедрения цифровых технологий в нотариальную практику.

Федеральной нотариальной палатой (ФНП) и региональными нотариальными палатами регулярно организуются семинары и вебинары, направленные на повышение квалификации действующих нотариусов. В мае 2025 г. проводился семинар для IT-специалистов нотариальных палат, во время которого обсуждались вопросы развития и защиты от уязвимостей ЕИС, а также функционирования удостоверяющих центров и обеспечения безопасности персональных данных в нотариальных конторах[306].

Однако ключевой проблемой является неравномерность подготовки кадров, что отмечается следующими фактами:

- **Нотариусы** являются высококвалифицированными юристами, но зачастую не обладают глубокими техническими знаниями в области информационной безопасности.
- **IT-специалисты**, обладая высоким уровнем технических компетенций (межсетевые экраны, шифрование, антивирусная защита), могут не в полной мере понимать специфику нотариального делопроизводства и юридические последствия утечки данных.

Данная ситуация приводит к разрыву в понимании и взаимодействии между юристами и техническими специалистами, что негативно сказывается на общей эффективности системы подготовки кадров.

Фонд «Центр инноваций и информационных технологий» (ФЦИИТ), созданный Федеральной нотариальной палатой в 2009 году, играет ключевую роль в обеспечении технологического развития и информационной безопасности нотариата. Основные направления деятельности ФЦИИТ включают:

- создание условий для внедрения современных информационно-коммуникационных технологий;
- формирование инфраструктуры нотариата;
- разработка мер по обеспечению информационной безопасности в условиях цифровизации[307].

На основе анализа выявлены следующие системные проблемы в сфере информационной безопасности нотариальной деятельности:

Проблема 1. Отсутствие специализированных образовательных стандартов. В российских юридических вузах нет программ, целенаправленно обучающих информационной безопасности. Как отмечает президент Федеральной нотариальной палаты, для нотариусов необходимы специалисты с качественным юридическим образованием, но базовых знаний недостаточно для эффективной работы в сфере ИБ.

Проблема 2. Неполное и нерегулярное повышение квалификации. Образовательные курсы носят общий характер и зачастую не учитывают специфику нотариальной деятельности. Система повышения квалификации затрагивает вопросы информационной безопасности, но не обеспечивает их глубокого изучения, что приводит к недостаточной подготовке специалистов.

---

[305] Заседание НОЦ «Цифровая образовательная среда» и Центра нотариального права «Путь к закону» [Электронный ресурс] // Юридический факультет МГУ имени М. В. Ломоносова. URL: https://www.law.msu.ru/news/zasedanie_noc_cifrovaya_obrazovatelnaya_sreda_i_centra_notarialnogo_prava_put_k_zakonu__2024-12-16-9543

[306] Технологии, социальные проекты и перспективы развития нотариата обсудили на правовом конгрессе в Екатеринбурге [Электронный ресурс] // Нотариальная палата Республики Марий Эл : [официальный сайт]. 06.06.2025. URL: https://notariat12.ru/news/view/1339

[307] Центр инноваций и информационных технологий (ФЦИИТ) // Федеральная нотариальная палата : официальный сайт. URL: https://notariat.ru/ru-ru/federal-notary-chamber/fondy-i-inye-struktury/centr-innovacij-i-informacionnyh-tehnologij/

Проблема 3. Разрыв между юридическими и техническими компетенциями. Недостаточно специалистов, которые сочетают знания законодательства и кибербезопасности. Снижается эффективность выполнения задач и контроля за их реализацией. Данная проблема связана с недостаточным междисциплинарным взаимодействием в образовательной и профессиональной среде.

Проблема 4. Технологии, опережающие образовательные программы. Современные технологии внедряются быстрее образовательных программ, например: искусственный интеллект, распределенные реестры и биометрия.

Выявленные проблемы требуют комплексного подхода в различных сферах:

В нормативно-правовой сфере нужно внести изменения, устанавливающие требования к уровню знаний в области информационной безопасности для нотариусов. Данная мера обеспечит защиту информации и соблюдение современных стандартов.

В образовательной сфере необходимо создавать образовательные программы, в разработке которых принимать участие должны Федеральная нотариальная палата, региональные палаты и юридические вузы. Данные программы необходимы и для безопасности нотариальной деятельности, и для готовности к современным вызовам и угрозам.

Таким образом, необходимо решить проблемы отсутствия специализированных образовательных программ, дисбаланса между юридическими и техническими компетенциями специалистов, учитывая динамичное развитие информационных технологий. Только системный и интегрированный подход к подготовке кадров обеспечит надежную защиту информации и поддержание высокого уровня доверия к нотариату в условиях цифровой трансформации.

В. В. Соколов,
магистрант 1 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Г. Г. Камалова, д.ю.н., доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Влияние информационных технологий на реализацию избирательных прав граждан в условиях цифровизации общества

Стремительно развиваясь, информационные технологии с каждым годом оказывают все более значительное воздействие на реализацию избирательных прав граждан. Несмотря на значительные преимущества, которые влечет за собой трансформация избирательных процессов в связи с введением в них цифровых технологий, этот процесс также влечет за собой угрозу возникновения новых правовых рисков и требует определенного совершенствования правового законодательства. Такие технологии, как электронные системы голосования, цифровые информационные ресурсы и онлайн платформы для агитации избирателей, повышают доступность избирательных процессов для граждан, однако вместе с тем могут повлечь образование дискриминации в отношении определенных групп граждан, не имеющих доступ к цифровым технологиям. Помимо этого, ряд исследователей указывает на то, что при осуществлении электоральных процессов дистанционным образом нарушает право на тайну голосования. Актуальность выбранной темы подтверждается отсутствием правовой концепции дистанционного электронного голосования при ежегодном повышении степени цифровизации избирательных процессов на территории Российской Федерации.

Основным законом, регулирующим проведение избирательного процесса в дистанционном формате на территории РФ, является Федеральный закон от 12 июня 2002 г. № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»[308]. Так, ст. 2, п. 62 данного Федерального закона определяет электронное голосование как «голосование на избирательном участке, участке референдума без использования бюллетеня, изготовленного на бумажном носителе, с использованием комплекса для электронного голосования». В то же время п. 62.1 этой статьи закрепляет дистанционное электронное голосование как голосование с использо-

[308] Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации : Федеральный закон от 12.06.2002 № 67-ФЗ [Электронный ресурс] // Собрание законодательства РФ. 2002. № 25. Ст. 2322. URL: https://base.garant.ru/184566/ (дата обращения: 06.03.2026).

ванием специального программного обеспечения, доступ к которому предоставляется на техническом устройстве избирателя, участника референдума. Различие между этими видами голосования заключается в месте и способе участия избирателя: электронное голосование проводится на оборудованных участках с использованием технических средств, тогда как дистанционное электронное голосование позволяет участвовать в выборах удалённо, используя интернет-порталы и программное обеспечение, разработанное и утверждённое Центральной избирательной комиссией РФ. При этом перед непосредственным участием в голосовании или референдуме гражданину, согласно п. 15. ст. 64.1 этого закона, необходимо, обратившись на специальный портал в сети «Интернет», пройти процедуру идентификации и аутентификации, только в этом случае он получит доступ к электронному голосованию. Таким образом, по сравнению с традиционной создается принципиально новая форма для осуществления гражданами избирательных прав, предоставляющая возможность избирателям после прохождения предварительной регистрации принимать участие в электоральных процессах без непосредственной явки на избирательный участок.

Помимо указания на то, что данная система является уязвимой для хакерских атак извне с целью изменения итогов голосования либо получения информации о результатах волеизъявления каждого гражданина, можно указать и на то, что избирательные органы не имеют возможности проконтролировать объём информации, который собирает и хранит каждая отдельная информационная система, используемая участниками избирательного процесса. При этом стоит отметить, что в данном механизме волеизъявления также отсутствует возможность контроля за соблюдением конституционных прав граждан, в частности за принципом тайного голосования. Как считает Д. А. Ежов, наличие необходимой процедуры идентификации создает угрозу для этого принципа, поскольку открывает реальную возможность узнать за кого избиратель отдал свой голос[309]. Е. Н. Босова утверждает, что при использовании технологий дистанционного электронного голосования принцип тайного голосования является весьма условным, поскольку, во-первых, избиратель должен быть пользователем федеральной государственный информационной системы «Единый портал государственных и муниципальных услуг» с действующей подтвержденной учетной записью. Во-вторых, блокчейн-технологии, применяемые при дистанционном голосовании, позволяют сохранить всю процедуру голосования, поэтому у лиц, имеющих доступ к этой системе, есть возможность установить личность избирателя и результат его волеизъявления[310]. Также значение имеет и тот факт, что законодательством в достаточной степени не определен правовой статус лиц, имеющих доступ к примененным при голосовании блокчейн-технологиям, на что указал член территориальной комиссии с правом решающего голоса Е. В. Дроздов[311].

На территории Российской Федерации первым этапом внедрения информационных технологий в избирательный процесс можно назвать учреждение Указом Президента РФ от 23.08.1994 № 1723 Государственной автоматизированной системы «Выборы» (далее – ГАС «Выборы»). В 2003 г. ГАС «Выборы» получила статус федеральной автоматизированной информационной системы, предназначенной для автоматизации информационных процессов подготовки и проведения выборов и референдумов, обеспечения деятельности избирательных комиссий, а также решения задач, не связанных с выборами[312]. Внедрение этой системы открыло возможность избирателям – участникам электорального процесса получать через сеть «Интернет», мобильную связь информацию о кандидатах, политических партиях, знакомиться с результатами голосования и принять осознанный выбор. Также политические партии и избирательные комиссии вместе с системой ГАС «Выборы» получили широкие возможности для подготовки, организации и проведения избирательного процесса. В. Н. Белоновский утверждает, что «введение этой системы стало результатом обобщения опыта работы избирательных комиссий и избирательного процесса в целом»[313]. Порядок организации работы по обеспечению безопасности информации, а также исчерпывающих комплекс организационных, технических

[309] Ежов Д. А. Электронное голосование: очевидные достоинства и потенциальные риски // Власть. 2023. Т. 31, № 5. С. 112–114.

[310] Босова Е. Н. Тайное волеизъявление избирателей: традиционное и дистанционное // Вестник Института права Башкирского государственного университета. 2023. № 3 (113).

[311] Особое мнение к протоколу Территориальной избирательной комиссии дистанционного электронного голосования об итогах дистанционного электронного голосования [Электронный ресурс]. URL: https://docs.yandex.ru/docs/view?tm=1678991968&tld=ru&name=osoboe-mnenie-drozdov.pdf&text (дата обращения: 06.03.2026).

[312] О Государственной автоматизированной системе Российской Федерации «Выборы» : Федеральный закон от 10.01.2003 № 20-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://base.garant.ru/ (дата обращения: 06.03.2026).

[313] Белоновский В. Н. Правонарушения и юридическая ответственность в избирательном праве. Историческая практика и современность : монография / под ред. А. С. Прудникова. М. : ЮНИТИ-ДАНА, 2005. С. 328.

и правовых мер защиты закреплен в постановлении Центральной избирательной комиссии Российской Федерации от 23 июля 2003 г. № 19-137-4. По мнению Н. Б. Исмелова, одним из наиболее важных к проработке направлений в этой сфере является обеспечение использования юридически значимых документов. Им предложено на законодательном уровне разработать и утвердить требования к форматам электронных документов, регламенты использования средств защиты информации, обеспечение использования электронной цифровой подписи, а также архивного хранения электронных документов[314].

Следующей важной мерой по внедрению информационных технологий в избирательный процесс стал переход в 2017 г. от открепительных удостоверений к системе «Мобильный избиратель». Порядок подачи гражданином заявления о голосовании по месту нахождения утвержден в постановлении Центральной избирательной комиссии Российской Федерации от 1 ноября 2017 г.[315]. Согласно данному постановлению гражданин вправе не ранее чем за 45 дней и не позднее чем за 5 дней до дня голосования подать заявление о голосовании по месту нахождения через территориальную или участковую избирательную комиссию, многофункциональный центр предоставления государственных и муниципальных услуг, а также через Единый портал государственных услуг. Однако на практике довольно распространены случаи, когда избирателем осуществляется одновременное голосование на двух участках, с целью предотвратить это был предпринят комплекс мер, согласно которым сведения об избирателе передаются в ГАС «Выборы» сразу после осуществления им волеизъявления. В свою очередь, Система «Мобильный избиратель», безусловно, оказывает положительное влияние на избирательные права граждан, выраженное в виде упрощения возможности на реализацию ими своих избирательных прав, а также общее снижение бюрократического барьера. Однако ряд исследователей подчеркивает тот факт, что включение данной системы в электоральный процесс влечёт за собой и определенные риски, к примеру, увеличивается количество случаев нарушения принципа, согласно которому от каждого избирателя должен поступать лишь один голос. «Внедрение механизма голосования по месту нахождения требует высокой точности ведения баз данных избирателей и эффективной системы межкомиссионного обмена информацией»[316]. Также уменьшение бюрократии и перевод голосования в электронный формат может повлечь за собой снижение прозрачности электорального процесса. Мнение многих исследователей можно суммаризировать утверждением Д. А. Ежова, который утверждает, что «усложнение информационных потоков и цифровизация избирательных процедур могут снижать уровень общественного контроля и доверия к результатам голосования»[317].

Н. А. Щиголева,
магистрант 2 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Г. Г. Камалова, д.ю.н., доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Электронный документооборот в бухгалтерском учете: проблемы практического применения

В условиях цифрового изменения экономики электронный документооборот (ЭДО) становится одним из основных элементом учетных процессов хозяйствующих субъектов. Несмотря на явные преимущества, такие как скорость, прозрачность, экономия ресурсов, на практике ЭДО в бухгалтерском учете связан не только с техническими трудностями. Цель данной статьи – провести системный анализ проблем практического применения ЭДО, классифицировать их по источникам возникновения и предложить пути минимизации рисков.

[314] Исмелов Н. Б. Государственная автоматизированная система «Выборы» как средство автоматизации избирательного процесса // Государство и право. 2016. № 7. С. 113–118.

[315] Центральная избирательная комиссия Российской Федерации. Постановление от 01.11.2017 № 108/903-7 «О Порядке подачи заявления о включении избирателя в список избирателей по месту нахождения».

[316] Ларин И. Г. Мобильный избиратель – новый формат реализации гражданами избирательных прав // Юридический вестник Самарского университета. 2020. Т. 6, № 2. С. 127–131.

[317] Ежов Д. А. Электронное голосование: очевидные достоинства и потенциальные риски // Власть. 2023. Т. 31, № 5. С. 112–114.

Переход на электронный документооборот является одним из основных моментов развития бухгалтерского учета в Российской Федерации. Нормативная база, заложенная Федеральным законом № 63-ФЗ «Об электронной подписи»[318] и приказами ФНС, создала правовые основы для признания юридической силы электронных документов. На текущий момент существует множество решений от операторов ЭДО (Астрал, Диадок, СБИС, Такском и др.), а при внедрении машиночитаемых доверенностей (МЧД) стандартизация выходит на новый уровень.

Однако изучив статистику внедрения и опросы практикующих бухгалтеров, мы понимаем, что эффективность ЭДО часто оказывается ниже того, что ожидали. Многие организации сталкиваются с тем, что автоматизация не снижает, а перераспределяет нагрузку с появлением новых рисков[319]. Цель данной статьи – не показать плюсы ЭДО, а показать какие проблемы возникают у организаций при цифоровизации бухгалтерии.

Вопреки ожиданиям, внедрение ЭДО может снижать уровень финансового контроля в организации. В классическом бумажном формате подпись руководителя на платежном поручении или договоре являлась физическим актом, требующим его личного участия. В цифровом пространстве широкое распространение получила практика перераспределения права подписи подчиненным (главному бухгалтеру, финансовому директору) путем передачи им носителей с ключами ЭП[320].

Если говорить о взаимоотношениях руководителя и подчиненного, это создает неравномерное распределение информации и конфликта интересов: сотрудник получает возможность самостоятельно инициировать транзакции от имени руководителя организации, минуя процедуры визирования. Эксперты отмечают рост числа ситуаций, связанных с выводом средств с использованием легитимных электронных подписей рядовых сотрудников, что в судебной практике сложно квалифицировать как взлом[321]. В данном случае решением является не запрет на делегирование, а внедрение многофакторной системы авторизации платежей в системе и строгое разграничение прав доступа внутри самого ЭДО, а не только на уровне носителя ключа.

Несмотря на законодательное закрепление равной силы бумажного и электронного документа (при соблюдении требований к подписанию), на практике сохраняется правовой пробел – непонятно, как применять МЧД в некоторых ситуациях. Основные риски связаны с:

1. Оспариванием факта подписания. Контрагент может заявить, что подпись была скомпрометирована, или что документ подписан неуполномоченным лицом. Ситуация усугублялась до введения МЧД, когда было сложно доказать полномочия представителя[322].
2. Доказательной базой. В отличие от бумажного документа, который существует материально, электронный документ требует доказательства его неизменности и факта отправки/получения[323]. Здесь решающую роль играет протокол оператора ЭДО, который должен быть правильно оформлен для предоставления в суд.

Многие организации, особенно в работе с контрагентами, по-прежнему требуют дублирования бумажных копий, что снижает экономический эффект от ЭДО[324].

Наиболее частая ошибка при внедрении ЭДО – использование его как отдельной программы, а не как часть бухгалтерского учета. Типичная ситуация: бухгалтер получает документ от контрагента в интерфейсе оператора (например в СБИС), распечатывает его или открывает в соседнем окне, а затем вручную переносит данные в 1С. При такой организации трудозатраты не снижаются, а риск арифметических или реквизитных ошибок остается высоким[325].

---

[318] Об электронной подписи : Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 31.07.2025) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 25.03.2026).

[319] Арутюнян Э. А., Колиева А. В. Внедрение системы электронного документооборота: риски и способы их преодоления [Электронный ресурс] // Международный студенческий научный вестник. 2023. № 6. С. 81. URL: https://www.elibrary.ru/item.asp?id=59391969 (дата обращения: 25.03.2026).

[320] Аверин А. А., Левчук П. П. Электронная подпись как средство защиты электронного документооборота [Электронный ресурс] // Вестник научного общества студентов, аспирантов и молодых ученых. 2015. № 3. С. 7–10. URL: https://www.elibrary.ru/item.asp?id=23681486 (дата обращения: 25.03.2026).

[321] Буданцев Р. А., Заборовская С. В. Опыт использования технологий электронного документооборота на предприятиях и организациях Российской Федерации // Документ в социокультурном пространстве: теории и цифровые трансформации : материалы VIII Междунар. науч.-практ. конф., посвящ. 80-летию Великой Победы, Казань, 16 мая 2025 года. Казань : Казан. гос. ин-т культуры, 2025. С. 153–157. URL: https://www.elibrary.ru/item.asp?id=83014833 (дата обращения: 25.03.2026).

[322] Там же.

[323] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2025) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 25.03.2026).

[324] Шалаумова Е. В., Кузнецов А. С. Оптимизация выполнения информационных процессов в системе предприятия с внедрением электронного документооборота [Электронный ресурс] // Нанотехнологии: наука и производство. 2024. № 2. С. 30–34. URL: https://www.elibrary.ru/item.asp?id=67889578 (дата обращения: 25.03.2026).

[325] Литвина К. Я. Информационные технологии в области централизации учета [Электронный ресурс] // Human Progress. 2023. Т. 9, № 5. С. 14. URL: https://www.elibrary.ru/item.asp?id=60000657 (дата обращения: 25.03.2026).

Эффективность ЭДО достигается только при прямом взаимодействии учетной системы организации и сервиса оператора. Проблема заключается в том, что типовая интеграция часто не учитывает специфику учетной политики конкретной организации (субконто, аналитические разрезы), а доработка требует ресурсов: и человеческих, в том числе привлечения квалифицированных программистов, и финансовых[326].

Сфера ЭДО представлена широким спектром поставщиков услуг. На территории Российской Федерации функционирует свыше сорока операторов. Если стороны договора используют разные платформы, непосредственная передача документов между ними невозможна без применения механизма роуминга, который предполагает обмен данными через специализированные шлюзы. Проблема заключается в том, что не все операторы имеют роуминговые соглашения друг с другом. Поэтому обмен с контрагентом из другой системы может быть проблематичен[327]. Также можно выделить процесс настройки роуминга, который часто требует ручного подтверждения со стороны обоих контрагентов и занимает время, а отсутствие единого стандарта обмена приводит к техническим сбоям при передаче файлов[328].

При смене оператора приходится вновь настраивать интеграции, перезаключать договоры и обучать сотрудников, а это всё приводит к расходам.

Сопротивление персонала является обыденной проблемой любых изменений, но в бухгалтерии же это еще и обостряется строгими правилами и ответственностью. Бухгалтер несет прямую ответственность за ошибки перед ФНС. Работа в новой системе, нестабильность соединения, риск случайного удаления, что-то не найти, либо сбои, ошибки или вирусы, навсегда потерять доступ к файлу – все это вызывает у сотрудников стресс и недоверие в цифровом пространстве[329]. Кроме того, внедрение ЭДО требует от бухгалтера навыков работы в новых программах, цифровой грамотности, понимания новых процессов и работы с электронными подписями, форматами XML, машиночитаемыми доверенностями. Недостаточная подготовка в этих вопросах приводит к тому, что бухгалтер продолжает вести параллельный учет в электронных таблицах или на бумажных носителях, что в конечном итоге усложняет и запутывает учет[330].

Проведя анализ, можно предложить следующие пути решения данных проблем:

1. Переход к автоматизированной системе внутреннего контроля (СВК). Существующая практика внутреннего контроля, которая основана на ручной сверке подписей, должна быть пересмотрена в пользу автоматизированных решений. Необходимо внедрение в систему маршрутов согласования, которые автоматически блокируют проведение документов, не прошедших все этапы визирования, независимо от наличия физической электронной подписи[331]. Таким образом, контроль будет осуществляться на уровне доступа к конкретным операциям в учетной системе, а не на уровне доступа к файлам на физических носителях (токенах).

2. При выборе поставщика услуг ЭДО и его последующей интеграции компаниям следует выбирать оператора ЭДО исходя не из стоимости тарифа, а из возможности бесшовной интеграции с используемой учетной системой[332].

Очень важно требовать от оператора предоставления открытого API или использования типовых конфигураций (например «1С-ЭДО»), что позволяет автоматически создавать документы в учете на основе поступивших файлов (счетов, актов, УПД) без участия человека[333].

3. Внедрение МЧД следует воспринимать не как принудительное требование, а как эффективное средство минимизации потенциальных угроз и правовых рисков. МЧД позволяет определять полномочия сотрудника в машиночитаемом виде, не оставляя сомнений в возможности оспаривания

---

[326] Арутюнян Э. А., Колиева А. В. Внедрение системы электронного документооборота: риски и способы их преодоления // Международный студенческий научный вестник. 2023. № 6. С. 81. URL: https://www.eli-brary.ru/item.asp?id=59391969.

[327] Официальный портал 1С-ЭДО. Настройка роуминга по заявке с сайта 1С-ЭДО [Электронный ресурс]. URL: https://edo.1c.ru/handbook/rabota-s-priglasheniyami/rouming/nastroyka-rouminga-po-zayavke-s-sayta-1s-edo/ (дата обращения: 25.03.2026).

[328] База знаний «Такском». Роуминг ЭДО в 1С: возможности автоматического обмена и список поддерживаемых операторов. URL: https://taxcom.ru/baza-znaniy/elektronnyy-dokumentooborot/stati/rouming-edo-v-1s/ (дата обращения: 25.03.2026).

[329] Шалаумова Е. В., Кузнецов А. С. Оптимизация выполнения информационных процессов в системе предприятия с внедрением электронного документооборота [Электронный ресурс] // Нанотехнологии: наука и производство. 2024. № 2. С. 30–34. URL: https://www.elibrary.ru/item.asp?id=67889578 (дата обращения: 25.03.2026).

[330] Литвина К. Я. Информационные технологии в области централизации учета [Электронный ресурс] // Human Progress. 2023. Т. 9, № 5. С. 14. URL: https://www.elibrary.ru/item.asp?id=60000657 (дата обращения: 25.03.2026).

[331] Аверин А. А., Левчук П. П. Электронная подпись как средство защиты электронного документооборота [Электронный ресурс] // Вестник научного общества студентов, аспирантов и молодых ученых. 2015. № 3. С. 7–10. URL: https://www.elibrary.ru/item.asp?id=23681486 (дата обращения: 25.03.2026).

[332] Литвина К. Я. Указ. соч. С. 14.

[333] Официальный портал 1С-ЭДО. Настройка роуминга по заявке с сайта 1С-ЭДО...

факта наличия у него права подписи. Одним из важных моментов является включение в договоры с контрагентами специальных разделов, которые будут регламентировать порядок разрешения споров при ЭДО и признавать данные из протоколов операторов в качестве надлежащих доказательств.

4. Повышение профессионализма и оптимизация процессов. Необходима разработка локального нормативного акта (Положения об ЭДО), который подробно дает описание порядка получения и хранения ЭП, действия при утрате ключей, а также регулирует регламент работы с входящими/исходящими документами и ответственность за нарушение сроков подписания[334]. Обучение сотрудников должно быть направлено на практическое применение знаний и навыков, включая анализ и проработку нестандартных ситуаций.

Электронный документооборот в бухгалтерском учете – это не просто замена бумажного носителя на цифровой, а глобальное изменение структуры учетного процесса. Проблемы практического применения возникают при взаимодействии права, технологий и человеческого фактора. Если внедрение электронного документооборота происходит формально, без пересмотра системы управления и контроля, а также без тесной связи с учетными программами, это не только увеличивает расходы на операции, но и приводит к появлению новых рисков, в том числе рисков мошенничества.

Успешная цифровизация возможна лишь при системном подходе, включающем автоматизацию процессов согласования, переход на МЧД, внедрение ЭДО в контур системы и повышение цифровой грамотности сотрудников, отвечающих за учет. Дальнейшие исследования в этой области должны быть направлены на разработку методик оценки эффективности ЭДО, принимая во внимание потенциальные риски, а также необходимо исследовать возможности применения блокчейн-технологий для достижения абсолютной гарантии сохранности и неизменности учетных данных.

А. М. Гущин,

магистрант 1 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Г. Г. Камалова, д.ю.н., доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Проблемы подготовки кадров в области обеспечения информационной безопасности

В мире цифровой трансформации экономики и общества вопрос подготовки квалифицированных специалистов в области информационной безопасности стоит очень остро. В статье анализируются основные проблемы существующей системы образования в сфере информационной безопасности: дефицит кадров, отставание образовательных программ от динамики киберугроз, недостаточность практической подготовки, слабая связь между образовательными учреждениями и индустрией. Рассматриваются факторы, препятствующие эффективной подготовке специалистов, включая устаревшую материально-техническую базу, нехватку квалифицированных преподавателей-практиков и отсутствие единых профессиональных стандартов. Предлагаются конкретные пути решения выявленных проблем на основе анализа современных тенденций и успешного отечественного опыта. Особое внимание уделяется необходимости формирования комплексной системы непрерывного профессионального развития специалистов в области информационной безопасности.

Российская экономика переживает беспрецедентный период цифровизации, сопровождающийся экспоненциальным ростом киберугроз. По данным исследований дефицит кадров цифровой безопасности превысил 500 тысяч человек[335]. Экономическая проблема превратилась в стратегическую угрозу цифровой безопасности России.

---

[334] Арутюнян Э. А., Колиева А. В. Внедрение системы электронного документооборота: риски и способы их преодоления [Электронный ресурс] // Международный студенческий научный вестник. 2023. № 6. С. 81. URL: https://www.elibrary.ru/item.asp?id=59391969 (дата обращения: 25.03.2026).

[335] Дмитриев О. Н., Макарова Е. Л. Кадровый дефицит в сфере информационной безопасности: масштабы проблемы и пути решения [Электронный ресурс] // Информационная безопасность регионов. 2024. Т. 21, № 2. С. 12–19. URL: https://elibrary.ru/item.asp?id=56847293 (дата обращения: 15.01.2025).

Недостаточная квалифицированность персонала, ответственного за обеспечение информационной безопасности, стала причиной двухкратного роста успешных кибератак на критическую инфраструктуру РФ с 2023 по 2024 гг., – говорят эксперты[336].

Тысячи специалистов по информационной безопасности выпускаются учебными учреждениями РФ, но они или не работают по специальности или оказываются неготовыми к реальной работе, и работодателю приходится их дополнительно обучать[337]. Из этого напрашивается очевидный вывод о том, что образовательная программа не соответствует реальным задачам, которые приходится решать на практике.

Образовательные программы не справляются с быстро меняющимися реалиями информационной безопасности, это приводит к тому, что информация, полученная студентом, становится неактуальной еще до его выпуска из образовательного учреждения.

Имеется также нехватка специалистов с высокой квалификацией, которые могли бы противодействовать APT и сложным целевым атакам.

Менее четверти от специалистов по информационной безопасности, согласно исследованиям, способны противодействовать таким угрозам[338]. Количество злоумышленников, способных создавать такие угрозы, растет несоразмерно быстрее, чем количество специалистов, способных этому противодействовать.

Ситуация в регионах еще более критическая, чем по стране в целом. У них нет средств и возможностей чтобы удержать хотя бы минимальное количество специалистов у себя. Централизация образовательных и профессиональных ресурсов в мегаполисах создает опасную асимметрию в уровне защищенности информационных систем в государстве.

При анализе нынешней системы подготовки кадров в сфере информационной безопасности можно заметить несколько критических проблем, носящих системный характер. Первая и наиболее существенная из них – отрыв теоретической подготовки от практических задач, с которыми сталкиваются специалисты в реальной профессиональной деятельности.

Современные образовательные программы по информационной безопасности перегружены дисциплинами общетеоретического характера, в то время как практическим навыкам работы с актуальными инструментами защиты, методами реагирования на инциденты и форензики уделяется недостаточное внимание. Студенты изучают математические основы криптографии, теорию информации и формальные модели безопасности, но при этом не получают опыта настройки современных систем защиты, анализа вредоносного кода или проведения аудита безопасности реальных информационных систем.

Вторая проблема связана с недостаточной квалификацией преподавательского состава в практических аспектах современной информационной безопасности. Большинство преподавателей вузов – академические специалисты, обладающие фундаментальными знаниями, но не имеющие актуального опыта работы в индустрии. Они не сталкиваются с современными киберугрозами в реальных условиях, не участвуют в расследовании инцидентов и реагировании на атаки. Приглашенные практики из компаний привлекаются эпизодически и не могут системно влиять на содержание образовательных программ[339].

Материально-техническая база большинства образовательных учреждений также не соответствует современным требованиям. Создание полноценных учебных полигонов, имитирующих реальную инфраструктуру организаций и позволяющих отрабатывать навыки защиты и противодействия атакам, требует значительных финансовых вложений. Программное обеспечение для обучения и практических занятий быстро устаревает, а его регулярное обновление и лицензирование обходятся дорого[340].

В системе подготовки специалистов по информационной безопасности существует проблема с практической подготовкой: компании из соображений безопасности не могут допустить студента к реальной задаче, а вузы не справляются с контролем качества практики – это делает практику формальной и неэффективной.

---

[336] Смирнов К. А., Петров И. В. Киберугрозы 2023–2024: аналитический обзор. М. : Центр стратегических исследований, 2024. 156 с.

[337] Иванова С. П. Профессиональные стандарты в области информационной безопасности: современное состояние и перспективы развития. М. : ИНФРА-М, 2024. 198 с.

[338] Там же.

[339] Федоров Н. В. Практико-ориентированное обучение в системе подготовки специалистов по информационной безопасности // Образование и наука в России и за рубежом. 2023. № 6 (95). С. 67–74.

[340] Васильев В. И., Кузнецова Т. В. Проблемы материально-технического обеспечения образовательного процесса в сфере информационной безопасности // Информационное общество. 2023. № 4. С. 28–36.

Еще одна проблема – это отсутствие единых, согласованных с индустрией, профессиональных стандартов и требований к квалификации специалистов различного уровня. Работодатели предъявляют множество требований к кандидатам, а образовательные учреждения формируют программы на основе своего понимания потребностей рынка труда, а выпускник не имеет четкого понимания о том, какие настоящие компетенции и навыки востребованы и как их продемонстрировать[341].

Ситуацию осложняет недостаточное внимание к развитию навыков коммуникации, работы в команде, критического мышления и принятия решений в сложных условиях. Специалисту по информационной безопасности необходимо не просто иметь технические знания, но и уметь взаимодействовать с подразделениями организации, объяснять технические риски руководству, участвовать в формировании политики безопасности. Образовательные программы часто упускают эти компетенции и не делают их частью целенаправленного развития в рамках образовательных программ.

В сфере информационной безопасности необходимо быстро адаптироваться, т. к. технологии и угрозы быстро меняются, а система дополнительного профессионального образования развита недостаточно[342].

Для того чтобы решить проблему подготовки кадров в сфере информационной безопасности, необходимо объединить усилия образовательных учреждений, работодателей, а также государства[343]. Для этого нужно взять курс на практическое обучение с высоким участием потенциальных работодателей.

Эффективными могли бы стать форматы «двойного руководства» выпускных работ с привлеченными практикующими специалистами через систему «профессоров практики»[344]. Необходимо развить «учебные полигоны» для отработки практических навыков в условиях, максимально приближенных к реальным[345].

В перспективе могут хорошо себя показать соревновательные форматы обучения (CTF, киберполигоны) и развитие системы независимой сертификации[346]. Нужно создавать сетевые образовательные программы, объединяющие ресурсы вузов и компаний потенциальных работодателей.

Система профессиональной сертификации должна быть независимой и доступной через дистанционные технологии с созданием сети сертификационных центров[347].

Особую роль в совершенствовании системы подготовки кадров играет развитие корпоративных программ подготовки и использование онлайн-форматов для обеспечения доступности обучения. Создание современных учебных центров и развитие программ переподготовки IT-специалистов значительно расширит кадровый потенциал отрасли[348].

Развитие программ переподготовки специалистов из смежных IT-областей является важным направлением. IT-специалисты, обладающие опытом разработки и администрирования систем, а также работы с сетями, уже имеют необходимые компетенции и могут быстро освоить специализацию в области информационной безопасности. Целевые программы переподготовки могли бы стать источником большого притока квалифицированных кадров в отрасль.

Использование потенциала онлайн-образования и открытых образовательных ресурсов для обеспечения доступности качественного обучения в регионах и для работающих специалистов улучшит качество подготавливаемых кадров. Ведущие вузы и образовательные центры, создавая и развивая онлайн-курсы, вебинары и образовательные платформы, позволят получать актуальные знания независимо от места проживания и графика работы[349].

Проблема подготовки кадров в сфере информационной безопасности требует системного решения, так как дефицит квалифицированных специалистов уже сейчас создает серьезные угрозы и риски для национальной безопасности и цифровой экономики РФ.

Главные проблемы подготовки кадров в сфере информационной безопасности неразрывно связаны с качеством подготовки и отрывом образования от потребностей индустрии информационной безопасности, устаревшей материально-технической базой и недостатком преподавателей-практиков, все это требует совместных усилий образовательных учреждений, работодателей и государства.

---

[341] Иванова С. П. Указ. соч.

[342] Дмитриев О. Н., Макарова Е. Л. Указ. соч.

[343] Арсеньев Д. Г., Ковалева И. А. Современные подходы к подготовке специалистов в области информационной безопасности [Электронный ресурс] // Вопросы кибербезопасности. 2024. № 3 (61). С. 45–53. URL: https://elibrary.ru/item.asp?id=54289176 (дата обращения: 15.01.2025).

[344] Федоров Н. В. Указ. соч. С. 67–74.

[345] Васильев В. И., Кузнецова Т. В. Проблемы материально-технического обеспечения образовательного процесса в сфере информационной безопасности // Информационное общество. 2023. № 4. С. 28–36.

[346] Смирнов К. А., Петров И. В. Указ. соч.

[347] Иванова С. П. Указ. соч.

[348] Григорьев А. С. Компетентностный подход к подготовке специалистов по защите информации: теория и практика. М. : Горячая линия-Телеком, 2023. 264 с.

[349] Дмитриев О. Н., Макарова Е. Л. Указ. соч.

Перспективные направления – это переход к обучению, ориентированному на практику, создание современных «учебных полигонов», а также развитие системы профессиональной сертификации и непрерывного образования. Решение этих проблем необходимо для обеспечения безопасного цифрового будущего страны.

С. Е. Красин,
магистрант 1 курса Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Научный руководитель: Г. Г. Камалова, д.ю.н., доцент
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

Стратегии развития национальных технологий для повышения технологического суверенитета

В современном мире технологическая дисциплина стала неотъемлемой частью национальной безопасности, экономики и стратегической самостоятельности государств. Возможность самостоятельно разрабатывать, производить и использовать передовые технологии определяет уровень суверенитета страны, её конкурентоспособность и устойчивость в условиях глобальных вызовов. В связи с этим вопросам развития национальных технологий уделяется особое значение: создание условий для инновационной деятельности, развитие научно-технического потенциала, формирование соответствующей инфраструктуры и нормативной среды.

В данном докладе рассматриваются основные стратегии развития национальных технологий для повышения технологического суверенитета. Особое внимание уделяется ключевым аспектам: формированию инновационной экосистемы, государственной поддержке научных исследований, развитию человеческого капитала, сохранению интеллектуальной собственности и построению международных сотрудничеств.

Технологический суверенитет заключается в способности государства к самостоятельной разработке, производству и контролю за ключевыми технологиями и научной инфраструктурой, которые являются важной частью для обеспечения экономической независимости и национальной безопасности.

Среди стратегий для формирования технологического суверенитета в государстве можно выделить:

1. *Финансовая поддержка государства.* Государство выделяет гранты и налоговые льготы для изобретателей. В 2026 году в России существует несколько программ, направленных на финансовую поддержку и развитие новых открытий. Среди них конкурс «Умник», проводящийся при поддержке Минэкономразвития и направленный на финансирование научных «стартапов».

2. *Развитие национальных научных и технологических инфраструктур.* Объединение научных, предпринимательских и государственных ресурсов при создании инновационных центров и лабораторий. Данное действие создает почву для эффективного внедрения научных достижений во все сферы производства. В качестве примера можно выделить создание в РФ технополисов «Сколково и Иннополис».

3. *Подготовка кадров.* Еще одной стратегией является обучение и подготовка целевых специалистов. Согласно данной стратегии происходит обучение молодых ученых и предпринимателей посредством финансирования обучения и повышения квалификации за счет государства.

Государство выделяет субсидии и гранты, а также создает программы для обмена знаниями между учебными заведениями, в том числе из-за рубежа.

4. *Правовое обеспечение по защите интеллектуальной собственности.* Создание новых технологий является интеллектуальной собственностью и требует всесторонней правовой защиты. Урегулирование данного вопроса в правовом поле, защита инноваций от краж, является стимулом для развития научной деятельности. Правовое обеспечение по защите интеллектуальной собственности формирует здоровую конкуренцию на рынке разработок.

5. *Внедрение национальных стандартов.* Создание правовой базы, которая регулирует разработку и внедрение в производство новых технологий будет способствовать минимизации рисков при инвестициях в разработку таких технологий[350].

[350] Гостинский В. В. Технологический суверенитет: концепции и стратегии // Вестник науки и образования. 2021. № 4. С. 15–22.

Указанные выше стратегии невозможны без механизмов их реализации. Среди таких механизмов следует выделить:

– обеспечение финансирования развития технологий посредством создания государственных программ и проектов;

– объединение научных и промышленных предприятий для совместных разработок;

– грантовая система: стимулирование исследований молодых ученых и стартапов;

– образовательные инициативы: совершенствование системы высшего технического образования, развитие программ профессиональной переподготовки;

– механизмы защиты и экспорта технологий: развитие системы патентования и экспорта инновационной продукции[351].

Выделим несколько стратегических направлений, к развитию которых должны быть приурочены национальные программы:

1. *Информационно-коммуникационные технологии (ИКТ).* ИКТ – фундамент современного цифрового общества и экономики. Важной задачей является создание национальных платформ, программных решений, развитие кибербезопасности и цифровой инфраструктуры.

2. *Биотехнологии и медицина.* Развитие этих сфер обеспечивает не только технологическую независимость в области здравоохранения, но и развитие фармацевтики, агробизнеса и сельского хозяйства.

3. *Энергетика и экология.* Важна разработка альтернативных источников энергии, технологий улавливания и хранения углерода, а также решений в сфере экологической безопасности.

4. *Машиностроение и высокоточные технологии.* Создание отечественного производства высокоточных машиностроительных комплектующих, робототехники, авиационно-космической техники.

5. *Новые материалы и наноиндустрия*[352].

В данном контексте необходимо выделить и проблемные аспекты при внедрении стратегий развития национальных технологий. Среди таковых: недолгосрочность финансирования проектов, отток квалифицированных кадров из государства, санкции и отсутствие привычной международной торговли (в том числе знаниями и достижениями), недостаточная координация между научными сообществами внутри страны[353].

В рамках работы также было принято решение выделить успешный международных опыт по внедрению стратегий. Таким образом, можно выделить:

– *Китай.* Развитие 10 секторов, призванных помочь в цифровизации, включая робототехнику, кибернетику и другие.

– *США.* Развитие искусственного интеллекта, квантовых технологий и кибербезопасности.

– *ЕС.* Создание единой цифровой экономики.

РФ в данный момент сосредоточена на развитии энергетики, атомных технологий и внедрении цифровых аспектов во все сферы производства[354].

В заключение можно выделить следующие перспективы для дальнейшего развития: укрепление связей между государством, научным сообществом и бизнесом; обеспечение стабильного финансирования, в том числе для долгосрочных проектов; финансирование подготовки кадров; развитие международного сотрудничества для обмена опытом и кадрами.

---

[351] Федеральная служба по интеллектуальной собственности. Национальная стратегия развития технологий РФ на 2030 год (утв. постановлением Правительства). Москва, 2022.

[352] Иванова Е. А., Петров В. П. Инновационная политика и развитие национальных технологий. М. : Наука, 2019. 304 с.

[353] Кузнецов А. П. Государственное регулирование инновационных процессов // Экономика и управление. 2020. № 6. С. 45–51.

[354] Захаров С. И. Международное сотрудничество в области технологий: вызовы и перспективы // Международная политика. 2022. Т. 18, № 3. С. 76–85.

Содержание

ОПИСАНИЕ ФУНКЦИОНАЛЬНОСТИ ИЗДАНИЯ:

Интерфейс электронного издания (в формате pdf) можно условно разделить на 2 части.

Левая навигационная часть (закладки) включает в себя содержание книги с возможностью перехода к тексту соответствующей главы по левому щелчку компьютерной мыши.

Центральная часть отображает содержание текущего раздела. В тексте могут использоваться ссылки, позволяющие более подробно раскрыть содержание некоторых понятий.

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ:

Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше; 8x DVD-ROM; разрешение экрана 1024×768 или выше; программа для просмотра pdf.

СВЕДЕНИЯ О ЛИЦАХ, ОСУЩЕСТВЛЯВШИХ ТЕХНИЧЕСКУЮ ОБРАБОТКУ И ПОДГОТОВКУ МАТЕРИАЛОВ:

Оформление электронного издания : Издательский центр «Удмуртский университет».

Макет и компьютерная верстка: И. А. Бусоргина.

Авторская редакция.

Подписано к использованию 12.08.2026
Объем электронного издания 2,9 Мб, тираж 10 экз.
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел.: +7(3412)263-751 E-mail: editorial@udsu.ru