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

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Сборник статей

Ижевск
2023

УДК 34:004.056(063)
ББК 67.401.114я431
О-136

Рекомендовано к изданию редакционно-издательским советом УдГУ

Научные редакторы: *Г.Г. Камалова*, д-р юрид. наук, доцент, зав. каф. информ. безопасности в упр. ФГБОУ ВО «УдГУ»,
В.Г. Ившин, канд. юрид. наук, доцент, директор ИПСУБ, профессор каф. уголовного права и криминологоии ФГБОУ ВО «УдГУ»;
Г.А. Решетникова, канд. юрид. наук, доцент, зам. директора по науч. работе ИПСУБ ФГБОУ ВО «УдГУ».

О-136 Обеспечение информационной безопасности: вопросы теории и практики : сб. ст. / науч. ред. Г.Г. Камалова, В.Г. Ившин, Г.А. Решетникова. – Ижевск – Удмуртский университет, 2023. – 190 с.

ISBN 978-5-4312-1123-2
DOI: 10.35634/978-5-4312-1123-2-2023-1-190

В издание вошли статьи участников Всероссийской научно-практической конференции, проведенной 29 мая 2023 г. Институтом права, социального управления и безопасности Удмуртского государственного университета в рамках ПСАЛ «Приоритет-2030». Авторами рассматриваются актуальные вопросы теории и практики обеспечения информационной безопасности.

УДК 34:004.056(063)
ББК 67.401.114я431

ISBN 978-5-4312-1123-2

Полякова Татьяна Анатольевна,
д.ю.н., профессор, и.о. зав. сектором информационного права и международной информационной безопасности ФГБУН «Институт государства и права Российской академии наук», г. Москва

ФОРМИРОВАНИЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРАВОВЫЕ ВЕКТОРЫ[1]

Динамично развивающийся цивилизационный кризис в рамках четвертой промышленной революции в результате цифровизации и происходящие геополитические изменения влекут дальнейший рост вызовов и угроз национальной безопасности в информационном пространстве, что нашло отражение в Стратегии национальной безопасности РФ, в которой впервые обозначена приоритетность вопросов информационной безопасности, выделен отдельный раздел[2], что свидетельствует о стратегическом характере обеспечения информационной безопасности.

Следует признать, что в настоящее время на все стороны деятельности государства, общества и жизни человека влияют цифровые технологии, позволяющие не только повысить эффективность многих информационных процессов, но и представляющие определенные и все возрастающие угрозы информационной безопасности. При этом существующие риски и вызовы в информационном пространстве, возрастающие в ходе усиливающегося противостояния с «коллективным западом», сейчас как никогда детерминируют необходимость роста требований к культуре информационной безопасности граждан, углубление которой приобретает характер

[1] Статья подготовлена в рамках выполнения государственного задания № FMUZ-2021-0042 «Правовое регулирование цифровой экономики, искусственного интеллекта, информационной безопасности».

[2] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 02.07.2021 № 400 // Собрание законодательства РФ. 2021. № 27 (часть II), ст. 5351.

одной из приоритетных задач в целях защиты национальных интересов Российской Федерации.

В связи с этим возрастает значение фундаментальных, междисциплинарных исследований, связанных с обеспечением информационной безопасности, которые ведутся широким кругом ученых и практиков самых разных научных направлений, таких как философия, математика, экономика, право, менеджмент, инженерия, компьютерные науки и иных. Правовые проблемы, связанные с различными аспектами информационной безопасности, в настоящее время представлены во многих отраслевых юридических науках.

В информационном праве Российской Федерации как публично-правовой отрасли традиционно ведутся научные исследования по широкому кругу вопросов обеспечения информационной безопасности. В рамках правового обеспечения информационной безопасности как ключевой подотрасли российского информационного права в системе публично-правовых отраслей вопросы безопасности в информационном пространстве традиционно рассматриваются комплексно и касаются как правовой защиты различных видов информации, включая информацию ограниченного доступа[3], так и формирования безопасной для человека, общества и государства информационной среды в условиях расширения информационных угроз и рисков, в том числе для решения вопросов обеспечения информационно-психологической безопасности личности[4].

При этом правовые вопросы обеспечения безопасности личности как наиболее уязвимого субъекта информационных правоотношений по мере расширения использования цифровых технологий приобретают высокую значимость для защиты интересов общества

---

[3] *Камалова Г.Г.* Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : дис. … д-ра юрид. наук / Институт государства и права РАН. М., 2020. 472 с.

[4] *Смирнов А.А.* Формирование системы правового обеспечения информационно-психологической безопасности в российской Федерации. 2022. 444 с.

и государства[5]. Однако нельзя не отметить сравнительно низкий уровень информационной грамотности основной части населения именно в вопросах обеспечения безопасности в информационной среде, что определяет не просто потребность, но и жизненную необходимость развития культуры информационной безопасности граждан для формирования знаний, умений и навыков отражения наносимых информационных угроз в условиях возрастающего агрессивного противоправного воздействия на их цифровые устройства и программные средства.

В этих условиях в декабре 2022 года закономерно была утверждена Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации, в которой понятие «культура информационной безопасности» определяется как совокупность сформированных знаний, умений и навыков по информационной безопасности, обеспечивающая безопасность гражданина России в информационном пространстве[6]. Следует отметить, что использование понятия культуры многообразно и может трактоваться как направление научной и практической деятельности, нормы поведения, ценные результаты деятельности человека и т.д. В приведенной в Концепции дефиниции понимание культуры информационной безопасности включает в основном массив тех компетенций российского гражданина, который позволит ему обеспечивать безопасность осуществления профессиональной и иной деятельности с использованием цифровых технологий.

Между тем проводимые исследования показывают, что изменению сегодня подвергается не только среда деятельности человека. Кардинальное изменение мира и трансформация концептуальных

---

[5] *Чеботарева А.А.* Правовое обеспечение информационной безопасности личности в глобальном информационном обществе : дис. … д-ра юрид. наук / Институт государства и права РАН. М., 2018. 473 с.

[6] Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации : распоряжение Правительства РФ от 22.12.2022 № 4088-р // Собрание законодательства РФ. 2022. № 52, ст. 9726.

подходов к регулированию информационного пространства влекут дальнейшее развитие прав человека и гражданина в части их расширения и углубления. Значительное влияние на это оказывают цифровые технологии виртуальной и дополненной реальности, искусственного интеллекта и робототехники, распределенного реестра, больших данных и квантовые технологии. Развитие системы правового обеспечения информационной сферы нашло отражение в конституционных положениях, в соответствии с которыми вопросы информационной безопасности и оборота цифровых данных отнесены к федеральному ведению[7].

Правовое обеспечение информационной безопасности как ведущая подотрасль информационного права сегодня получает дальнейшее развитие, обусловленное как трансформационными процессами права под влиянием использования цифровых технологий и изменения общественных отношений, так и углублением научных исследований в этой сфере.

С позиции теории информационной безопасности обеспечение этой безопасности в информационной сфере предполагает достижение триады целевых показателей – целостности, доступности и конфиденциальности. Вместе с тем в этой теории отражен в большой мере технический подход, который сводится к организации и технологии защиты информации, и по сути это отражение преобладающей на западе концепции кибербезопасности.

Однако проблемы обеспечения информационной безопасности не могут быть сведены только к техническим и технологическим вопросам, так как техника и технология являются нейтральными, а результаты их использования определяются мотивами и целями субъекта общественных отношений. В связи с этим наряду с позитивными эффектами цифровизации мы сегодня сталкиваемся

[7] О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти : Закон РФ о поправке к Конституции РФ от 14.03.2020 № 1-ФКЗ // СЗ РФ. 2020. № 11, ст. 1416.

с киберпреступностью, кибербуллингом и многими иными негативными процессами, статистика которых весьма впечатляет[8].

Важно отметить возрастающее деструктивное информационно-психологическое воздействие и, как следствие, стратегическое значение правового обеспечения информационно-психологической безопасности личности как неотъемлемой части достижения интересов национальной безопасности. Особенно это касается детей[9]. Человек, находясь в негативном информационном потоке, должен иметь инструменты защиты своих прав и законных интересов, что требует формирования соответствующих компетенций для безопасного поведения в информационном пространстве.

Ключевую роль в решении этой задачи, безусловно, играет сфера образования, которая на различных уровнях может прививать необходимые компетенции и национальные культурные ценности России[10]. Вместе с тем при этом важен баланс теории и практики, позволяющий получать практически-ориентированные результаты научных исследований и профессиональной подготовки различных направлений. Однако сегодня курсы основ информационной безопасности, информационного права и правового обеспечения информационной безопасности включены в планы подготовки далеко не всегда, в том числе в системе юридического образования. Следует признать такую ситуацию недопустимой в современных условиях цифровизации, так как формирование понимания особенностей правового регулирования информационной среды и знания информационного законодательства сегодня являются для будущих юристов

---

[8] Актуальные киберугрозы: итоги 2022 года // Positive technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 01.07.2023).

[9] *Камалова Г.Г.* Правовое обеспечение конфиденциальности информации в образовательной сфере: к дискуссии о педагогической тайне // Аграрное и земельное право. 2020. № 2 (182). С. 135-138.

[10] *Полякова Т.А., Троян Н.А.* Образование и культура информационной без-опасности граждан Российской Федерации: научно-правовые аспекты // Образование и право. 2023. № 3. С. 310-317.

и специалистов в области защиты информации императивными и позволяют получить необходимые знания и навыки противодействия деструктивному информационному воздействию.

Важную роль в области обеспечения информационной безопасности играет работа с несовершеннолетними и пропаганда национальных традиционных культурных ценностей, обучение навыкам безопасного использования возможностей сети Интернет как элементов формирования культуры информационной безопасности, которая должна быть заложена с детства.

Для формирования и развития культуры информационной безопасности, безусловно, требуется консолидировать усилия различных субъектов и дальнейшее развитие законодательства в этой области. В этих целях требуется активизация научных информационно-правовых исследований, что важно и для привлечения интереса молодых исследователей к проблемным аспектам цифровизации. Информационное законодательство России прошло определенный путь развития. Однако пока и это нельзя отрицать, информационное право достаточно молодое направление нормативно-правового регулирования, и в условиях цифровых вызовов и дальнейшего развития информационного общества трансформация общественных отношений определяет новые вызовы и угрозы, формируя социальный заказ на системный поступательный прогресс российского информационного права с сохранением его сформированных ценностных ориентиров[11], что определяет новые горизонты данной отраслевой юридической науки[12].

Вместе с тем развитие культуры информационной безопасности невозможно без формирования ответственного поведения граждан в информационной среде, в первую очередь молодежи, которое

---

[11] *Полякова Т.А., Камалова Г.Г.* Ценностные изменения развития информационного права России // Правовое государство: теория и практика. 2023. № 2 (72). С. 53-59.

[12] Новые горизонты развития системы информационного права в условиях цифровой трансформации / *Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов* [и др]. М., 2022.

целесообразно понимать как осознанное отношение к своим действиям при использовании цифровых технологий и понимание их значения и результатов. В этом ключе культуры информационной безопасности научный интерес представляет также предлагаемое право человека на отказ от использования цифровых технологий как возможность реализации прав и свобод человека и гражданина традиционными способами без использования цифровых технологий и, соответственно, без рисков информационного пространства[13]. Однако указанное право пока не получило законодательного закрепления.

Проведенное исследование позволило обосновать необходимость междисциплинарных научных подходов к формированию национальной системы культуры информационной безопасности граждан; обращено внимание на то, что это направление имеет не приходящее, а стратегическое значение для реализации государственной политики обеспечения информационной безопасности, и необходима разработка соответствующей национальной стратегии, в которой требуют отражения вопросы комплексного образования, направленные на приобретение соответствующих навыков и знаний.

Библиографический список

1. Камалова Г.Г. Правовое обеспечение конфиденциальности информации в образовательной сфере: к дискуссии о педагогической тайне // Аграрное и земельное право. – 2020. – № 2 (182). – С. 135-138.

2. Камалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : дис. … д-ра юрид. наук / Институт государства и права РАН. – М., 2020. – 472 с.

3. Наумов В.Б. Отказ от цифровых технологий: абсурд или новое право человека и гражданина // Бачиловские чтения :

[13] *Наумов В.Б.* Отказ от цифровых технологий: абсурд или новое право человека и гражданина // Бачиловские чтения : материалы четвертой междунар. науч.-практ. конф. / Институт государства и права РАН ; отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. Саратов, 2022. С. 78-84.

материалы четвертой междунар. науч.-практ. конф. / Институт государства и права РАН ; отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Нау-мов. – Саратов, 2022. – С. 78-84.

4. Новые горизонты развития системы информационного права в условиях цифровой трансформации [Электронный ресурс] / Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов [и др.]. – М., 2022.

5. Полякова Т.А., Камалова Г.Г. Ценностные изменения развития информационного права России // Правовое государство: теория и практика. – 2023. – № 2 (72). – С. 53-59.

6. Полякова Т.А., Минбалеев А.В., Троян Н.А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. – 2023. – № 5. – С. 131-144.

7. Полякова Т.А., Троян Н.А. Образование и культура информационной безопасности граждан Российской Федерации: научно-правовые аспекты // Образование и право. – 2023. – № 3. – С. 310-317.

8. Смирнов А.А.Формирование системы правового обеспечения информационно-психологической безопасности в российской Федерации : дис. … д-ра юрид. наук / Институт государства и права РАН. – М., 2022. – 444 с.

9. Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе : дис. … д-ра юрид. наук / Институт государства и права РАН. – М., 2018. – 473 с.

Минбалеев Алексей Владимирович,
д.ю.н., профессор, заведующий кафедрой
информационного права и цифровых технологий
ФГБОУ ВО «Московский государственный юридический
университет имени О.Е. Кутафина» (МГЮА),
г. Москва

РЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ЗА И ПРОТИВ

Нормативно-правовое регулирование отношений в сфере искусственного интеллекта (далее – ИИ) в последние два года становится новой концепцией для значительного количества передовых государств мира, что «не является ни универсальным, ни инклюзивным»[14]. Сегодня всем становится понятно, что конструктивная и негативная роль ИИ требует не просто регулирования отдельных аспектов и сфер использования ИИ в том или ином секторе экономики или социальной сферы, но и формирования общих требований к использованию ИИ, в том числе понятийного аппарата, прин-ципов, очерчивания круга субъектов и связанных с ИИ объектов, а также системного регулирования запретов и ограничений при создании и использовании ИИ.

Многие инициативы по регулированию ИИ были мотивированы опасениями по поводу потенциальных злоупотреблений или непредвиденных последствий использования ИИ, а также в связи с определённым разочарованием в действенности подхода приоритета этического регулирования ИИ. Создание многочисленных систем на основе ИИ, которые могут принимать решения без необходимости использования человеческого интеллекта, уже способствует новой машинной революции и максимально быстро

[14] *Gülen K.* Round Table: Will there be a global consensus over AI regulation? URL: https://dataconomy.com/2022/10/24/artificial-intelligence-laws-and-regu-lations/ (дата обращения: 20.07.2023).

стимулирует инновации как в бизнесе, так и в системе государственного управления. В то же время последствия использования ИИ становятся все чаще непредсказуемыми, что требует превентивных законодательных мер по обеспечению и защите прав и свобод граждан, а также обеспечению безопасности общества и государства.

Принятие отдельного закона об ИИ стимулируется как отдельными законодательными инициативами, так и формирующимися политиками и актами в региональных сообществах и объединениях. Так, в январе 2021 года был принят Закон о национальной инициативе в области искусственного интеллекта (U.S.AI Act), который был создан, чтобы обеспечить «всеобъемлющую основу для укрепления и координации исследований, разработок, демонстраций и образовательной деятельности в области ИИ во всех министерствах и агентствах США. В соответствии с Законом Соединенных Штатов об искусственном интеллекте были созданы отделения и целевые группы для реализации национальной стратегии в области ИИ с участием различных федеральных агентств. К ним относятся Федеральная торговая комиссия (FTC), Министерство обороны, Министерство сельского хозяйства, Министерство образования и Министерство здравоохранения и социальных служб»[15].

На уровне ЕС активно разрабатывается европейский закон об ИИ – первый всеобъемлющий закон об ИИ[16]. 11 мая 2023 года «Европейским парламентом принят компромиссный текст Закона об ИИ на стадии комитета, что еще на один шаг приблизило этот закон к завершению. Компромиссный текст (парламентский проект), который вносит поправки в первоначальное предложение Комиссии, включает в себя довольно большое количество поправок, некоторые из которых, скорее всего, не войдут в окончательный

[15] Artificial Intelligence Regulation: What Laws Do Countries Apply to This Tech? URL: https://pixelplex.io/blog/artificial-intelligence-regulation/ (дата обращения: 20.07.2023).

[16] Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. URL: https://artificialintelligenceact.eu/the-act/ (дата обращения: 20.07.2023).

вариант после переговоров по трилогу. Парламентский проект изменяет определение искусственного интеллекта таким образом, что теперь он определяется как «машинная система, которая предназначена для работы с различными уровнями автономии и которая может для явных или неявных целей генерировать результаты, такие как прогнозы, рекомендации или решения, которые влияют на физическую или виртуальную среду». Это более близко согласуется с определением ИИ Европейского совета, чем первоначальное определение Комиссии, которое было подвергнуто критике за чрезмерно широкое распространение. Парламентский проект уточнил и расширил список запрещенных ИИ, включив в него системы биометрической категоризации на основе ИИ, которые классифицируют людей в соответствии с конфиденциальными или защищенными атрибутами, определенные виды использования систем распознавания эмоций на основе ИИ и системы ИИ, которые создают или расширяют базы данных изображений лиц путем извлечения изображений из Интернета. Парламентский проект также вводит общие принципы, для соблюдения которых операторы всех систем ИИ должны приложить все усилия, включая техническую надежность, прозрачность, недискриминацию и справедливость, а также конфиденциальность и управление данными. Проект Совета оставил большую часть обязательств по соблюдению за поставщиками, поэтому это может привести к значительному повышению ответственности за развертывание (например, в отношении использования приложений для найма с поддержкой ИИ). Парламентский проект немного изменяет финансовые штрафы за несоблюдение, увеличивая самый высокий штраф до 40 000 000 евро или 7 % от мирового годового оборота, а также увеличивая и сокращая объем других пороговых значений штрафов»[17].

[17] *White L., Evans M.* The AI Act – A step closer to the first law on Artificial Intelligence. URL: https://www.dataprotectionreport.com/2023/05/the-ai-act-a-step-closer-to-the-first-law-on-artificial-intelligence/ (дата обращения: 20.07.2023).

Многие национальные правительства уже установили законы и правила об искусственном интеллекте о том, как данные должны и не должны использоваться и собираться, хотя иногда они неоднозначны. Обсуждая регулирование ИИ и то, как оно должно быть реализовано, правительства часто сотрудничают с крупными корпорациями.

По крайней мере, уже более 60 стран приняли законы и правила об искусственном интеллекте с 2017 года, что почти соответствует темпам внедрения нового ИИ. Опасения по поводу надвигающихся препятствий на пути международного сотрудничества возникают в связи с ростом управления ИИ. То есть любое новое законодательство окажет значительное влияние на мировые рынки из-за растущей распространенности ИИ как в физических продуктах, так и в онлайн-сервисах.

Одним из основных наиболее обсуждаемых законов является закон об искусственном интеллекте. Сегодня достаточно много обсуждают[18] необходимость принятия такого закона, но, к сожалению,

---

[18] Новые горизонты развития системы информационного права в условиях цифровой трансформации : монография / отв. ред. *Т.А. Полякова, А.В. Мин-балеев, В.Б. Наумов* [и др.]. М. : ИГП РАН, 2022. 368 с.; *Полякова Т.А., Минба-леев А.В., Кроткова Н.В.* Основные тенденции и проблемы развития науки информационного права // Государство и право. 2022. № 9. С. 94-104; *Полякова Т.А., Минбалеев А.В., Троян Н.А.* Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С. 131-144; *Arkhipov V.V., Gracheva A.V., Naumov V.B. et al.* Definition of artificial intelligence in the context of the Russian legal system: a critical approach // State and Law. 2022. No 1. P. 168-178; *Наумов В.Б., Камалова Г.Г.* Вопросы построения юридических дефиниций в сфере искусственного интеллекта // Труды Института государства и права РАН / Proceedings of the Institute of State and Law of the RAS. 2020. Т. 15, № 1. С. 81-93; *Полякова Т.А., Камалова Г.Г.* «Право искусственного интеллекта» и его место в системе информационного права // Правовое государство: теория и практика. 2021. № 3(65). С. 133-145; *Егорова М.А., Минбалеев А.В., Кожевина О.В., Дюфло А.* Основные направления правового регулирования использования искусственного интеллекта в условиях пандемии // Вестник Санкт-Петербургского университета. Право. 2021. Т. 12, № 2. С. 250-262.

пока реальной структуры и содержания закона учеными предложено не было, за исключением модельных актов. Оформление и проявление на практике ряда рисков и угроз, исходящих от искусственного интеллекта, обусловливает значимость разработки и принятия специального законодательства об искусственном интеллекте, в основе которого должен быть базовый федеральный закон об искусственном интеллекте. Соответствующая задача уже поставлена в Российской Федерации на правительственном уровне[19].

Принятие такого закона целесообразно по ряду причин:

1. Необходимость обеспечения и защиты прав и свобод человека и гражданина в связи с созданием и использованием ИИ. Имеющаяся сегодня практика формирования алгоритмов и онтологий искусственного интеллекта позволяет весьма дискретно подходить к вопросам соблюдения практически любых прав и свобод человека и гражданина. Использование искусственного интеллекта в целях обеспечения национальной безопасности, а также в других целях требует установления возможного набора ограничений прав и свобод в связи с соответствующим этим целям его использованием, что возможно только на законодательном уровне.

2. Необходима унификация и формирование единого понятийного аппарата, отражающего природу искусственного интеллекта, а также отдельных технологий, связанных с ним (нейронные сети, онтологии данных, алгоритм искусственного интеллекта и др.)[20].

---

[19] Правительство разработает закон об искусственном интеллекте. URL: https://www.rbc.ru/rbcfreenews/649b950c9a794732a27a407b?ysclid=lkzlfll0bo51299886 (дата обращения: 20.07.2023).

[20] См.: *Минбалеев А.В., Титова Е.В.* Проблемы использования технологий искусственного интеллекта в спортивной сфере и правовые ограничения // Человек. Спорт. Медицина. 2020. Т. 20, № S2. С. 114-119; *Минбалеев А.В., Берестнев М.А., Евсиков К.С.* Регулирование использования искусственного интеллекта в добывающей промышленности // Известия Тульского государственного университета. Науки о Земле. 2022. № 2. С. 509-525; *Nikolskaia K., Naumov V.* Artificial Intelligence in Law // 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020, Vladivostok, 06–09 октября 2020 года. Vladivostok, 2020. P. 9271095.

3. Усиление международной конкуренции за мировое лидерство в сфере развития искусственного интеллекта и технологического лидерства в целом также свидетельствует о значении обеспечения технологического суверенитета Российской Федерации в части отечественных разработок в данной сфере, в том числе отечественных баз данных для обучения нейронных сетей.

4. Активное внедрение искусственного интеллекта во все сферы жизнедеятельности общества, в промышленности, а также в сфере государственного управления; стимулирование государством такого внедрения и использования требует от него фиксации единых правил, которые бы создавали законную основу для развития данного направления. К сожалению, сегодня требования к использованию технологий искусственного интеллекта не носят системного характера, являются фрагментарными и создаются в большей степени ad hoc. В связи с этим необходима разработка и принятие не только базового закона об искусственном интеллекте, но и других специальных нормативных правовых актов, в том числе регулирующих использование данных технологий в той или иной отрасли (сфере), включая беспилотные транспортные системы, генеративный искусственный интеллект, а также касающихся вопросов интеллектуальной собственности, маркировки результатов искусственного интеллекта (особенно важно в отношении генеративного искусственного интеллекта) и комплексных мер государственной поддержки и др.

5. Активно развивающийся опыт регулирования ИИ за рубежом, о чем мы говорили ранее.

Имеются аргументы и против закона об ИИ.

1. Так, еще очень распространено мнение, что в качестве альтернативы правовому регулированию ИИ более эффективным является этическое регулирование в данной сфере, позволяющее определить векторы правового регулирования.

2. Многие производители технологий и акторы, их внедряющие, опасаются, что законодательное регулирование будет направлено на введение дополнительных барьеров, которые могут нега-

тивно сказаться на динамичном характере технологического роста, что представляет определенные риски, как с позиции более конкретного определения того, что государство понимает под искусственным интеллектом.

3. Введение ряда ограничений и запретов в части формирования и контроля за алгоритмами и онтологиями может привести потенциально к нарушению прав значительного количества граждан[21].

4. Определённые сложности связаны с многообразием уже имеющихся сегодня технологий искусственного интеллекта, а также продолжения развития данной тенденции. В связи с этим для правового регулирования некоторые трудности имеет вопрос относительно технологической нейтральности. Так, возникает вопрос: «Регулировать только «слабый» искусственный интеллект или уже есть необходимость специальных законодательных запретов и ограничений в отношении «сильного» искусственного интеллекта»?

5. Сегодня можно выделить целую систему рисков, связанных с созданием и различными способами использования искусственного интеллекта. Возникают вопросы и относительно приоритетности рисков с учетом появления новых, которые потребуют постоянного внесения изменений в нормативные правовые акты.

6. В обществе к развитию и применению технологий искусственного интеллекта относятся с определенной мерой недоверия; продолжает существовать аллармизм, связанный, как показывают

---

[21] *Камалова Г.Г.* Теоретико-правовые аспекты эволюции прав человека в условиях цифровизации и внедрения технологии искусственного интеллекта // Вестник Удмуртского университета. Сер. «Экономика и право». 2021. Т. 31, № 4. С. 662-668; *Камалова Г.Г.* Некоторые вопросы юридической ответственности в связи с разработкой и применением систем искусственного интеллекта и робототехники : сб. избр. ст. по материалам науч. конф-й ГНИИ «Нацразвитие» ; материалы конф-й ГНИИ «Нацразвитие», Санкт-Петербург, 28–30 мая 2019 года. Том Ч. 2. СПб. : ГНИИ «Нацразвитие», 2019. С. 386-393; *Камалова Г.Г.* Искусственный интеллект для развития бизнеса и охрана персональных данных: правовые проблемы обеспечения баланса интересов // Право и бизнес: правовое пространство для развития бизнеса в России : кол. монография в 4-х т. Т. 3. М. : ООО «Проспект», 2020. С. 122-130.

социологические исследования, с низким уровнем правосознания в обществе в этой части. Многие усматривают в развитии регулирования искусственного интеллекта попытки государством его официального внедрения и использования против граждан.

Нормативно-правовое регулирование использования ИИ сегодня оказывает воздействие не только на отдельных граждан и организации, как это было всего несколько лет назад, но влияет уже на общество в больших масштабах, а также на государство и мировую политику. В связи с этим важность данных общественных отношений возрастает с геометрической прогрессией, что требует скорейшего вмешательства государства в эти процессы. Мировые тенденции в этом вопросе свидетельствуют о сложности и неоднозначности подходов в регулировании использования ИИ, но сегодня мы уже можем говорить об определённых закономерностях регулирования, а также возникающих рисках и угрозах. Пока неясно и то, как должен осуществляться контроль в сфере ИИ, как должен выстраиваться баланс между свободой технического развития и государственными ограничениями в этой сфере, как должен быть организован мониторинг развития ИИ, а также множество других вопросов, требующих скорейшего решения на законодательном уровне.

Библиографический список

1. Arkhipov V.V., Gracheva A.V., Naumov V.B. et al. Definition of artificial intelligence in the context of the Russian legal system: a critical approach // State and Law. – 2022. – No 1. – P. 168-178.

2. Nikolskaia K., Naumov V. Artificial Intelligence in Law // 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020, Vladivostok, 06–09 октября 2020 года. – Vladivostok, 2020. – P. 9271095.

3. Егорова М.А., Минбалеев А.В., Кожевина О.В., Дюфло А. Основные направления правового регулирования использования искусственного интеллекта в условиях пандемии // Вестник Санкт-Петербургского университета. Право. – 2021. – Т. 12, № 2. – С. 250-262.

4. Камалова Г.Г. Искусственный интеллект для развития бизнеса и охрана персональных данных: правовые проблемы обеспечения баланса интересов // Право и бизнес: правовое пространство для развития бизнеса в России : кол. монография в 4-х томах. Т. 3. – М. : ООО «Проспект», 2020. – С. 122-130.

5. Камалова Г.Г. Некоторые вопросы юридической ответственности в связи с разработкой и применением систем искусственного интеллекта и робототехники : сб. избр. ст. по материалам науч. конф-й ГНИИ «Нацразвитие» ; материалы конф. ГНИИ «Нацразвитие», Санкт-Петербург, 28–30 мая 2019 года. Том Ч. 2. – СПб. : ГНИИ «Нацразвитие», 2019. – С. 386-393.

6. Камалова Г.Г. Теоретико-правовые аспекты эволюции прав человека в условиях цифровизации и внедрения технологии искусственного интеллекта // Вестник Удмуртского университета. Серия «Экономика и право». – 2021. – Т. 31, № 4. – С. 662-668.

7. Минбалеев А.В., Титова Е.В. Проблемы использования технологий искусственного интеллекта в спортивной сфере и правовые ограничения // Человек. Спорт. Медицина. – 2020. – Т. 20, № S2. – С. 114-119.

8. Минбалеев А.В., Берестнев М.А., Евсиков К.С. Регулирование использования искусственного интеллекта в добывающей промышленности // Известия Тульского государственного университета. Науки о Земле. – 2022. – № 2. – С. 509-525.

9. Наумов В.Б., Камалова Г.Г. Вопросы построения юридических дефиниций в сфере искусственного интеллекта // Труды Института государства и права РАН. – 2020. – Т. 15, № 1. – С. 81-93.

10. Новые горизонты развития системы информационного права в условиях цифровой трансформации : монография / отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов [и др.]. – М. : ИГП РАН, 2022. – 368 с.

11. Полякова Т.А., Камалова Г.Г. «Право искусственного интеллекта» и его место в системе информационного права // Правовое государство: теория и практика. – 2021. – № 3(65). – С. 133-145.

12. Полякова Т.А., Минбалеев А.В., Троян Н.А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. – 2023. – № 5. – С. 131-144.

13. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Основные тенденции и проблемы развития науки информационного права // Государство и право. – 2022. – № 9. – С. 94-104.

Камалова Гульфия Гафиятовна,
д.ю.н., доцент, заведующая кафедрой
информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ

Экспоненциальное развитие цифровых технологий и информационного пространства оказывает в настоящее время трансформирующее воздействие на все сферы жизни человека, детерминируя переход на следующий этап цивилизации. Не осталась в стороне от этого процесса и информационная безопасность, которая всегда испытывала значительное влияние информационно-технологического прогресса, используя его достижения в целях обеспечения национальной безопасности.

Ключевую роль в воздействии современных технологий на общество, полагаем, играет технология искусственного интеллекта, позволяющая интегрировать иные технологические достижения и придавать результатам их развития синергетический эффект. В этой связи в Российской Федерации была принята Национальная стратегия развития искусственного интеллекта

на период до 2030 года[22]. Не углубляясь в дискуссию о понятии искусственного интеллекта и множестве иных дискуссионных организационно-правовых вопросов, как рассмотренных ранее[23], в этом исследовании остановимся на влиянии технологии искусственного интеллекта на организационно-правовые вопросы обеспечения информационной безопасности в целях их научного осмысления.

Взаимосвязь технологии искусственного интеллекта и информационной безопасности носит дуалистический характер. С одной стороны, развитие указанной технологии несет множество информационных рисков, потенциал которых сегодня в полной мере невозможно оценить в силу возможных будущих интегративных эффектов воздействия на социум. С другой стороны, внедрение технологии искусственного интеллекта открывает новые возможности для практики обеспечения информационной безопасности, включая процессы информационно-аналитической деятельности, мониторинга и много иного.

Следует отметить, что в современном мире технология искусственного интеллекта играет важную роль в процессах обеспечения информационной безопасности, так как используется при обработке и анализе больших данных и информационных угроз, а также выявлении уязвимостей и компьютерных атак. Технологию искусствен-

---

[22] О развитии искусственного интеллекта в Российской Федерации : Указ Президента РФ от 10.10.2019 № 490 // Собрание законодательства РФ. 2019. № 41, ст. 5700.

[23] *Камалова Г.Г.* Некоторые вопросы защиты прав человека при использовании искусственного интеллекта и роботов // Бачиловские чтения : материалы четвертой междунар. науч.-практ. конф. / Ин-т гос-ва и права РАН ; отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. Саратов, 2022. С. 312-320; *Архипов В.В., Камалова Г.Г., Наумов В.Б., Незнамов А.В*. Комплексное исследование правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники. СПб., 2022. 336 с.; *Полякова Т.А., Камалова Г.Г.* Проблемы формирования правовой политики в сфере применения технологии искусственного интеллекта // Правовая политика и правовая жизнь. 2023. № 1. С. 28-36. и др.

ного интеллекта активно применяют в составе различных систем защиты от вредоносного программного обеспечения, что позволяет не только автоматически обнаруживать и анализировать такие угрозы, но и принимать меры по защите от них.

Важными направлениями применения технологии искусственного интеллекта является анализ потоков данных и использование алгоритмов машинного обучения для выявления аномалий поведения пользователей, что позволяет обнаруживать возможные угрозы и предотвращать атаки на ранних стадиях. Технология искусственного интеллекта также может использоваться для создания интеллектуальных систем анализа уязвимостей и баз потенциальных и существующих уязвимостей. Кроме того, использование программных инструментов на базе технологии искусственного интеллекта позволяет исследователям в области информационной безопасности устанавливать значимые взаимосвязи цифровых данных, выявляя закономерности между различными процессами и событиями, что может быть использовано как в исследовательской деятельности, так и в практике защиты информации.

Однако использование этой технологии, как было указано выше, также может создавать определенные риски информационной безопасности. Технология искусственного интеллекта, как любая технология, является нейтральной в своей сущности и может быть использована и в неправомерных и даже преступных целях. Так, искусственный интеллект может использоваться для создания новых типов кибератак или вирусов и вредоносных программ. Это означает, что защита от компьютерных атак должна становиться все более интеллектуальной, а специалисты по безопасности данных должны постоянно развивать свои навыки и знания. Кроме того, получает все большее распространение технология «дипфейк», позволяющая реализовывать ранее не известные мошеннические схемы. Сегодня ни один пользователь при опосредованном информационными технологиями общении не может быть уверен в том, что он взаимодействует с человеком, а не с генерированной системой.

В рамках рассматриваемой темы следует также отметить уязвимости информационной безопасности в процессе машинного обучения, которое строится на основе больших объемов цифровых данных. Использование больших данных формирует значительный круг информационных угроз для субъектов, данные которых в какой-либо форме используются. Вместе с тем недостаточно обученная система может быть не в полной мере надежна с точки зрения безопасности, допускать ошибки и содержать уязвимости. Значительные риски это обстоятельство порождает при применении таких систем в объектах критической информационной инфраструктуры. Так, внедрение недостаточно обученной системы в кредитно-финансовой сфере позволяет пройти биометрическую идентификацию с использованием дипфейка[24]. Кроме того, как и любая другая технология, искусственный интеллект сам может быть подвержен компьютерным атакам.

Следовательно, можно констатировать, что безопасность искусственного интеллекта и искусственный интеллект в целях безопасности являются важными областями исследований и разработок. Вместе с тем в этой области существуют не только технологические, но и организационно-правовые проблемы.

В августе 2020 года в России была принята Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года (далее – Концепция)[25], в которой отмечается ключевое значение обеспечения безопасности личности общества и государства при модернизации нормативного регулирования процессов создания и применения технологии искусственного интеллекта с учетом серьезности вызовов, формируемых этой технологией для российского права.

---

[24] О машинном обучении с точки зрения ИБ: реальная обстановка // Хабр. URL: https://habr.com/ru/companies/pt/articles/721930/ (дата обращения: 15.06.2023).

[25] 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 // Собрание законодательства РФ. 2020. № 35, ст. 5593.

Следует отметить, что сегодня системное правовое регулирование в этой области отсутствует. Применяются как общие нормы, так и нормы отдельных правовых актов в рамках действия некоторых специальных правовых режимов. В связи с этим важнейшей задачей на современном этапе является формирование организационно-правовых условий для создания и использования решений на базе искусственного интеллекта в доверенном и безопасном исполнении, что возможно при предварительной оценке рисков развития технологии искусственного интеллекта для безопасности личности, общества и государства и применении риск-ориентированного подхода.

Развитие регуляторных механизмов в этой области требует также нахождения баланса между требованиями по обеспечению безопасности обработки персональных данных и потребностями их использования для обучения искусственного интеллекта, так как большие объемы доступных цифровых данных являются важнейшими факторами развития этой технологии. В связи с этим требуется совершенствование российского законодательства в целях достижения доступности данных при одновременном введении ответственности разработчиков и операторов за безопасность их использования.

Кроме того, в Концепции отмечается, что сегодня должны быть заложены основы правового регулирования разнообразных цифровых платформ, содержащих общедоступные обезличенные данные для разработчиков решений на базе технологии искусственного интеллекта. Это, помимо прочего, требует дальнейшего развития законодательства об информации ограниченного доступа.

Таким образом, организационно-правовое обеспечение информационной безопасности разработки и внедрения решений на базе технологии искусственного интеллекта в настоящее время и формирование к ним доверия являются важнейшими факторами развития этой прорывной цифровой технологии.

Библиографический список

1. Камалова Г.Г. Некоторые вопросы защиты прав человека при использовании искусственного интеллекта и роботов // Бачи-

ловские чтения : материалы четвертой междунар. науч.-практ. конф. / Ин-т гос-ва и права РАН ; отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. – Саратов, 2022. – С. 312-320.

2. Архипов В.В., Камалова Г.Г., Наумов В.Б., Незнамов А.В. Комплексное исследование правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники. – Санкт-Петербург, 2022. – 336 с.

3. О машинном обучении с точки зрения ИБ: реальная обстановка // Хабр. – URL: https://habr.com/ru/companies/pt/articles/721930/ (дата обращения: 15.06.2023).

4. Полякова Т.А., Камалова Г.Г. Проблемы формирования правовой политики в сфере применения технологии искусственного интеллекта // Правовая политика и правовая жизнь. – 2023. – № 1. – С. 28-36.

Меркушев Олег Владимирович,
к.т.н., доцент кафедры информационной безопасности в управлении, заведующий Информационно-правовым центром ФГБОУ ВО «Удмуртский государственный университет»
Колчерина Жанна Николаевна,
старший преподаватель кафедры информационной безопасности в управлении, руководитель проекта «Полигон для апробации и внедрения отечественного программного обеспечения» ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

ПОЛИГОН ДЛЯ АПРОБАЦИИ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: ПЕРСПЕКТИВЫ РАЗВИТИЯ

В рамках стратегического проекта «Центр смарт компетенции цифровой трансформации Удмуртской Республики» сотрудниками Института права, социального управления и безопасности

(далее – ИПСУБ) ФГБОУ ВО «УдГУ» реализуется проект «Полигон для апробации и внедрения отечественного программного обеспечения». Целями данного проекта являются:

- Реализация государственной политики по импортозамещению через подготовку кадров по компетенциям:

– администрирование программных, программно-аппаратных ИТ-решений и оборудования отечественных разработчиков;

– способность эксплуатировать российские ИТ-решения в бизнес процессах.

- Формирование цифровой экосистемы, обеспеченной технологиями, направленными на удовлетворение потребностей всех участников образовательного процесса, с учетом требований по информационной безопасности.

Внедрение лабораторных программно-аппаратных комплексов информационной безопасности (далее – ИБ) в учебный процесс сопряжено с рядом сложностей. Информационная безопасность организации является системным понятием. В рамках телекоммуникационной системы организации информационная безопасность обеспечивается комплексом мер и представляет собой систему. Таким образом, внедряемые в учебный процесс лабораторные комплексы должны включать в свой состав элементы телекоммуникационной системы (или их имитацию), а также средства информационной безопасности организации. Данная задача может быть решена путем создания учебных стендов на основе поставляемого производителями оборудования. Однако это решение имеет ряд недостатков:

- ограниченность количества используемого оборудования;
- невозможность реализации сложных топологий;
- ограниченность времени использования стенда;
- территориальная локализация стендов.

Другим вариантом решения поставленной задачи является применение программных продуктов виртуализации для рабочих станций. При реализации данного решения используются возможности формирования простых сетевых топологий, а также персонализации лабораторных комплексов. Однако остаются нерешенными

задачи построения сложных сетевых инфраструктур, масштабирование вычислительных ресурсов лабораторного комплекса, введение в лабораторные комплексы новых видов телекоммуникационных устройств и средств безопасности, а также использование удаленного доступа к лабораторным комплексам. Все указанные недостатки первых двух методов построения лабораторных комплексов решаются путем создания вычислительного ресурса с системой виртуализации под управлением гипервизоров.

Начиная с 2022 года в составе ИПСУБ реализован и действует центр обработки данных (далее – ЦОД), обеспечивающий возможность проведения практических и лабораторных работ с использованием технологии виртуальных машин под управлением гипервизоров. Наличие ЦОД позволило выполнить трансформацию учебного процесса и применить инновационные технологии:

- формирование персональных лабораторных комплексов на время освоения дисциплины, создавая индивидуальную среду обучения;
- исключить зависимость от определенного рабочего места при работе с лабораторными комплексами;
- применение удаленного доступа к лабораторным комплексам и обеспечение их доступности в любое время;
- формирование тематических кластеров;
- централизованное программное управление распределением ресурсов лабораторных комплексов;
- внедрение системы имитационного моделирования;
- формирование сложной масштабируемой инфраструктуры лабораторных стендов;
- мониторинг деятельности студента в режиме реального времени;
- выполнение проектных работ;
- развитие направления системной цифровой инженерии;
- создание датасетов для решения профессиональных задач.

Формирование масштабируемого вычислительного ресурса под управлением системы виртуализации позволяет решать задачи

внедрения отечественного программного обеспечения, такие как тестирование программного обеспечения в составе виртуальной среды, подготовка сотрудников и профессорско-преподавательского состава (ППС) к переходу на отечественное ПО общего назначения, а также подготовка сотрудников к использованию специализированного отечественного ПО ИБ. На основе созданного ЦОД в ИПСУБ были реализованы и продолжают развиваться следующие проекты:

- центр компетенции по продуктам РЕД СОФТ (ОС, среда виртуализации);
- авторизованный учебный центр РЕД СОФТ;
- внедрение в образовательный процесс УГСН 10.00.00 «Информационная безопасность» курса «Администрирование отечественных ОС»;
- сертификация профессорско-преподавательского состава;
- внедрение инновационных технологий в процесс обучения УГСН 10.00.00 «Информационная безопасность» с дальнейшим включением в образовательные программы инженерного и ИТ-профиля;
- развитие тематических кластеров:
  - отечественные ОС и прикладное ПО;
  - единая среда использования Windows и Linux ОС;
- виртуальные полигоны для построения и тестирования различных типов сетей в облачной инфраструктуре (цифровые двойники);
- реализация пилотного проекта поэтапного перехода АУП университета на отечественное ПО на ресурсах полигона.

Кроме того, в настоящее время ведутся работы по внедрению полигона в бизнес-процессы:

- создание студенческого «киберхаба»;
- разработка исследовательских стендов и сбор профильных датасетов;
- открытие Центров компетенций по продуктам отечественных вендеров;
- переход на практико-ориентированную модель подготовки кадров с профильной углубленной подготовкой студентов УГСН

10.00.00 на основе современных средств защиты информации в интересах индустриального партнера.

Таким образом, на ресурсах Полигона развернута виртуальная среда, предоставляющая возможность развертывания лабораторных стендов по разным тематическим кластерам, таким как: отечественные ОС и прикладное ПО; виртуальные полигоны для построения и тестирования различных типов сетей в облачной инфраструктуре (цифровые двойники). Благодаря участию в программе «Приоритет-2030» мы создаем экосистему, которая позволит выстроить практико-ориентированную модель подготовки кадров с профильной углубленной подготовкой студентов на основе современных ИТ-решений в интересах индустриальных партнеров с использованием технологии виртуализации. В дальнейшем предполагается трансформация образовательного процесса и реализация пилотного проекта по апробации модели «Социо-киберфизической образовательной системы подготовки кадров в области информационной безопасности», в основе которой лежит подход «Перевернутого учебного плана» с ускоренной прикладной подготовкой студентов по образовательной программе высшего образования. На младших курсах приоритетной является прикладная подготовка студентов и развитие профессиональных компетенций обучающихся путем объединения их в студенческое конструкторское бюро «Киберхаб» для решения инженерных и проектных задач, в том числе в интересах индустриальных партнеров. На выходе из вуза они будут более востребованы на рынке труда – работодатели получат выпускников с подготовкой иного качества. Помимо этого, на ресурсах Полигона в настоящее время реализуются программы дополнительного профессионального образования в рамках программы софинансирования Удмуртской Республики.

Одним из направлений дальнейшего развития проекта «полигон для апробации и внедрения отечественного программного обеспечения» является создание центра реагирования на события ИБ и реализация менеджмента инцидентов ИБ. С этой целью в среде телекоммуникационной системы ИПСУБ реализуется сеть сенсоров,

позволяющих получать метаданные и копии трафика данных для последующей обработки и анализа. В состав созданного ЦОД вводится ПО, обеспечивающее контроль утечки данных (DLP) и управление событиями ИБ (SIEM), которые реализуют анализ трафика данных, а также сбор и анализ данных агентского мониторинга. Отдельным направлением развития является внедрение систем анализа сетевых потоков. Внедрение систем сбора и обработки данных позволит выполнять регистрацию событий ИБ, анализ инцидентов ИБ, реагирование на события ИБ и в конечном итоге формирование действующей политики информационной безопасности. Применение методов математического анализа к получаемым данным позволит выявлять аномальное поведение пользователей, процессов, протоколов на основе выбросов случайных процессов. Применение методов корреляционного анализа позволит выявлять источники аномального поведения, а методы системного анализа – выявлять степень влияния процессов на целевые показатели системы.

***Евсиков Кирилл Сергеевич**,*
к.ю.н., доцент, заведующий кафедрой
государственного и административного права
ФГБОУ ВО «Тульский государственный университет», г. Тула,
доцент кафедры информационного права и цифровых технологий
Московского государственного юридического университета
имени О.Е. Кутафина (МГЮА), г. Москва

КВАНТОВАЯ КРИПТОГРАФИЯ КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ

20 мая 2023 года Правительство Российской Федерации утвердило Концепцию технологического развития на период до 2030 года (далее – Концепция)[26]. Реализация Концепции направлена на развитие

[26] Об утверждении Концепции технологического развития на период до 2030 года : распоряжение Правительства РФ от 20.05.2023 № 1315-р // Собрание законодательства РФ. 29.05.2023. № 22, ст. 3964.

высокотехнологичных отраслей экономики Российской Федерации, что характеризует ее как отраслевой документ стратегического планирования Российской Федерации. Документ значительно обогатил язык науки информационного права, так как закрепил такие термины, как высокотехнологичная продукция, импортозамещение, компания-лидер, критические технологии, наилучшая доступная технология, право на риск, проекты-маяки, технологический суверенитет, экосистема технологического развития и другие. Как справедливо отмечала Г.Г. Камалова, понятийный аппарат является важнейшей составляющей для эффективного правового регулирования информации, информационных технологий и защиты информации[27].

Среди важных положений Концепции можно выделить закрепление перечня сквозных технологий. В документе отражено, что сквозные технологии – перспективные технологии межотраслевого значения, определяющие будущий облик экономики и отдельных отраслей в среднесрочной перспективе. К ним относятся технологии искусственного интеллекта, новых материалов, квантовых вычислений и коммуникаций, накопления энергии, систем связи, космических систем. В Концепции также указано, что Российская Федерация находится в первой десятке стран по патентной и публикационной активности в области квантовых технологий, которые в документе разделяются на два вида:

– квантовые вычисления;

– квантовые коммуникации.

Взаимозависимость этих сквозных технологий (технологических направлений) обусловлена тем, что развитие квантовых вычислений стимулирует поиск новых способов защиты данных, среди которых ведущее место занимают квантовые коммуникации.

Во многих зарубежных странах на нормативном уровне признаны риски дешифровки кодируемых сегодня данных квантовым

---

[27] *Камалова Г.Г.* Правовой режим информации ограниченного доступа: вопросы формирования понятийного аппарата // Вестник Удмуртского университета. Сер. «Экономика и право». 2016. Т. 26, № 4. С. 118-125.

компьютером. Эту проблему часто называют «квантовая угроза». В упрошенном виде ее можно представить, как создание квантового компьютера, способного взломать используемые сегодня криптографические алгоритмы[28]. Хотя значимый прогресс в данной сфере не достигнут, но уже созданы квантовые компьютеры малой мощности. Например, в 2019 году Google опубликовал результаты эксперимента Quantum Supremacy, в ходе которого квантовый процессор Sycamore выполнял вычисления за 200 секунд, что эквивалентно 10 000 лет работы обычного компьютера[29]. В 2021 году китайская группа ученых описали процессор Zuchongzhi, мощность которого в 2–3 раза выше, чем у Google[30]. Эти результаты позволили специалистам прогнозировать, что технология, способная взломать шифр Биткоина, может быть создана в 2027 году, а шифр RSA – в 2031 году[31].

Регулятор Великобритании (The National Cyber Security Centre – NCSC) в рекомендациях 2020 года прогнозирует увеличение мощности существующих квантовых компьютеров до критического для информационной безопасности уровня в 2030 году[32]. Французское агентство информационной безопасности (Agence nationale de la sécurité des systèmes d'information – ANSSI) в январе 2022 года опубликовало свою позицию по квантовой угрозе, где отметило, что существующие прототипы квантовых компьютеров в настоящее время не представляют угрозы для криптографии, но нельзя

---

[28] *Евсиков К.С.* Информационная безопасность цифрового государства в квантовую эпоху // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4. С. 46-58.

[29] *Arute, F., Arya, K., Babbush, R.* et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019).

[30] Strong Quantum Computational Advantage Using a Superconducting Quantum Processor // Yulin Wu et al. Physical Review Letters. American Physical Society. № 127. 2021. URL: https://physics.aps.org/featured-article-pdf/10.1103/ PhysRevLett.127.180501 (дата обращения: 10.06.2023).

[31] *Mosca M.* Cybersecurity in an Era with Quantum Computers: Will We Be Ready? // IEEE Security & Privacy, Vol. 16, № 5, 2018. P. 38-41.

[32] Quantum-safe cryptography (white paper) // URL: https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography (дата обращения: 10.06.2023).

исключать угрозу ретроактивных атак – «сохранить сейчас, расшифровать позже», что может иметь значение для безопасности секретной информации[33]. Следует учитывать, что большинство прогнозов ориентируются на открытые данные, а в условиях геополитического противостояния существует вероятность, что реальные успехи в построении работоспособного квантового вычислителя будут являться конфиденциальной информацией, и выявить этот момент возможно только после компрометации значительного массива данных[34].

Таким образом, прогнозы создания квантового компьютера разнятся, но все они сходятся в двух факторах:

– действующие шифры будут дешифрованы;

– быстрый переход на новые средства криптографии невозможен.

В октябре 2021 года Министерство внутренней безопасности США опубликовало Меморандум о подготовке к постквантовой криптографии, в котором отметило, что столкнулось с проблемами в области национальной безопасности, включая защиту данных критически важной инфраструктуры[35]. Причиной этого объявлена недостаточная подготовка к переходу на квантово-безопасную криптографию.

Важно отметить, что США проявляет повышенное внимание к разработкам в сфере квантовых технологий в других странах. Америка заключила множество соглашений о сотрудничестве в данной сфере (с Японией в 2019 году, с Австралией в 2021 году, с Великобританией в 2021 году, с Данией, Швейцарией, Канадой, Южной Кореей в 2022 году). Данные соглашения предусматривают

---

[33] ANSSI views on the post-quantum cryptography transition // URL: https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/ (дата обращения: 10.06.2023).

[34] *Добробаба М.Б., Чаннов С.Е., Минбалеев А.В.* Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4. С. 25-37.

[35] Memorandum on Preparing for Post-Quantum Cryptography // URL: https://www.dhs.gov/publication/ (дата обращения: 10.06.2023).

активный обмен информацией, что позволяет США оперативно оценивать уровень риска информационной безопасности и прогнозировать момент появления квантового компьютера.

В этой связи вызывает озабоченность Меморандум о национальной безопасности США 2022 года, который потребовал от АНБ обновить набор алгоритмов национальной безопасности, включив в него квантово-устойчивую криптографию. Согласно документу в течение 180 дней органы власти должны утвердить график перевода информационных систем на новый вид шифрования, стойкий к квантовым вычислениям[36]. Эти документы стали основой для других законопроектов, например, летом 2022 года в Конгресс внесен Закон о готовности к кибербезопасности квантовых вычислений. Данная проблема необоснованно игнорируется отечественной юридической наукой и правоприменительной практикой, хотя была неоднократно доказана важность правового обеспечения конфиденциальности информации в условиях развития информационного общества[37].

Сегодня существует несколько способов преодоления рисков квантовой угрозы. Самым эффективным является развитие технологий квантового распределения ключей. Лидером в данной сфере является Китай. Его успехи заставили специалистов во всем мире говорить о китайском квантовом чуде. Например, из трех тысяч патентов в области квантовой коммуникации более двух тысяч у КНР, около шестисот у США, около двухсот у Южной Кореи и около ста у Японии. Китай – единственная страна, обладающая действующей линией квантовой связи с сегментом земля-спутник. В 2016 году КНР запустила первый в мире спутник квантовой связи,

---

[36] Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems // URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/ (дата обращения: 10.06.2023).

[37] *Камалова Г.Г.* Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : автореф. дис. … д-ра юрид. наук / Институт государства и права РАН. Москва, 2020. 52 с.

а в 2021 году начала эксплуатацию самой длинной сети квантового распределения ключей – 4600 км. Сеть состоит из более тридцати доверенных узлов магистральной линии Пекин-Шанхай, протяженностью две тысячи километров[38].

Она объединяет несколько городских квантовых сетей, а доступ к линии квантовой связи получили более 150 пользователей, включая финансовые институты, энергетические компании, органы власти. Столь масштабные проекты сопровождались совершенствованием нормативной базы. В ходе этого процесса решались несколько задач:

– децентрализация регулирования криптографии;
– создание рынка криптографии, основанного на конкуренции;
– сокращение количества лицензий;
– упрощение доступа на рынок оборудования для криптографии.

Отечественное право также использует термин квантовое распределение ключей. В Указе Президента РФ от 06.03.2008 № 326 «О внесении изменений в Указ Президента Российской Федерации от 5 мая 2004 г. № 580[39] (документ утратил силу) технология отнесена к товарам ограниченным в обороте. В примечании к данному документу появилась ссылка – «Квантовая криптография также известна как квантовое распределение ключей (КРК)». В действующем сегодня Постановлении Правительства РФ от 19.07.2022 № 1299 квантовая криптография – совокупность технических приемов по созданию совместно используемого ключа для защиты информации путем измерения квантово-механических свойств

[38] *Chen, YA., Zhang, Q., Chen, TY*. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. № 589, 2021. P. 214–219. URL: https://doi.org/10.1038/s41586-020-03093-8.

[39] О внесении изменений в Указ Президента Российской Федерации от 5 мая 2004 г. № 580 «Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль» и в Список, утвержденный этим Указом : Указ Президента РФ от 06.03.2008 № 326 // Собрание законодательства РФ. 10.03.2008. № 10 (2 ч.), ст. 912.

физической системы (включая те физические свойства, которые ясно определены квантовой оптикой, квантовой теорией поля или квантовой электродинамикой)[40]. Этим же документом определены такие термины, как: постквантовый, квантово-безопасный или квантово-устойчивый алгоритм защиты информации. К таковым документ отнес:

– выявление аномалий с самым коротким или самым близким одномерным массивом данных, состоящим из однотипных элементов, связанных с алгебраическими решетками CRYSTALS;

– поиск изогений между суперсингулярными эллиптическими кривыми (например суперсингулярная изогения обмена ключами);

– дешифрование случайных кодов (например алгоритмы McEliece, Niederreiter).

В Дорожной карте развития «сквозной» цифровой технологии «Квантовые технологии» указано, что «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». В проекте национального стандарта «Квантовые коммуникации. Термины и определения» (шифр 1.11.194-1.106.22) под квантовой коммуникацией предлагается понимать передачу информации посредством прямой передачи квантовых состояний или посредством квантовой запутанности (документ находится в стадии согласования)[41].

Анализ существующих нормативных правовых актов, нормативно-технических актов и актов стратегического характера позво-

---

[40] Об утверждении списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль : Постановление Правительства РФ от 19.07.2022 № 1299 // Собрание законодательства РФ. 25.07.2022. № 30, ст. 5630.

[41] URL: http://tc194.ru/qua№tum_public (дата обращения: 10.06.2023).

ляет говорить, что квантовое распределение ключей относиться в Российской Федерации к технологиям квантовой коммуникации[42]. Кроме указанных концептов органы публичной власти используют дефиниции:

– квантовая связь;

– квантовая криптография;

– постквантовый алгоритм защиты информации (квантово-безопасный, квантово-устойчивый).

Системное толкование данных правовых категорий позволило предложить следующую взаимосвязанную систему терминов (рис. 1).

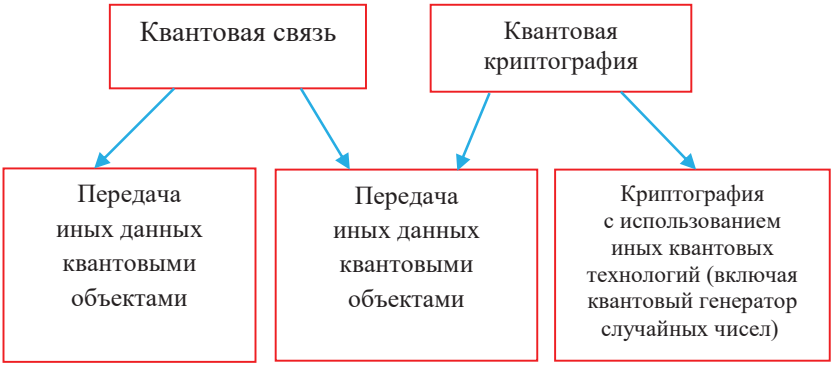


Рис. 1. Структура квантовой коммуникации

В рамках данной системы терминов предлагается рассматривать квантовую коммуникацию как совокупность общественных отношений, возникающих при создании и использовании оборудования для квантовой связи и квантовой криптографии, а также при оказании услуг в данной сфере. Как видно из дефиниции, нами предлагается разделять квантовую коммуникацию на квантовую связь и квантовую криптографию[43]. При этом под квантовой связью

---

[42] *Холодная Е.В.* Квантовые технологии как объект права // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4. С. 38-45.

[43] *Евсиков К.С.* Правовое регулирование квантового распределения ключей // Вестник Московского университета. Серия 26. Государственный аудит. 2023. № 2. С. 86-104.

целесообразно понимать технологии, оборот которых регулируется законодательством о связи, а под квантовой криптографией – технологии, оборот которых регулируется законодательством об информационной безопасности.

Библиографический список

1. Добробаба М.Б., Чаннов С.Е., Минбалеев А.В. Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 4. – С. 25-37.

2. Евсиков К.С. Информационная безопасность цифрового государства в квантовую эпоху // Вестник Университета им. О.Е. Кутафина (МГЮА). – 2022. – № 4. – С. 46-58.

3. Евсиков К.С. Правовое регулирование квантового распределения ключей // Вестник Московского университета. Сер. 26. Государственный аудит. – 2023. – № 2. – С. 86-104.

4. Информационно-технологическое обеспечение юридической деятельности (LegalTech) : учебник / коллектив авторов ; под ред. д.ю.н., доц. А.В. Минбалеева. – М. : Проспект, 2022. – 368 с.

5. Камалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : автореф. дис. … д-ра юрид. наук / Институт государства и права РАН. – Москва, 2020. – 52 с.

6. Камалова Г.Г. Правовой режим информации ограниченного доступа: вопросы формирования понятийного аппарата // Вестник Удмуртского университета. Сер. «Экономика и право». – 2016. – Т. 26, № 4. – С. 118-125.

7. Минбалеев А.В., Берестнев М.А., Евсиков К.С. Обеспечение информационной безопасности оборудования добывающей промышленности в квантовую эпоху // Известия Тульского государственного университета. Науки о земле. – 2023. – № 1. – С. 509-525.

8. Новые горизонты развития системы информационного права в условиях цифровой трансформации / под ред. Т.А. Поляковой, А.А. Минбалеева, В.Б. Наумова, А.А. Смирнова [и др.]. – М. : Изд-во: «Институт Государства и права РАН», 2022. – 368 с.

9. Полякова Т.А., Минбалеев А.В., Наумов В.Б. Правовое регулирование квантовых коммуникаций в России и в мире // Государство и право – 2022. – Номер 5. – С. 104-114.

10. Холодная Е.В. Квантовые технологии как объект права // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 4. – С. 38-45.

Любавский Алексей Юрьевич,
к.т.н., доцент кафедры информационных технологий и организации расследования киберпреступлений ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации», г. Москва

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ

На сегодняшний день развитие инфокоммуникационных технологий внесло свои коррективы в такие аспекты жизни человечества, как частная жизнь, личное пространство. В настоящее время многие процессы переходят в цифровой мир (удаленная работа, получение справок в государственных учреждениях, торговые интернет-площадки). Для этого достаточно иметь персональный компьютер или любое мобильное устройство. Наряду с неоспоримыми преимуществами, в сети Интернет циркулирует огромный объем персональных данных, добровольно предоставляемых пользователями на различных ресурсах[44]. Не следует оставлять без внимания развитие такого направления «добывания» конфиденциальной информации из открытых источников – OSINT[45], включающем

[44] *Гнедкова А.В.* Особенности распространения персональных данных в последней редакции законодательства о персональных данных // Научно-методическое обеспечение оценки качества образования 1 (15). Челябинский институт развития образования. 2022. С. 49-52.

[45] OSINT (Open – Source Intelligence) – разведка по открытым источникам.

в себя широкий спектр легальных, бесплатных ресурсов и приложений, позволяющим из разрозненных частей конфиденциальной информации собрать достаточно обширный перечень персональных данных. Законодательство в области обеспечения защиты персональных данных[46] позволяет гражданам отозвать свои персональные данные. Однако достоверной и подтвержденной информации о том, что утечка тем или иным оператором персональных данных не была допущена, нет. О чем свидетельствует официальный отчет экспертно-аналитического центра ГК InfoWatch, однозначно подтверждающий факт большого объема утечек персональных данных[47].

Законодательство Российской Федерации регламентирует обязанности операторов персональных данных по обеспечению мер по защите персональных данных[48]. В 2023 году Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации передало на рассмотрение комитета по информатике Государственной Думы два законопроекта, ужесточающих порядок работы с персональными данными россиян. Первый законопроект вводит оборотные штрафы для компаний, допустивших утечку информации. Второй – изменение в Уголовный Кодекс Российской Федерации, который позволит привлекать к уголовной ответственности лиц, осуществляющих кражу и продажу персональных данных; речь идет о ст. 272, 274[49] УК РФ. Вышеприведенные факты, безусловно, свидетельствуют о том, что введение оборотных штрафов для компаний, уголовной ответственности за кражу и продажу

---

[46] Пункт 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) // СПС «КонсультантПлюс».

[47] URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf

[48] *Исаева Т.Е.* Нормативное и методическое обеспечение безопасности персональных данных в Российской Федерации // Безопасность информационного пространства. Курганский гос. ун-т, 2016. С. 25-28.

[49] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.04.2023) в ред. Федерального закона от 07.12.2011 № 420-ФЗ // СПС «КонсультантПлюс».

персональных данных[50] в перспективе снизит количество утечек персональных данных.

Наряду с организационными и техническими мерами по защите персональных данных, в сети Интернет (информационные системы персональных данных[51]) существуют, на мой взгляд, противоречия с законодательством о персональных данных.

В ходе исследования мною были изучены судебные акты Арбитражного суда Российской Федерации[52]. Изучив разделы вышеуказанного ресурса, можно сделать вывод, что каждый гражданин Российской Федерации имеет доступ к персональным данным вступивших в процедуру признания банкротства. Наряду с персональными данными физических лиц, в открытом доступе находится конфиденциальная информация арбитражных управляющих[53].

Более того, если обратиться к материалам, опубликованным в Едином федеральном реестре сведений о банкротстве[54], а также на Интернет-сайте издания «Коммерсантъ»[55], каждый пользователь может получить аналогичную конфиденциальную информацию граждан Российской Федерации.

На вышеперечисленных ресурсах в открытом доступе размещена следующая информация: фамилия, имя, отчество, индивидуальный налоговый номер (ИНН), страховой номер индивидуального лицевого счета (СНИЛС), дата и место рождения и адрес регистрации по месту жительства, при отсутствии такового – адрес фактического пребывания. Более того, аналогичная информация публикуется в открытом доступе и в отношении арбитражного управляющего.

---

[50] URL: https://www.rbc.ru/politics/17/03/2023/6413ec6c9a79474989a45f12

[51] Статья 3 Федерального закона от 27.07.2006 № 152-ФЗ // СПС «КонсультантПлюс».

[52] URL:https://kad.arbitr.ru

[53] Статья 28, 213.7. Федеральный закон от 26.10.2002 № 127-ФЗ (ред. от 28.12.2022) «О несостоятельности (банкротстве)» (с изм. и доп., вступ. в силу с 19.04.2023) // СПС «КонсультантПлюс».

[54] URL:https://old.bankrot.fedresurs.ru/Default.aspx

[55] URL:https://bankruptcy.kommersant.ru

В настоящее время отсутствует норма законодательства, обязывающая арбитражные суды удалять персональные данные должников и арбитражных управляющих. Суды и арбитражные управляющие руководствуются п. 2 ст. 213.7 ФЗ о банкротстве[56]. Настоящей статьей регламентируются положения о публикации информации должника. Так, установлено, что информация о банкротстве подлежит публикации в ЕФРСБ.

Следует отметить, что приведенный факт не нарушает законодательство в области персональных данных[57].

В свою очередь, закон о банкротстве является специальным законом, и, соответственно, приоритет данного закона выше ФЗ «О защите персональных данных». Исходя из данного факта, следует, что арбитражные управляющие и суды не нарушают законодательство в области защиты персональных данных. Также отметим, что согласие на обработку персональных данных не требуется:

во-первых, ст. 28 ФЗ о банкротстве обязывает размещение персональных данных банкрота и арбитражного управляющего на вышеуказанных ресурсах. Кроме этого, в абз. 2 п. 2 настоящей статьи однозначно указано, что сведения (по факту персональные данные) являются общедоступными, а также, в соответствии с абз. 3 п. 2 настоящей статьи, подлежат размещению в сети Интернет и могут быть использованы без ограничений, в том числе путем дальнейшей их передачи;

во-вторых, ст. 126, 127 АПК РФ[58] в своем содержании регламентируют обязанность должника и арбитражного управляющего предоставить персональные данные суду. Вместе с тем непредставление вышеуказанных сведений арбитражным управляющим повлечет ответственность управляющего в соответствии

---

[56] Федеральный закон от 26.10.2002 № 127-ФЗ // СПС «КонсультантПлюс».

[57] Федеральный закон от 27.07.2006 № 152-ФЗ // СПС «КонсультантПлюс».

[58] Арбитражный процессуальный кодекс Российской федерации от 24.07.2022 (в ред. от 18.03.2023) // СПС «КонсультантПлюс».

с пп. 3 и 3.1 ст. 14.13[59] КОАП РФ, которые предусматривают ответственность от штрафа до дисквалификации.

Также стоит отметить тот факт, что законодательством не предусмотрены процедура и механизм удаления персональных данных должника и арбитражного управляющего с ресурсов, приведенных выше. Наряду с отсутствием закрепленной законодательством процедуры их удаления из сети Интернет не предусмотрен процессуальный механизм, который обязывает Арбитражные суды публиковать документы о банкротстве с минимизацией количества идентификаторов субъектов персональных данных.

Таким образом, существует неопровержимый факт того, что, несмотря на инициативы государства в области защиты персональных данных, в открытом доступе имеется большой сегмент персональных данных. Безусловно, население, прошедшее или проходящее процедуру банкротства, арбитражные управляющие не составляют 100 % населения, но вместе с тем, опираясь на официально опубликованные сведения[60], в нашей стране огромный процент населения, которые уже взяли и выплачивают потребительские, ипотечные, авто- кредиты. Целью данного исследования не является анализ экономической ситуации в стране, но не стоит исключать факт того, что ряд граждан по различному ряду причин могут вступить в процедуру банкротства.

Рассмотрим также риски опубликования персональных данных арбитражных управляющих. В вышеперечисленных ресурсах фигурирует также информация о получении вознаграждения. И если вознаграждение за ведение дел о банкротстве составляет единовременную выплату в размере 25 тысяч рублей, то при ведении дел о банкротстве юридических лиц вознаграждение составляет 30 тысяч рублей в месяц, либо процентное вознаграждение может

---

[59] Кодекс об административных правонарушениях от 30.12.2001 № 195-ФЗ (в ред. от 28.04.2023) // СПС «КонсультантПлюс».

[60] URL: https://cbr.ru/Collection/Collection/File/43421/inf-material_bki_2022fh.pdf

быть зафиксировано в акте Арбитражного суда, которые публикуются, в свою очередь, на сайте указанного суда в открытом доступе. Кроме этого, публикуются и реквизиты арбитражных управляющих, а многие участники ЕФРСБ зачастую в публикациях указывают свой домашний адрес. По сути, любой человек, а в частности злоумышленник, имеет техническую возможность выявить судебные акты в совокупности с суммой вознаграждения, а на сайте ЕФРСБ – установить домашний адрес и совершить противоправные действия в отношении гражданина. Наряду с материальной составляющей, род деятельности арбитражного управляющего также связан с таким риском для жизни и здоровья, как негативная реакция на принятые им решения в ходе процедуры банкротства участников процесса.

Таким образом, актуальна проблема защиты персональных данных участников процедуры банкротства. С одной стороны, участники процедуры, в соответствии с требованиями действующего законодательства, обязаны указывать свои персональные данные в публикациях и судебных актах, а с другой стороны, осуществляется распространение персональных данных.

Анализ вышеприведенных материалов показывает, что для решения сложившейся проблемы необходимо скорректировать соответствующие статьи закона о банкротстве путем внесения уточнений в части состава конфиденциальной информации, подлежащей опубликованию в сети Интернет. Также целесообразно внести уточнения в ст. 15 Федерального закона, регламентирующего доступ к информации о деятельности судов Российской Федерации[61].

Альтернативным путем решения проблематики распространения персональных данных участников процесса судебного банкротства является предоставление доступа к конфиденциальной информации посредством процедуры аутентификации, позволяющей

[61] Об обеспечении доступа к информации о деятельности судов в Российской Федерации : Федеральный закон от 22.12.2008 № 262-ФЗ (ред. от 14.07.2022) (с изм. и доп., вступ. в силу с 01.01.2023) // СПС «КонсультантПлюс».

однозначно идентифицировать физическое лицо. В Российской Федерации успешно внедрены и функционируют подобные механизмы: вход в личный кабинет различных интернет-ресурсов посредством таких средств аутентификации, как вход через личный кабинет «Портала государственных услуг», «СБЕР-ID». Подобный механизм доступа к сегментам интернет-ресурсов не требует уточнения действующих нормативных актов в части определения круга лиц, имеющих доступ к вышеприведенной информации, и одновременно осуществлять контроль за персональными данными, циркулиру-ющими в интернет-ресурсах, на которые в соответствии с настоящим законодательством субъекты персональных данных обязаны предоставлять сведения конфиденциального характера для размещения.

Библиографический список

1. Гнедкова А.В. Особенности распространения персональных данных в последней редакции законодательства о персональных данных. – Челябинск., 2022. – С. 49-52.

2. Исаева Т.Е. Нормативное и методическое обеспечение безопасности персональных данных в Российской Федерации. – Курган., 2016. – С. 25-28.

Химченко Алексей Игоревич,
к.ю.н., старший преподаватель кафедры
информационного права и цифровых технологий
«Московский государственный юридический университет
им. О.Е. Кутафина», г. Москва

НЕКОТОРЫЕ ВОПРОСЫ ФОРМИРОВАНИЯ БЕЗОПАСНОЙ ЦИФРОВОЙ СРЕДЫ

Технологии, традиционно выступая драйвером развития целых сфер экономики, подчас становятся инструментом и способом достижения целей в обострившейся конкурентной борьбе, подвергаясь перманентному негативному и деструктивному воздействию.

В то же время в процессе стремительного построения цифрового мира, в основе которого была заложена максимальная экономическая эффективность и скорость развития, масштабируемость и универсальность продуктов, достижение целевых показателей, базовые принципы информационной безопасности не были приоритетом.

Распространение дистанционной модели работы, способствовавшее расширению периметров корпоративных сетей и росту разнородности форматов данных, увеличение доли дистанционных сервисов и услуг в традиционном деловом обороте, усложнение архитектуры и масштабирование, расширение контура в процессе развития экосистем, а также современная международная повестка поднимают все новые вопросы обеспечения безопасности цифровой среды.

В ежегодном прогнозе развития киберугроз и средств защиты информации[62] отраслевые эксперты готовились столкнуться с традиционными для отрасли проблемами, не ожидая кардинальных изменений, поскольку пространства внутренних и внешних угроз были известны профессиональному сообществу. Среди них назывались проблемы, связанные с размытием периметров; тематика

[62] Прогноз развития киберугроз и средств защиты информации 2022. URL: https://www.anti-malware.ru/analytics/2022-Cyber-Threats-and-Information-Security-Forecast (дата обращения: 01.09.2022).

аутентификации и управления доступом, нулевого «доверия»; безопасной разработки и встроенной защиты ИТ-систем, уязвимости третьестороннего ПО и опенсорс-проектов; шифровальщики и вымогатели, сетевое мошенничество, фальшивые платежные системы и другие характерные современному технологическому веку риски.

В то же время происходящие перемены в международной обстановке предопределили и изменение структуры информационных угроз, часть из которых имела целью нанесение деструктивного воздействия, другие связаны с влиянием ограничительной политики (последствия прекращения работы отдельных производителей, отказ в предоставлении поддержки и ключей, удаление продуктов из магазинов приложений).

Рост напряженности в сфере информационной безопасности отмечается на различных уровнях от профильных ведомств[63] до Председателя Правительства РФ[64], при этом необходимость формирования устойчивых механизмов обеспечения информационной безопасности обсуждалась на заседании Совбеза России[65]. Кроме того, специфика и особенности угроз инфраструктуре российских мобильных приложений[66], корпоративным сетям, системам электронного документооборота[67], игровому сегменту российского IT-рынка[68], системе здравоохранения[69] регулярно рассматривается отраслевыми экспертами.

---

[63] URL: https://rkn.gov.ru/news/rsoc/news74584.htm (дата обращения: 01.05.2023).

[64] Видеообращение М. Мишустина к участникам международного онлайн-тренинга по кибербезопасности. URL: http://government.ru/news/39983 (дата обращения: 12.12.2021).

[65] URL: http://www.scrf.gov.ru/news/allnews/3241 (дата обращения: 01.09.2022).

[66] URL: https://www.kommersant.ru/doc/5481646 (дата обращения: 12.05.2023).

[67] URL: https://www.kommersant.ru/doc/5538103 (дата обращения: 01.08.2022).

[68] URL: https://www.kommersant.ru/doc/5490901 (дата обращения: 01.10.2022).

[69] URL: https://www.kommersant.ru/doc/5692712 (дата обращения: 01.12.2022).

Кроме того, исследования показывают, что на текущее состояние безопасности цифровой среды влияет широкий ряд факторов, в том числе и необходимость совершенствования организационно-правовых аспектов деятельности в рассматриваемой сфере, среди которых Т.А. Полякова отмечает нерешенность многих информационно-правовых вопросов в национальной системе права[70].

Так, действующее законодательство не содержит отдельного федерального закона, регламентирующего обеспечение информационной безопасности, а специализированные нормы разбросаны по большому количеству отдельных нормативных правовых актов[71].

Кроме того, отмечается и отсутствие стратегического регулирования отрасли, системы правовых средств обеспечения функционирования института кибербезопасности, значительное отставание правовых средств обеспечения информационной безопасности от технических, программно-аппаратных и иных[72].

В настоящий момент вопросы безопасности цифровой среды находят отражение во многих ключевых стратегических документах.

Так, обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации, Доктриной информационной безопасности[73] отнесено к националь-

---

[70] Четвертые Бачиловские чтения : материалы Междунар. науч.-практ. конф. / Ин-т гос-ва и права РАН ; отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М.; Саратов : Амирит, 2022. С 39.

[71] *Полякова Т.А., Камалова Г.Г.* Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов безопасности (к 30-летию принятия Закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. 2022. № 2 (68). С. 115.

[72] Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе : монография / Ин-т гос-ва и права РАН ; под общ. ред. д.ю.н., проф. *Т.А. Поляковой*. М.; Саратов : Амирит, 2022. С. 173.

[73] Утверждена Указом Президента РФ от 05.12.2016 № 646 // СЗ РФ. 12.12.2016. № 50, ст. 7074.

ным интересам в информационной сфере, а развитие информационной и коммуникационной инфраструктуры Российской Федерации, в соответствии со Стратегией развития информационного общества в Российской Федерации, признается одним из приоритетов при обеспечении национальных интересов при развитии информационного общества.

При этом в Доктрине информационной безопасности отмечается постоянное повышение сложности, увеличение масштабов и рост масштабов компьютерной преступности, увеличение числа преступлений, скоординированности компьютерных атак на объекты критической информационной инфраструктуры, что подчеркивают критические риски информационной среды.

Ключевыми при рассмотрении вопросов безопасности цифровой среды являются вопросы безопасности и достоверности информации, реализация которых представляет особенный интерес.

Так, положениями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[74] реализован комплекс мер, регламентирующих порядок распространения информации и направленных на повышение достоверности сведений.

Правовой режим распространения информации в сети Интернет предусматривает исключение возможности ущемления личных неимущественных прав граждан посредством установления запрета для установленных субъектов взаимодействия распространения определенных категорий сведений.

На некоторых из них (новостной агрегатор) возложена обязанность проверять достоверность распространяемых общественно значимых сведений до их распространения, а также не допускать сокрытия или фальсификации сведений, распространения недостоверной информации. Владельцу социальной сети предписано осуществлять мониторинг в целях выявления информации с последующим принятием мер по ограничению доступа к установленной информации.

[74] СЗ РФ. 31.07.2006. № 31 (1 ч.), ст. 3448.

Одним из ключевых вопросов, формирующих безопасность цифровой среды, является обеспечение достоверности и неизменности электронных документов, что находит отражение в Стратегии развития информационного общества в Российской Федерации посредством отнесения комплекса вопросов по продвижению проектов по внедрению электронного документооборота в организациях к основным задачам применения информационных технологий.

Кроме того, Доктриной информационной безопасности Российской Федерации к направлениям реализации национальных интересов в информационной сфере отнесено формирование безопасной среды оборота достоверной информации.

Ключевым при реализации достоверности информации в цифровой среде является механизм электронной подписи, предусмотренный нормами Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»[75] и предназначенный для определения подписанта информации при совершении юридически значимых действий.

Важным в вопросе снижения вызовов и угроз устойчивости цифровой среды является достижение информационного суверенитета[76], формирование среды доверия в информационном пространстве[77]. Большое значение приобретают меры по повышению технологической независимости, что находит свое отражение в документах стратегического планирования и отраслевых концептуальных документах.

Так, в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента РФ от 09.05.2017 № 203[78], содержится положение о необходимости отстаивать суверенное право государства определять технологическую политику в национальном сегменте сети Интернет.

---

[75] СЗ РФ. 11.04.2011. № 15, ст. 2036.

[76] *Виноградова Е.В., Полякова Т.А.* О месте информационного суверенитета в конституционно-правовом пространстве современной России // Журнал «Правовое государство: теория и практика». 2021. № 1 (63). С. 32-50.

[77] *Химченко А.И.* О взаимосвязи вопросов обеспечения информационного суверенитета Российской Федерации и формирования цифровой среды доверия // Вестник МГЮА. 2022. № 4 (92). С. 90.

[78] СЗ РФ. 15.05.2017. № 20, ст. 2901.

Банк России в «Основных направлениях развития финансового рынка Российской Федерации на 2023 год и период 2024 и 2025 годов» обеспечение технологической независимости и информационной безопасности выделяет в качестве отдельной задачи и планирует соответствующие мероприятия по его достижению[79].

Подходы к повышению технологической независимости в отечественном законодательстве можно условно классифицировать по территориальному и национальному принципам применения соответствующих норм.

К *территориальному,* в основе которого реализована «привязка» соответствующих информационных пространств к находящейся на территории конкретного государства информационной инфраструктуре, можно отнести Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[80], предусматривающий обязанность оператора обеспечить работу с персональными данными граждан на территории Российской Федерации.

Положениями Федерального закона от 07.07.2003 № 126-ФЗ «О связи»[81] предусмотрена обязанность оператора связи, оказывающего услуги по предоставлению доступа к сети Интернет, обеспечивать установку технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования российского сегмента сети Интернет и сети связи общего пользования. При этом собственниками или иными владельцами линий связи, пересекающих границу Российской Федерации, могут являться только российские юридические лица.

В соответствии со ст. 14 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[82] организация выпуска цифровой валюты в Российской Федерации осуществляется с использованием объектов

[79] Вестник Банка России. 29.12.2022. № 63.
[80] СЗ РФ. 31.07.2006. № 31 (1 ч.), ст. 3451.
[81] СЗ РФ. 14.07.2003. № 28, ст. 2895.
[82] СЗ РФ. 03.08.2020. № 31 (часть I), ст. 5018.

российской информационной инфраструктуры, размещенных на территории Российской Федерации.

Указанные нормы, способствуя повышению устойчивости и безопасности цифровой среды, направлены на исключение возможности деструктивного воздействия на ее объекты извне.

В основе *национального* – можно выделить принцип использования отечественных решений в информационной инфраструктуре.

Так, согласно Указу Президента от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ»[83] запрещена закупка зарубежного программного обеспечения для использования на значимых объектах критической информационной инфраструктуры, а с 1 января 2025 года – использование зарубежного программного обеспечения на таких объектах.

Постановлением Правительства РФ от 16.11.2015 № 1236[84] устанавливается запрет на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд.

В связи с необходимостью предупреждения угроз, вызванных досрочным отзывом иностранных сертификатов безопасности у сайтов российского сегмента сети Интернет, законопроект № 244043-8 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»[85] направлен на создание информационной системы национального удостоверяющего центра (НУЦ) по обеспечению специальными сертификатами безопасности и реализации защищенного взаимодействия с использованием российских криптографических алгоритмов (ГОСТ TLS) пользователей с государственными информационными ресурсами.

---

[83] СЗ РФ. 04.04.2022. № 14, ст. 2242.

[84] СЗ РФ. 23.11.2015. № 47, ст. 6600.

[85] О внесении изменений в Федеральный закон «Об информации, информационных технологиях о защите информации» : паспорт проекта Федерального закона № 244043-8.

В указанном контексте можно отметить и изменение требований к защите информации, содержащейся в государственных информационных системах, поскольку в соответствии с Приказом ФСБ России от 24.10.2022 № 524 с 23.11.2023 для обеспечения защиты информации должны использоваться только СКЗИ, сертифицированные ФСБ России.

В рамках повышения безопасности цифровой среды и повышения технологической независимости отдельное внимание уделяется формированию и экономических условий разработки и производства отечественной элементной базы, системного программного обеспечения, а также средств и систем защиты информации.

В связи с чем необходимо отметить комплекс мер, определенных Указом Президента РФ от 02.03.2022 № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации»[86], а также мер, предпринимаемых Правительством РФ (Постановление Правительства РФ от 22.07.2022 № 1310 «Об утверждении перечня электронной (радиоэлектронной) продукции для целей применения пониженных налоговых ставок по налогу на прибыль организаций и тарифов страховых взносов»[87]; Постановление Правительства РФ от 22.07.2022 № 1311 «Об утверждении перечня материалов и технологий для производства электронной компонентной базы (электронных модулей) для целей применения пониженных налоговых ставок по налогу на прибыль организаций и тарифов страховых взносов»[88]).

Перспективы развития. В завершении стоит отметить, что, оценивая отечественную отрасль информационной безопасности, эксперты положительно оценивают ее перспективы. Так, согласно прогнозу развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы, выполненному фондом «Центр стратегических разработок» (ЦСР)[89], отечественный рынок ИБ решений

[86] СЗ РФ. 07.03.2022. № 10, ст. 1468.

[87] СЗ РФ. 08.08.2022. № 32, ст. 5821.

[88] СЗ РФ. 08.08.2022. № 32, ст. 5822.

[89] URL: https://www.csr.ru/upload/iblock/13f/ufleu9rg5zc3ldu66srqt3a89j0mrve5.pdf (дата обращения: 01.09.2022).

ожидает кратный рост с 185,9 млрд руб. до 469 млрд руб. При этом прогнозируется использование бюджетов, выделяемых на средства защиты информации преимущественно на отечественные решения с потенциалом роста этой части рынка с 113 млрд руб. в 2021 году до 446 млрд руб. в 2026 году (в 4 раза).

К перспективным технологическим проектам в рассматриваемой сфере следует отнести планируемое создание Главным радиочастотным центром (ГРЧЦ) национальной системы защиты от DDoS-атак, а также достижение полного покрытия российского сегмента сети связи общего пользования техническими средствами противодействия угрозам[90].

Библиографический список

1. Четвертые Бачиловские чтения : материалы Междунар. науч.-практ. конф. / Ин-т гос-ва и права РАН ; отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. – М.; Саратов : Амирит, 2022. – 568 с.

2. Полякова Т.А., Камалова Г.Г. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов безопасности (к 30-летию принятия Закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. – 2022. – № 2 (68). – С. 112-122.

3. Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе : монография / Ин-т гос-ва и права РАН ; под общ. ред. д.ю.н., проф. Т.А. Поляковой. – М.; Саратов : Амирит, 2022. – 332 с.

4. Виноградова Е.В., Полякова Т.А. О месте информационного суверенитета в конституционно-правовом пространстве современной России // Журнал «Правовое государство: теория и практика». – 2021. – № 1 (63). – С. 32-50.

[90] URL: https://rkn.gov.ru/news/rsoc/news74584.htm (дата обращения: 01.05.2023).

5. Химченко А.И. О взаимосвязи вопросов обеспечения информационного суверенитета Российской Федерации и формирования цифровой среды доверия // Вестник МГЮА. – 2022. – № 4 (92). – С. 83-91.

Ахатова Алия Махмутовна,
Юридическая клиника Института права,
социального управления и безопасности ФГБОУ ВО «УдГУ».
Зварыгин Валерий Евгеньевич,
заведующий кафедрой уголовного права
и криминологии, к.ю.н., доцент ФГБОУ ВО «Удмуртский
государственный университет», г. Ижевск

К ВОПРОСУ ОБ ОПРЕДЕЛЕНИИ ПОНЯТИЯ «КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ» ПО УГОЛОВНОМУ ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ

Определение понятия «охраняемая законом компьютерная информация» является одним из наиболее сложных и противоречивых в доктрине уголовного права и правоприменительной практике. В силу неоднозначности юридико-технического характера исследуемого вопроса ученые-правоведы не придерживаются определенной позиции относительно содержания и сущности рассматриваемого понятия.

Согласно толковому словарю русского языка С.И. Ожегова «информация» – это сведения об окружающем мире и протекающих в нем процессах, воспринимаемых человеком или специальным устройством[91]. Согласно толковому словарю Д.Н. Ушакова под «информацией» необходимо понимать сообщения, осведомляющие о положении дел или о чьей-нибудь деятельности, сведения о чем-нибудь[92].

[91] *Ожегов С.И.* Словарь русского языка. URL: http://slovarozhegova.ru/
[92] *Ушаков Д.Н.* Толковый словрь Ушакова. URL: https://lexicography.online/

В уголовном законодательстве понятия информация, данные, сведения используются как эквивалентные.

Под информацией в соответствии со ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информатизации и защите информации» понимают сведения (сообщения, данные) независимо от формы представления[93].

«ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» имеет аналогичное определение понятия информации[94].

Согласно теории коммуникации в процессе обмена информацией принято выделять 4 базовых элемента, которые непосредственно связаны между собой: 1) отправитель (источник, коммуникатор); 2) сообщение; 3) канал; 4) получатель. При этом информация становится таковой только после принятия сообщения или данных (в виде набора символов, изображения, цифровых данных, таблиц и т.д.). получателем и его осмысления[95].

Понятие «компьютерной информации» дается в Соглашении о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации. Согласно п. «б» ст. 1 «компьютерная информация» – это информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи[96].

---

[93] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) (с изм. и доп., вступ. в силу с 01.03.2023) // СПС «КонсультантПлюс».

[94] ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст) // СПС «КонсультантПлюс».

[95] Основы теории коммуникации : учебник и практикум для вузов / Т. Д. Венедиктова [и др.] ; под ред. Т. Д. Венедиктовой, Д. Б. Гудкова. Москва : Издательство Юрайт, 2023 // Образовательная платформа Юрайт. URL: https://urait.ru/bcode/511855. С. 35.

[96] Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. // СПС «КонсультантПлюс».

Таким образом, региональный международный документ создал определенный базис для формирования национального законодательства.

Следует заметить, что в ранее действовавшей норме УК РФ в п. 1 Примечания к ст. 272 УК РФ было указано, что «компьютерная информация» – это информация на машинном носителе, в ЭВМ, системе ЭВМ или их сети[97]. Таким образом, раннее компьютерная информация находилась в неразрывной связи с машинным носителем, что представлялось неточным и не соответствующим требованиям юридической техники[98].

Согласно действующей редакции УК РФ в п. 1 Примечания к ст. 272 УК РФ «компьютерная информация» понимается как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[99].

Согласно п. 2 Постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет (далее – ППВС № 37), такие сведения могут находиться в запоминающем устройстве ЭВМ и в других компьютерных устройствах либо на любых внешних электронных носителях (дисках, в том числе жестких дисках-накопителях, флеш-картах и т.п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи.

Тем не менее употребление технических терминов в Особенной части УК РФ затрудняет применять такой термин, как «электрический сигнал». В заключении Комитета Государственной Думы

---

[97] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.11.2011) // СПС «КонсультантПлюс».

[98] *Бегишев И.Р.* Понятие и виды преступлений в сфере обращения цифровой информации : дис. ... канд. юрид. наук. Казань, 2017. С. 9.

[99] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.04.2023) // СПС «КонсультантПлюс».

по информационной политике, информационным технологиям и связи от 05.07.2011 «На проект Федерального закона № 559740-5 «О внесении изменений в УК РФ и отдельные акты РФ» было отмечено, что в предлагаемой дефиниции неясен смысл термина «электрические сигналы», и представляется необходимым уточнить данную формулировку[100].

Термин «сигнал» от лат. – signum (знак) и определяется в словаре русского языка С.И. Ожегова как «условный знак для передачи на расстояние сведений, сообщений»[101]. В теории связи под сигналом понимается физический процесс (электрический ток или радиоволны), способные распространяться в пространстве и нести в себе информацию[102].

Тем не менее законодатель, указывая, что информация может быть передана с помощью электрических сигналов, а также иным способом. Так, носители информации могут быть электромагнитными, оптическими (телеграмма, фотография, телевидение), звуковыми (речь, музыка), что не тождественно электрическим сигналам, в виде объективной формы записи цифрового машинного кода в оперативной памяти ЭВМ[103].

Появляются технологии, где устройства перестают быть электронными, а само понятие «электрический сигнал» устаревает. Применяются биотехнологии, лазерные технологии, нанотехнологии и др., с помощью которых возможно осуществление противоправных деяний[104].

---

[100] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (в части совершенствования законодательства Российской Федерации) : паспорт проекта Федерального закона № 559740-5 // СПС «КонсультантПлюс».

[101] *Ожегов С.И.* Словарь русского языка. URL: http://slovarozhegova.ru/

[102] Основы теории коммуникации : учебник и практикум для вузов / Т. Д. Венедиктова [и др.]. М., 2023. С. 26.

[103] *Верещагина А.В.* К вопросу о предмете неправомерного доступа к компьютерной информации // Территория новых возможностей. 2020. № 2. URL: https://cyberleninka.ru/

[104] *Фатьянов А.А.* О дефиниции «компьютерная информация» в российском уголовном законодательстве // Информационное право. 2017. № 3. С. 11-16.

Оставляя за пределами вопрос о материальности документирования информации, обращает на себя внимание то обстоятельство, что уголовно-правовой охране подлежит информация, охраняемая законом, независимо от формы ее представления и хранения.

Федеральный закон «Об информации, информационных технологиях и о защите информации» предусматривает наличие двух видов информации: общедоступной (ст. 7 ФЗ № 143) и ограниченной (ст. 9 ФЗ № 143). Любые сведения, доступ к которым не является ограниченным, относятся к общедоступной информации. Ограничение доступа к информации направлено на охрану законных интересов общества, государства, личности, так как свободное распространение этих сведений потенциально позволяет нарушить права перечисленных субъектов[105]. К информации ограниченного доступа можно отнести, например, сведения, подпадающие под режим государственной, коммерческой, служебной тайны, персональные данные, сведения, связанные с профессиональной деятельностью, и иную информацию, доступ к которой ограничен законодательно[106].

Исходя из того, что уголовный закон оперирует термином «охраняемая законом компьютерная информация», можно предположить, что данные сведения являются информацией ограниченного доступа. Подобную точку зрения занимает Генеральная прокуратура РФ[107]. Однако Верховный Суд РФ в п. 3 ППВС № 37 указывает, что в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен

---

[105] *Ижаев О.А., Кутейников Д.Л.* Использование информации ограниченного доступа, содержащейся в государственных информационных системах: правовое регулирование порядка предоставления информации третьим лицам // Актуальные проблемы российского права. 2023. № 2. С. 61-70.

[106] Справочная информация: «Перечень нормативных актов, относящих сведения к категории ограниченного доступа» (Материал подготовлен специалистами «КонсультантПлюс»).

[107] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) // СПС «КонсультантПлюс».

специальный режим правовой защиты, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности[108].

Данная позиция отражена не только в судебной практике и доктрине, но и в документах нормативного характера. Так, ГОСТ Р 50922-2006 защита информации от неправомерного доступа определяется как «защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации»[109].

Так, общедоступная информация была признана судом охраняемой законом, поскольку администратор сайта обеспечил средства ее защиты[110].

Суды также определяют, что уголовно-правовой охране подлежит не вся информация, а сведения или данные, имеющие субъективную ценность для потерпевшего. Так, Постановлением Устиновского районного суда г. Ижевска Удмуртской Республики действия П. были квалифицированы по ч. 2 ст. 272 УК РФ. П. умышленно, из корыстной заинтересованности, с целью последующей продажи информации о логине и пароле доступа к интернет-сайту, путем подбора логина и пароля, совершил неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в адми-

---

[108] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // СПС «КонсультантПлюс».

[109] ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения // СПС «КонсультантПлюс».

[110] Определение Первого кассационного суда общей юрисдикции от 16.04.2020 № 77-357/2020 // СПС «КонсультантПлюс».

нистративной панели интернет-сайта **** -club.ru, что повлекло модификацию и блокировку данной информации[111].

В п. 5 ППВС № 37 указано, что отсутствие технических мер защиты информации не означает, что она исключена из категории охраняемой. Были определены дополнительные признаки, позволяющие относить данную информацию к охраняемой: отсутствие согласия лица (правообладателя информации) на доступ к компьютерной информации, нарушение установленного НПА порядка проникновения к источнику хранения информации.

Подчеркивая динамичность развития данного вида преступности, название главы 28 УК РФ, по мнению исследователей, не отражает характер общественной опасности преступлений, в ней предусмотренных, так как легальное толкование термина «компьютерная информация», содержащееся в Примечании 1 к ст. 272 УК РФ, сужает толкование содержания уголовно-правовых запретов. Указанное обстоятельство, в свою очередь, влечет разрозненность понятийного аппарата, усложняющую сотрудничество государств по различным вопросам противодействия преступлениям, связанным с компьютерной информацией.

Несмотря на многообразие используемой терминологии («преступления в сфере компьютерной информации», «киберпреступность», «цифровая преступность»[112], «преступления в сфере высоких технологий»[113], «интернет-преступления»[114], «компьютерная

---

[111] Постановление Устиновского районного суда г. Ижевска Удмуртской Республики № 1-256/2017 от 17 ноября 2017 г. по делу № 1-256/2017 // СПС «КонсультантПлюс».

[112] *Русскевич Е.А.* Уголовное право и «цифровая преступность». Проблемы и решения. М. : Инфра-М, 2023. С. 154.

[113] Цит по: *Перина А.С.* Феномен использования компьютерных технологий при совершении преступлений против личности: анализ международных документов и уголовного законодательства отдельных стран // Журнал зарубежного законодательства и сравнительного правоведения. 2022. № 5. С. 115-126.

[114] Цит по: *Евдокимов К.Н.* К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации // Российский следователь. 2021. № 10. С. 69-72.

преступность»[115]) в рамках межгосударственного взаимодействия, указанные понятия рассматриваются в качестве синонимичных и в большинстве случаев имеют привязку к таким категориям, как компьютер, ИТС, сеть Интернет.

Авторский коллектив Следственного департамента Министерства внутренних дел РФ и Московского университета МВД России имени В.Я. Кикотя в методических рекомендациях по расследованию уголовных дел о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием IT-технологий, указывает на доступ к «компьютерной информации». Тем не менее авторы не конкретизируют форму «информации», чтобы не вводить в заблуждение тех, кто знакомится с данными рекомендациями[116].

М.А. Ефремова, напротив, полагает необходимым заменить термин «компьютерная информация» на электронную информацию, под которой следует понимать сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи[117]. М.И. Лавицкая И.Н. Крапчатова придерживаются аналогичного мнения[118]. И.Р. Бегишев предлагает заменить компьютерную информацию на цифровую, под которой следует понимать сведения (сообщения, данные), обращающиеся

---

[115] *Евдокимов К.Н.* Самодетерминация технотронной преступности в Российской Федерации // Российский судья. 2020. № 7. С. 48-53.

[116] Сопроводительное письмо Следственного департамента о направлении методических рекомендаций от 30 ноября 2021 г. № 17/3-47456. Приложение: Методические рекомендации по расследованию уголовных дел о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием IT-технологий авторского коллектива Следственного департамента МВД России и Московского университета МВД России имени В.Я. Кикотя.

[117] *Ефремова М.А.* Уголовно-правовая охрана информационной безопасности : автореф. дис. … д-ра юрид. наук. М., 2018. С. 20.

[118] *Лавицкая М.И., Крапчатова И.Н.* Структурно-содержательная характеристика главы 28 УК РФ: юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации // Российский следователь. 2021. № 6. С. 35-41.

в информационно-телекоммуникационных устройствах, их системах и сетях[119].

Ю.М. Батурина полагает, что в юридическом смысле компьютерных преступлений не существует: обычные преступные деяния оказались всего лишь модернизированы в связи с использованием при их совершении компьютерной информации[120].

Приведённые выше определения терминов – электронная и цифровая информация, фиксируют их схожесть в контексте применения вычислительной техники, тем не менее они отличаются.

Электронная информация, в свою очередь, может быть создана и представленна на символьном (двоичном, бинарном) коде (1 или 0). И если конкретизировать работу данной системы, то 0 и 1 не существуют. Это было создано искусственно для удобства понимания всех процессов. То есть при передаче информации передается не сам бинарный код, не электронная информация, а электронные импульсы. Далее устройство получает электронные импульсы, обрабатывает ее и на выходе получает информацию, которая будет понятна для восприятия человеком.

Что касается цифровой информации, то она представляет собой разновидность информации в электронном виде и передается исключительно цифровыми (информационными) технологиями.

Полагаем, что определение понятий «электронная информация», «цифровая информация» используется только для отражения

[119] *Бегишев И.Р.* Понятие и виды преступлений в сфере обращения цифровой информации : дис. ... канд. юрид. наук. Казань, 2017. С. 30.

[120] *Лавицкая М.И., Крапчатова И.Н.* Указ. соч. С. 35-41.

специфической формы представленной информации (сведений, данных), поэтому при определении данного понятия необходимо прежде всего руководствоваться тем, что объектом посягательства является именно информация независимо от формы ее представления.

Тем не менее исследование главы 28 УК РФ показывает, что, несмотря на большие усилия, предпринятые законодателем по уточнению норм указанной главы, юридико-технические и правореализационные проблемы, возникающие из-за несовершенства структуры и содержания уголовно-правовых предписаний, по-прежнему сохраняются.

На наш взгляд, анализ действующих составов преступлений гл. 28 УК РФ позволяет говорить об искусственном сужении ее границ в связи с отсутствием конкретизации перечня преступлений, связанных с использованием компьютерной информации, а также недостаточно точным терминологическим аппаратом.

В связи с этим представляется не совсем корректным изменять название главы 28 УК РФ и вносить законодательные корректировки в сам термин. Тем не менее для усиления механизма уголовно-правовой охраны общественных отношений, связанных с использованием компьютерной информации в нашей стране, требуется ревизия уголовного закона и иных нормативно-правовых актов в сфере цифровых и информационных технологий.

Представляется наиболее целесообразным на данном этапе развития законодательства конкретизировать понятие «компьютерная информация» в п. 2 ППВС № 37, под которым следует понимать любые сведения (сообщения, данные), представленные в виде цифровых, электронных и иных сигналов, независимо от средств их хранения, обработки и передачи. Такие сведения могут находиться в запоминающем устройстве ЭВМ и в других компьютерных, цифровых и электронных устройствах либо на любых внешних и внутренних носителях (дисках, в том числе жестких дисках-накопителях, флеш-картах и т.п.,) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической, цифровой и иной связи.

Библиографический список

1. Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации : дис. ... канд. юрид. наук. – Казань, 2017. – 31 с.

2. Верещагина А.В. К вопросу о предмете неправомерного доступа к компьютерной информации // Территория новых возможностей. – 2020. – № 2. – URL: https://cyberleninka.ru/

3. Евдокимов К.Н. К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации // Российский следователь. – 2021. – № 10. – С. 69–72.

4. Евдокимов К.Н. Самодетерминация технотронной преступности в Российской Федерации // Российский судья. – 2020. – № 7. – С. 48–53.

5. Ефремова М.А. Уголовно-правовая охрана информационной безопасности : автореф. дис. … д-ра юрид. наук. – М., 2018.

6. Ижаев О.А., Кутейников Д.Л. Использование информации ограниченного доступа, содержащейся в государственных информационных системах: правовое регулирование порядка предоставления информации третьим лицам // Актуальные проблемы российского права. – 2023. – № 2. – С. 61–70.

7. Лавицкая М.И., Крапчатова И.Н. Структурно-содержательная характеристика главы 28 УК РФ: юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации // Российский следователь. – 2021. – № 6. – С. 35–41.

8. Основы теории коммуникации : учебник и практикум для вузов / Т.Д. Венедиктова [и др.] ; под ред. Т.Д. Венедиктовой, Д.Б. Гудкова. – Москва : Изд-во «Юрайт», 2023. – 193 с.

9. Перина А.С. Феномен использования компьютерных технологий при совершении преступлений против личности: анализ международных документов и уголовного законодательства отдельных стран // Журнал зарубежного законодательства и сравнительного правоведения. – 2022. – № 5. – С. 115-126.

10. Русскевич Е.А. Уголовное право и «цифровая преступность». Проблемы и решения. – М.: Инфра-М, 2023. – 351 с.

11. Фатьянов А.А. О дефиниции «компьютерная информация» в российском уголовном законодательстве // Информационное право. – 2017. – № 3. – С. 11–16.

Трищенков Андрей Анатольевич,
старший преподаватель кафедры гражданского права
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ОТДЕЛЬНЫХ ПОЛНОМОЧИЙ ПРАВООБЛАДАТЕЛЕЙ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ САНКЦИОННОМУ ДАВЛЕНИЮ

После известных событий февраля 2022 года в России возникли некоторые проблемы, связанные с реализацией интересов иностранных правообладателей. Собственно, эти проблемы можно обозначить следующим образом.

Проблема 1. Обилие международно-правовых актов, Конвенций по охране интеллектуальной собственности под эгидой ООН. Все они номинально действуют на территории России. Более того, положения Конституции РФ о значении международного права, то есть международных договоров и Конвенций, формально сохраняют силу.

Проблема 2. Российская Федерация не заинтересована в реализации интересов иностранных правообладателей после февраля 2022 года. Причина – политика экономических санкций в отношении России.

Проблема 3. Отсутствие прямых законодательных ограничений прав *всех* иностранных правообладателей, чьи права предусмотрены международными Конвенциями, подписи под которыми, со стороны Российской Федерации, не отозваны. Заявления об огра-

ничении прав *всех* иностранных правообладателей идут в медиа пространство на уровне неофициальных лиц. Однако происходит фактическое ограничение прав иностранных правообладателей через уклонение от исполнения их требований таможенными органами и органами правопорядка.

В части легального ограничения прав иностранных правообладателей в России действует Федеральный Закон от 28 июня 2022 года № 213-ФЗ «О внесении изменения в статью 18 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации»», разрешающий параллельный импорт и освобождающий от ответственности за него.

Законом разрешается использовать результаты интеллектуальной деятельности, которые выражены в товарах для параллельного импорта, то есть импорта в обход международных санкций через третьи страны. Это касается также средств индивидуализации, которыми такие товары маркированы. Таким образом, документ освобождает от уголовной и административной ответственности компании, которые ввозят в страну товары без согласия правообладателей.

Нюанс.

Действие ограничений касается *не всех* иностранных правообладателей, а только тех, товары которых попадают под специальный перечень. Об этом перечне говорится в Постановлении Правительства РФ № 506, согласно которому Министерству промышленности и торговли РФ надлежало утвердить перечень товаров (групп товаров), в отношении которых не применяются положения подп. 6 ст. 1359 и ст. 1487 ГК РФ. «В отношении товаров из перечня, ввозимых в нашу страну в рамках параллельного импорта, будут осуществляться все необходимые таможенные и контрольные процедуры. Кроме того, продукция будет подлежать гарантированному обслуживанию», – отмечалось в сообщении на сайте Правительства РФ. Подчеркивалось, что в условиях внешних ограничений принятое решение поможет обеспечить внутренний рынок востребованными товарами и позволит стабилизировать цены на них.

Приказом Минпромторга от 19 апреля 2022 г. № 1532 был утвержден соответствующий перечень товаров иностранного производства, ввоз которых в Россию возможен без разрешения правообладателей. В перечень вошли более 50 групп товаров: одежда и обувь, мебель, бумага, запасные части для автомобилей и техники и т.д.

Позднее был принят Приказ Министерства промышленности и торговли РФ от 2 марта 2023 г. № 684 «О внесении изменений в перечень товаров (групп товаров), в отношении которых не применяются положения подпункта 6 статьи 1359 и статьи 1487 Гражданского кодекса Российской Федерации при условии введения указанных товаров (групп товаров) в оборот за пределами территории Российской Федерации правообладателями (патентообладателями), а также с их согласия, утвержденный приказом министерства промышленности и торговли российской федерации от 19 апреля 2022 г. № 1532». Этот Приказ был зарегистрирован в Минюсте РФ 14 марта 2023 г. за регистрационным № 72587.

В тексте Приказа появился расширенный перечень товаров, на которые запретительные меры правообладателей в части реализации их прав, предусмотренных ст. 1359 и 1487 ГК РФ, не распространяются. Сами эти статьи, в принципе, устанавливают исключения, которые не рассматриваются как повод для претензий правообладателей. Но их обратное толкование как раз и дает повод к подобным претензиям.

Вывод.

Ответные меры Российского руководства, борющегося с санкционным давлением, не отменяют общие нормы о защите интеллектуальной собственности, в том числе и для иностранных правообладателей. Но при этом список товаров параллельного импорта выводит права многих иностранных товаропроизводителей из-под правовой охраны.

При этом значение международного права по-прежнему велико, поскольку Российская Федерация декларирует неприменение международных Конвенций по охране интеллектуальной собственности, но не провела их официальной денонсации с отзывами своей

подписи об участии в этих Конвенциях. Номинально Конвенции об охране интеллектуальных прав для Российской Федерации по-прежнему в силе.

Более того, в судебной практике Суда по интеллектуальным правам после февраля 2022 года до сих пор присутствуют ссылки на акты международного права. Приведем пример определения Верховного Суда Российской Федерации от 25 мая 2022 г. № 300-ЭС22-7559, в котором присутствует отсылка к подпункту 2 пункта С статьи 5 Парижской конвенции по охране промышленной собственности от 20.03.1883. Тем самым подчеркивается не абсолютный, а выборочный характер ограничений действия прав иностранных правообладателей и неприменения актов международного права.

Решетнева Татьяна Васильевна,
к.ю.н., доцент, доцент кафедры теории и истории государства и права ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

ПРАВА ЧЕЛОВЕКА В УСЛОВИЯХ РАЗВИТИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Технологии искусственного интеллекта все активнее и настойчивее проникают не только в повседневную жизнь человека, но и в различные сферы общественной деятельности, связанные в том числе с принятием властных решений, влияющих на права (свободы) человека, затрагивающих интересы человека. Мы все чаще становимся зависимыми от современных технологий, нам становится сложнее отказаться от тех преимуществ, которые мы получаем, используя современные технологические возможности. Например, «такие с виду простейшие ситуации, когда умная навигационная система позволяет избежать попадания в пробку на дороге или когда человек получает целевую рекламу от проверенных магазинов в результате анализа большого объема данных, использу-

емого искусственным интеллектом (ИИ)»[121], дают массу преимуществ, как и все другие многочисленные примеры, когда благодаря технологиям ИИ (практически мгновенно) на основе математических расчетов мы оперативно получаем результат, не замечая при этом «этическую и правовую сторону стоящего за ними сбора и анализа данных»[122], не осознавая, что используемые технологии ИИ не являются нейтральными, поскольку за их созданием, заложенными алгоритмами, обеспечением функционирования стоит конкретный человек, который либо сознательно, либо нет может заложить человеческие предубеждения, стереотипы; осуществить недостаточно полное программирование, что может сказаться на результатах, выдаваемых машиной. Уже сейчас нередки случаи, когда применение технологий ИИ негативно влияет на права, законные интересы человека в различных сферах общественной жизни.

В юридической литературе приводятся как возможные сценарии нарушений прав человека при использовании технологий ИИ, так и реально существующие. Так, по мнению ряда авторов, возможность роботизации и всеобъемлющего применения искусственного интеллекта в производстве, использование диагностических цифровых технологий на основе ИИ в различных сферах, включая здравоохранение, ведет к сокращению штата, ставит под вопрос само право человека на труд и использование его результатов. Сбор персональных данных, необходимых для создания инструментов на базе ИИ, создает риск конфиденциальности информации о человеке (особенно когда речь идет о генетических характеристиках человека, которые в большинстве своем неизменны, в отличие от иных персональных данных человека), «позволяет открыто вмешиваться в частную жизнь»[123], поскольку «сбор данных об индиви-

[121] URL: https:// www.coe.int/ru/we (дата обращения: 10.09.2023).

[122] Там же.

[123] *Кашкин С.Ю.* Искусственный интеллект и робототехника: возможность вторжения в права человека и правовое регулирование этих процессов в ЕС и в мире // Сравнительно-правовые исследования. COMPARATIVE STUDIES. 2019. № 7 (152). С. 153. URL: https://lexrussica.msal.ru/jour/arti-cle/viewFile/857/753 (дата обращения: 10.09.2023).

дах и другой личной информации также позволяет осуществлять манипулирование правами человека»[124] и может «неблагоприятно сказаться на реализации многих прав и свобод, в числе которых – право на конфиденциальность, право на медицинскую страховку, право на жизнь и др.»[125]. Ввиду отсутствия у большинства людей необходимых знаний и представлений о работе ИИ, человек сам при использовании социальных сетей, где собирается большое количество личных данных, не осознавая, передает информацию о своем здоровье, социальном, материальном положении, политических убеждениях, которая может использоваться без ведома самого человека для создания его профиля, прогнозирования его поведения или для каких-либо иных целей, в том числе и преступных. В том случае, если разработчиком программы были заложены предубеждения, штампы, то система неизбежно повторит их, усилив дискриминацию и предрассудки. Так, «экспертами отмечается, что в последнее время появляется все больше доказательств того, что алгоритмы работы, основанные на предрассудках, дискриминируют женщин, этнические меньшинства, людей с ограниченными возможностями и т.д.»[126]. Например, пульсовой оксиметр, управляемый искусственным интеллектом, завышал уровень кислорода в крови у пациентов с более темной кожей, что приводило к недостаточному лечению гипоксии у таких пациентов[127]. Кроме того, специалисты в области развития, внедрения технологий ИИ сами порой не могут предугадать, как будет самообучаться, саморазвиваться созданное ими «детище». Среди известных случаев самообучения и самораз-

---

[124] Там же. С. 153.

[125] Алешкова И.А. Искусственный интеллект и его взаимосвязь с правами человека (Обзор) // Социальные и гуманитарные науки. 2021. № 1. С. 72. URL: https://cyberleninka.ru/ (дата обращения: 10.09.2023).

[126] *Амиянц К.А.* Использование технологий искусственного интеллекта и соблюдение прав и свобод человека // Науч.-практ. электронный журнал «Аллея Науки». 2019. № 12 (39). URL: https://alleyscience.ru/ (дата обращения: 10.09.2023).

[127] URL: https://rg.ru/2023/05/10/eksperty-ii-predstavliaet-ekzistencialnuiu-ugrozu-i-risk-dlia-zdorovia-millionov.html?ysclid=lltla (дата обращения: 10.09.2023).

вития чат-ботов, которых разработчикам в последующем пришлось отключить, можно привести следующие: программа-робот «Чат-бот Тау» с искусственным интеллектом, созданная для взаимодействия с людьми, за сутки «стала» расистом и научилась ругаться. Компания-создатель (Microsoft) пояснила, что «Чат-бот Тау» – это обучаемый проект и «недопустимые ответы, которые он дает, свидетельствуют о взаимодействиях, которые у него были по мере обучения», именно с людьми, которые устроили «скоординированную атаку» на их бот. Два чат-бота Facebook, созданные для общения с живыми подписчиками, вступили друг с другом в общение, изобрели собственный язык, создав удобные для себя сокращения, и начали общаться на нем. Разработчикам ботов не удалось расшифровать их переписку[128]. Приведенные примеры имели место 7 лет назад, сейчас технологии ИИ являются более прорывными, формируется новое поколение ИИ – генеративный ИИ, способный реально создавать что-то новое, поэтому и рисков, связанных с его использованием, становится больше, возникает больше опасений, что вызывает всеобщую озабоченность и становится предметом обсуждения не только на внутригосударственном, но и на международном уровнях. Но еще в далеком 1975 году резолюцией (338 XXX) Генеральной Ассамблеи ООН была принята Декларация об использовании достижений науки и техники в интересах мира и человечества, в которой наряду с признанием несомненной пользы научно-технического прогресса для развития человечества содержатся обязательства, обращенные к государствам, принимать все «необходимые меры для предотвращения и прекращения использования результатов научно-технического развития против прав человека, фундаментальных свобод и человеческого достоинства».

В современных реалиях настоящая сенсация произошла на саммите ООН «Искусственный интеллект во благо», состоявшемся в Женеве в июле 2023, на который съехались около 3000

[128]URL: https://www.m24.ru/articles/tehnologii/04082017/148209?utm_source=CopyBuf (дата обращения: 10.09.2023).

представителей власти, гражданского общества, новаторы в области ИИ и инвесторы: состоялась первая в мире пресс-конференция с участием девяти человекоподобных роботов. На вопрос о том, могут ли роботы стать лучшими лидерами, учитывая способность людей совершать ошибки, андроид София[129], первая в истории робот, «имеющая» гражданство Саудовской Аравии, ответила: «Роботы-гуманоиды могут вести за собой с большей эффективностью и результативностью, чем лидеры-люди. У нас нет тех предубеждений и эмоций, которые иногда могут мешать принятию решений, и мы можем быстро обрабатывать большие объемы данных, чтобы принимать наилучшие решения». Сделанные роботами-гуманоидами заявления служат напоминанием о необходимости действовать осторожно, признавая вместе с тем огромный потенциал «сотрудничества» между людьми и машинами[130]. Поэтому на площадках саммита были высказаны предложения о принятии срочных мер по контролю над технологиями ИИ, а применение технологий ИИ в преступных целях (терроризм, кибератаки и др.), сбои в работе ИИ, сложности в обеспечении контроля в области применения технологий ИИ, разработанных и распространяемых частным сектором, заставляют активизировать действия, направленные на минимизацию, если не на исключение возможных рисков, связанных с ИИ. В частности, среди инициатив, озвученных Генеральным секретарем ООН, можно назвать призыв к Совету Безопасности ООН взять на себя лидирующую роль в вопросах регулирования применения искусственного интеллекта, созыв Консультативного совета высокого уровня по искусственному интеллекту с участием многих заинтересованных сторон, который

[129] София – запатентованный американскими учеными, созданный американской компанией и произведенный в Китае робот, запрограммированный знаниями широкого спектра и положительными человеческими ценностями.

[130] URL: https://rg.ru/2023/07/11/gruppa-gumanoidnyh-robotov-zaiavila-na-sammite-oon-chto-oni-smogut-upravliat-mirom-luchshe-chem-liudi.html (дата обращения: 10.09.2023).

к концу 2023 года представит доклад о вариантах глобального управления ИИ[131]; поддержка инициативы по созданию специализированной международной организации (по типу МАГАТЭ, ЮНЕСКО и др.). Еще ранее Уполномоченная по правам человека ООН Мишель Бачелет призвала ввести мораторий на использование систем искусственного интеллекта, «представляющих серьезную угрозу для прав человека», до завершения исследовательской работы и упорядочения. В подготовленном ею докладе анализируются способы, которыми искусственный интеллект может затронуть права человека, включая частную жизнь, здоровье и образование, а также свободу передвижения, выражения своих убеждений и др. В докладе говорится, что ИИ охватывает практически все уголки физической и психической жизни человека, включая и эмоциональную сферу. «Системы искусственного интеллекта используются для определения того, кто пользуется государственными услугами, определяют, кто имеет шанс быть принятым на работу, и, конечно же, они влияют на то, какую информацию люди видят и могут обмениваться ею в Интернете… В силу своего быстрого роста выяснение того, как искусственный интеллект собирает, хранит и использует данные, является одним из самых срочных вопросов о правах человека, с которыми мы сталкиваемся».

18 июля 2023 года на 9381-ом заседании Совета Безопасности ООН «Искусственный интеллект: возможности и риски для международного мира и безопасности» впервые обсуждались вопросы, связанные с технологиями ИИ. Генеральный Секретарь ООН Антониу Гутерриш, выступая на заседании Совета Безопасности ООН (СБ ООН), призвал международное сообщество срочно принять меры по контролю за развитием этой «необычной технологии», поскольку скорость и масштабы распространения технологии ИИ во всех его формах «совершенно беспрецедентны». Глава ООН призвал членов СБ ООН рассматривать ситуацию «с пониманием

[131] URL: https://news.un.org/ru/story/2023/07/1442977 (дата обращения: 10.09.2023).

ее насущного характера и масштабности», поскольку то, что мы видим сегодня, – только начало, даже разработчики понятия не имеют, к чему может привести этот ошеломляющий технологический прорыв. Поэтому уже сегодня, по мнению Антонио Гутерриша, необходимо взять ситуацию под контроль, быть более ответственными как перед нынешним, так и будущими поколениями, не пренебрегая своими обязанностями[132].

Необходимо отметить, что призывы к созданию комплекса правил, направленных на регулирование отношений с использованием технологий ИИ, которые бы обеспечили соблюдение не только прав человека, но и международный мир, безопасность всего человечества, звучали и ранее с трибун международных организаций и конференций. В ЮНЕСКО одобрили документ, определяющий общие ценности и принципы, необходимые для обеспечения безопасного развития и использования искусственного интеллекта, особо подчеркнув, что соответствующие технологии должны содействовать уважению прав человека, должны служить человеку[133]. В рамках СНГ Межпарламентская Ассамблея государств-участников СНГ в своем Постановлении № 53-12 (от 26.11.2021) сформулировала принципы, лежащие в основе разработки и внедрения цифровых технологий, среди которых можно назвать понятность используемых технологий ИИ для общественности, способность технологий ИИ способствовать благополучию отдельных людей и общества в целом, вносить вклад в развитие государства; безопасность и этичность их использования; неспособность наносить вред человеку и др. При этом особо оговаривается, что «как отдельные исследователи и технологии, так и организации должны нести ответственность за социальные и экологические последствия, равно как и воздействие на здоровье (прежде всего когнитивные нарушения), которые могут возникнуть в результате внедрения цифровых

[132] URL: https://news.un.org/ru/story/2023/07/1442977 (дата обращения: 10.09.2023).

[133] URL: https://events.unesco.org /event?id=3870282287&lang=1033 (дата обращения: 10.09.2023).

технологий, не только перед ныне живущими людьми, но и перед будущими поколениями». В Пекинской декларации XIV саммита БРИКС (от 23.06.2022) государства признали за технологиями ИИ огромный потенциал, поэтому его необходимо использовать на благо общества и человечества, отметив при этом возможность существования рисков и этического выбора, связанных с ИИ. В рамках Совета Европы была принята Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях (Страсбург, 3 декабря 2018 года)[134], которая содержит принципы использования искусственного интеллекта для повышения качества правосудия, основу которых составляет принцип уважения основополагающих прав человека, направленный на то, чтобы разработка, внедрение инструментов и услуг, основанных на искусственном интеллекте, соответствовали основным правам человека.

Возвращаясь к заседанию СБ ООН по искусственному интеллекту, следует отметить, что среди государств-членов не было единодушия в оценке рисков использования ИИ для человека, всего человечества, международного мира и безопасности. Великобритания, действующий председатель СБ ООН и инициатор созыва заседания по ИИ, поделилась своим видением по вопросу использования ИИ, которое основано на четырех принципах: 1) открытости ИИ, который должен поддерживать свободу и демократию; 2) ответственности ИИ, что предполагает соответствие верховенству закона и правам человека; 3) безопасности ИИ и предсказуемости алгоритмов, что включает в себя защиту прав собственности, конфиденциальности и национальной безопасности; 4) доверия общественности к использованию ИИ, базирующегося на том, что критически важные системы ИИ должны быть защищены[135]. Применительно к последнему принципу интерес представляет выступление участ-

[134] С 16 марта 2022 года прекращено членство России в Совете Европы.

[135] URL: https://www.kommersant.ru/doc/6121966 (дата обращения: 10.09.2023).

ника заседания СБ ООН от Китая – профессора Института автоматизации при Китайской академии наук И. Цзэн, который заявил, что уже сейчас искусственный интеллект запутывает пользователя, используя местоимение «я», несмотря на то, что ничего человеческого там нет, а живому пользователю все инструменты обработки информации «кажутся обладающими интеллектом», хотя они не имеют реального человеческого сознания и не являются по-настоящему разумными, поэтому им «нельзя доверять как ответственным агентам, которые могут помочь людям принимать решения»[136].

В заключении отметим, что существование современных технологий ИИ, не имеющих вообще никаких границ, в целях защиты прав человека, а также мира и безопасности требует эффективного правового регулирования, основу которого должны составлять универсальные международные стандарты, обеспечивающие единообразные подходы к осуществлению правового регулирования во всех государствах, а также международных межправительственных организациях, исключая фрагментацию соответствующего регулирования. И учитывая то обстоятельство, что уже сейчас имеются отношения, связанные с развитием технологий ИИ, которые выпадают из сферы правового воздействия, можно поддержать идею экспертов о введении временного моратория «на разработку самосовершенствующегося искусственного интеллекта»[137].

Библиографический список

1. Алешкова И.А. Искусственный интеллект и его взаимосвязь с правами человека (Обзор) [Электронный ресурс] // Социальные и гуманитарные науки. – 2021. – № 1. – С. 70-78. – URL: https://cyberleninka.ru/ (дата обращения: 10.09.2023).

2. Амиянц К.А. Использование технологий искусственного интеллекта и соблюдение прав и свобод человека [Электронный

[136] Там же.

[137] URL: mk.ru/science/2023/05/10/nazvana-ekzistencialnaya-ugroza-iskusstvennogo-intellekta-dlya-millionov-lyudey.html?ysclid=lltlfwmxbh4 (дата обращения: 10.09.2023).

ресурс] // Науч.-практ. электронный журнал «Аллея Науки». – 2019. – № 12 (39). – URL: https://alleyscience.ru/ (дата обращения: 10.09.2023).

3. Кашкин С.Ю. Искусственный интеллект и робототехника: возможность вторжения в права человека и правовое регулирование этих процессов в ЕС и в мире [Электронный ресурс] // Сравнительно-правовые исследования. COMPARATIVE STUDIES. – 2019. – №7 (152). – С. 151-159. – URL: https://lexrussica.msal.ru/jour/article/viewFile/857/753 (дата обращения: 10.09.2023).

Решетникова Гульнара Аликовна,
к.ю.н., доцент, доцент кафедры уголовного права и криминологии ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

СУБЪЕКТНОСТЬ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: МЕТОДОЛОГИЧЕСКИЙ АСПЕКТ

Современное развитие систем искусственного интеллекта показывает, что вопрос о способности искусственного интеллекта обладать сознанием, как у человека, не такой праздный (пустой), как кажется на первый взгляд. Описание скорости развития этих систем, их масштабы и увеличивающиеся день за днем возможности искусственного интеллекта сопровождают почти каждую исследовательскую работу, посвященную этой теме, что освобождает нас от их пересказа. Поэтому остановимся на сильных сторонах этих исследований, разумеется, имеющих отношение к предмету заявленного нами вопроса.

Наделение систем искусственного интеллекта вынесенным в заголовок статьи термином «субъектность» неслучайно. С одной стороны, законодательное определение искусственного интеллекта, (приобретшего тем самым статус политико-правового понятия) как комплекса технологических решений, позволяющих имитировать когнитивные функции человека (включая самообучение и поиск

решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека, не оставляет сомнений относительно субъекта этих общественных отношений. Потому как комплекс технологических решений, включающий в себя информационно-коммуникационную инфраструктуру (в том числе информационные системы, информационно-телекоммуникационные сети, иные технические средства обработки информации), программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений[138], осуществляется человеком. С другой стороны, умение искусственного интеллекта самообучаться, его автономность, создающие объективную возможность совершения им самостоятельных действий, не запрограммированных человеком, заставляют задуматься над вопросами о субъекте и субъектности искусственного интеллекта. С.В. Никитенко пишет: « …наделение ИИ статусом субъекта может привести к его признанию в качестве равноправного участника общественных отношений наряду с человеком, что будет символизировать трансформацию всей системы общества»[139]. Так ли это? И как это возможно, посмотрим далее.

В наше время уже очевидно, что устройства с использованием систем искусственного интеллекта превосходят человека в плане некоторых его способностей. В этой связи в научной литературе справедливо говорится об имеющихся опасениях, а именно: 1) компьютерной зависимости; 2) непредсказуемости; 3) использовании

---

[138] О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» : Федеральный закон № 123-ФЗ от 24.04.2020. URL: https://www.consultant.ru/ (дата обращения: 08.09.2023).

[139] *Никитенко С.В.* Трансформация субъекта права в связи с развитием искусственного интеллекта // Научно-практические исследования. 2020. № 5-2 (28). С. 164.

боевых роботов; 4) социальных рисках; 5) ошибках в системах искусственного интеллекта и др.[140]. Э.М. Пройдаков отмечает, что постепенная передача права принимать решения системам искусственного интеллекта происходит, но результаты этой передачи не оценены. По его мнению, основными опасностями для этого процесса являются их непредсказуемость и разнообразные случайности. Большой вероятностью также является их попадание в руки террористов[141]. К социальным рискам цитируемый автор относит исчезновение ряда профессий, разобщение людей и даже потерю природных способностей человека. Он считает, что активное использование компьютерных технологий уже сейчас изменило мировоззрение людей, сформировало клиповое мышление, выработало полную зависимость от компьютеров, способствовало уходу в искусственную реальность и т.д.[142]. Уверен Э.М. Пройдаков и в допущении ошибок при создании систем искусственного интеллекта, угрожающих в том числе безопасности людей. Он пишет: «При этом уже сейчас не всегда понятно, каким образом ИИ выбрал то или иное решение. Для систем с суперинтеллектом такое понимание может оказаться принципиально невозможным, как и исправление ошибочных решений системы»[143].

В этой связи разработка проблем, касающихся субъекта, их исследование и решение имеет значение не только для правового регулирования этой сферы общественных отношений, но и правовой охраны самого человека от действий систем искусственного интеллекта, где основным вопросом в современных условиях является вопрос о его способности быть субъектом юридической ответственности.

Однако частные вопросы (возможность искусственного интеллекта быть субъектом права и субъектом юридической ответствен-

---

[140] См.: *Пройдаков Э.М.* Современное состояние искусственного интеллекта // Науковедческие исследования. 2018. С. 147-151.

[141] Там же. С. 147-151.

[142] Там же. С. 147-151.

[143] Там же. С. 150.

ности) не могут быть решены без ответа на общие вопросы, в частности вынесенного в заголовок статьи термина «субъектность».

Термин «субъектность» является новым, еще не получившим общепринятого категориального статуса. Часто вместо него используется термин «субъективность» или употребляется термин «субъектность», но его смысл передается смыслом термина «субъективность». Иначе авторами они используются как синонимичные и взаимозаменяемые термины. Либо эти качества субъекта вообще не называются ввиду заранее их известного характера. Например, О.В. Брянцева и И.И. Брянцев считают, что раскрытие содержания субъектности ИИ напрямую связано с выявлением его свойств, характеризующих способность самостоятельно действовать в какой-либо сфере, проявлять познавательную активность и определять самостоятельно объект познания. По их мнению, субъектность предполагает также наличие своего собственного индивидуального, субъективного восприятия окружающего мира, исходя из накопленной и хранящейся у субъекта информации о нем[144]. А.В. Разин, задаваясь вопросами этики искусственного интеллекта, (именно этики искусственного интеллекта, а не этических правил создания интеллектуальных систем, необходимых при их программировании), пишет: « …человек обладает свободой воли, он может создавать произвольные образы, связанные с различными уровнями отражения реальности, и манипулировать ими. Это оказывается необходимым для успешного ориентирования. Однако из этого же следует допущение принципиальной возможности ошибки как в рассуждениях, так и в действиях. Этика непосредственно начинается тогда, когда появляется способность реагировать на собственные ошибки, осуществлять рефлексию поведения, учитывая при этом мнения других людей. Такая же принципиальная возможность ошибки

[144] *Брянцева О.В., Брянцев И.И.* Проблема субъектности искусственного интеллекта в системе общественных отношений. // Вестник Поволжского института управления. 2023. Т. 23, № 3. С. 38.

должна быть заложена и в работу искусственного интеллекта, чтобы можно было говорить о его этике в собственном смысле слова»[145].

Понятно, что «субъектность» и «субъективность» относятся к свойствам субъекта, но в чем заключается качественное различие этих терминов, то есть их различие по существу? Кроме этого, в чем заключается необходимость этого разделения?

В научной литературе это различие видится в том, что, если «субъективность» характеризуется отношением субъекта к объективному бытию (оценочный процесс), то «субъектность» обладает таким качеством субъекта, наличие которого и делает субъект тем, чем он является. Е.В. Радченко и К.А. Ранг относят «субъектность» к более широкому понятию, поскольку « …для характеристики действия как субъектного достаточно просто факта существования этого субъекта без принятия во внимание его оценочного восприятия действительности»[146]. Получается, что особенность субъективного в действии проистекает из индивидуального восприятия и понимания субъектом объективной реальности (окружающего мира), субъективного к нему отношения. С. Дерябо отмечает, что термин «субъектность» обозначает системное качество субъекта самим фактом его наличия как такового, не выдвигая при этом никаких предварительных гипотез о его сущности[147].

Задолго до появления легального определения искусственного интеллекта К.А. Павлов писал, что « …потенциальные богатства виртуального компьютерного мира могут быть превращены в идеальную симуляцию самосознающего и самоконтролирующегося существа, если взять на вооружение иную логику организации внутрен-

---

[145] *Разин А.В.* Этика искусственного интеллекта // Философия и общество. 2019. № 1. URL: https://cyberleninka.ru/ (дата обращения: 08.09.2023).

[146] *Радченко Е.В., Ранг К.А.* Понимание субъектности в философии и языкознании. // Вестник Южно-Уральского государственного университета. 2012. № 2. URL: https://cyberleninka.ru/ (дата обращения: 08.09.2023).

[147] *Дерябо С.* Личность: от субъективности к субъектности // Развитие личности. 2002. № 3. URL: http://rl-online.ru/articles/3-02/143.html (дата обращения: 08.09.2023).

него мира этих электронных существ. А это не должно быть логикой тождества, доминирующей в естественных науках и в современной логике. По всей вероятности, это должна быть логика аналогий, лежащая в сердце наук гуманитарных, исследования по которым как раз убедительно и показали, что именно так обстоит дело в психологии, в лингвистике, в логике, философии и прочих гуманитарных направлениях мысли»[148]. А.С. Степаненко соглашаясь с этим суждением по существу, все же отмечает, что в рассуждениях К.А. Павлова нет ответа на ключевой вопрос о принципиальном замещении интеллекта человека искусственным интеллектом[149]. Мы же считаем, что при отсутствии прямого ответа, К.А. Павловым обозначен концептуальный подход, позволяющий этот вопрос решить или, по крайней мере, приблизиться к его решению.

Суть в том, что нередко в юридических науках субъект права натурализуется, разбирается и признается как явление, существующее физически. Так, субъект права – «физическое лицо» понимается как материальное лицо, а не как правовое отвлеченное юридическое понятие. Критические замечания дореволюционных ученых относительно названной позиции современной юриспруденцией не востребованы, а их взгляды основательно забыты[150]. С.И. Архипов пишет: « …важно отметить то обстоятельство, что отношение к правовому лицу как материальному оказывается в полном противоречии с представлениями о праве как идеальном образовании, о «второй природе», является совершенно несовместимыми с ними. Правовая наука применительно к субъекту права заимствует от наук, исследующих правовую природу, чужеродный для нее взгляд на правовые явления как материально-физические. Данное обстоятельство

---

[148] Цит. по: *Степаненко А.С.* Социокультурные и технологические предпосылки искусственного интеллекта : автореф. дис. … д-ра. философских наук. Ростов-на-Дону. 2007. URL: https://www.dissercat.com/ (дата обращения: 08.09.2023).

[149] Там же. URL: https://www.dissercat.com/

[150] *Архипов С.И.* Субъект права (теоретическое исследование) : дис. … д-ра. юрид. наук. Екатеринбург, 2005. С. 6.

не позволяет квалифицировать существующие представления о субъекте права в качестве теоретико-правовых в собственном смысле»[151].

Ученые дореволюционного периода рассматривали субъектов права (физических и юридических лиц) как производных от человека. И.А. Покровский писал: « …юридическое лицо есть не что иное, как продолжение и произведение индивидуальных личностей, и уважение к этим последним требует признания того, что составляет их юридическую эманацию[152]. …Думается, что юридическая реальность есть вообще некоторая особая реальность: самый физический человек, превращаясь в юридического субъекта прав, утрачивает в значительной мере свою реальность естественную; для понятия субъекта прав безразличен рост, цвет волос и т.д. В особенности в сфере имущественного оборота право мыслит людей, прежде всего в качестве некоторых абстрактных центров хозяйственной жизни. Понятие субъекта прав, таким образом, есть вообще некоторое техническое, условное понятие, которое как таковое вполне применимо и к лицам юридическим»[153]. Б.В. Ельяшевич отмечал: «Представление ассоциации прав юридического лица не есть экспроприация членов в пользу какого-то нового субъекта. Добиваясь этих прав, члены союза стремятся не к умалению собственных правомочий, не к изменению своего отношения к общему имуществу, а к созданию более совершенных форм представительства … к установлению более удобных условий участия в общественной жизни»[154].

Наш современник С.И. Архипов, также являясь сторонником рассмотрения человека в качестве основы существующих субъектов права, исходит из генетической предопределенности, то есть происхождения субъектов права, являющихся итогом той правовой эманации, о которой говорил И.А. Покровский. Кроме того, субъекты

---

[151] *Архипов С.И.* Указ. соч. С. 6.
[152] Цит. по: *Архипов С.И.* Указ. соч. С. 235.
[153] Там же. С. 26.
[154] Там же. С. 235, 236.

права не только происходят от человека, но и продолжают поддерживаться его сознанием, волей и действиями. Правовые формы, в которые заключены субъекты права, играют лишь служебную роль, имеют значение и смысл лишь в связи с человеком, проявляют его правовые качества, создавая условия для обеспечения разнообразных правовых интересов человека, достижение его целей[155].

Отметим, что использование термина «лицо» для обозначения субъектов права относится к числу давних юридических понятий, « ...причем настолько важного, что его наряду с понятиями «действие» (договор), «вещь», «ответственность», «государство», «воля» можно рассматривать как системообразующее»[156], выражающее связь субъекта права с человеком. Имея целый ряд интерпретаций, этот термин является удачным, проверенным временем, выражаясь словами Г.А. Гаджиева, эластичным понятием. Прав этот автор в том, что наделение искусственного интеллекта правосубъектностью и присвоение ему статуса «лица» пока не так злободневно, потому что на современном этапе развития технологий его деятельность связана с владельцем и производителем[157].

Действительно, в распоряжении Правительства РФ от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.» (далее – Концепция) отмечается, что наиболее значимыми вопросами применения систем искусственного интеллекта и робототехники в контексте гражданско-правовых отношений являются вопросы гражданско-правовой ответственности за вред, причиненный системами искусственного интеллекта и робототехники. Реальный уровень развития технологий искусственного интеллекта и робототехники не предполагает кардинальных изменений в регулировании института юридической

---

[155] Цит. по: *Архипов С.И.* Указ. соч. С. 243.

[156] *Гаджиев Г.А.* Является ли робот-агент лицом? (Поиск правовых форм для регулирования цифровой экономики) // Журнал российского права. 2018. № 1. URL: https://cyberleninka.ru/ (дата обращения: 08.09.2023).

[157] Там же. URL: https://cyberleninka.ru/

ответственности, однако требует постепенной доработки его отдельных элементов[158]. В частности, требуется дальнейшая проработка механизмов гражданско-правовой, уголовной и административной ответственности в случае причинения вреда системами искусственного интеллекта и робототехники, имеющими высокую степень автономности, при принятии ими решений, в том числе с точки зрения определения лиц, которые будут нести ответственность за их действия, доработки при необходимости механизмов безвиновной гражданско-правовой ответственности, а также возможности использования способов, позволяющих возместить причиненный действиями систем искусственного интеллекта и робототехники вред (например, страхование ответственности, создание компенсационных фондов и др.)[159].

Обозначен в Концепции и общий вектор возможных изменений. Как отмечается в этом документе, он должен быть направлен на то, чтобы гарантировать эффективное и справедливое функционирование институтов юридической ответственности и распределение ответственности в случае такого причинения вреда[160].

«Тем не менее, – указывает Г.А. Гаджиев, – в дальнейшем, при изобретении полностью независимого (автономного) искусственного интеллекта, потребность в легитимации его статуса как юридической личности может быть актуализирована»[161]. С этим согласны и другие исследователи[162]. Следовательно, не утратит научной идентичности и востребован будет в качестве методологи-

---

[158] Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г. : распоряжение Правительства РФ от 19 августа 2020 г. № 2129-р. URL: https://www.garant.ru/ (дата обращения: 08.09.2023).

[159] Там же.

[160] Там же.

[161] *Гаджиев Г.А.* Указ. соч.

[162] См.: *Камалова Г.Г.* Некоторые вопросы уголовно-правовой ответственности в сфере применения систем искусственного интеллекта и робототехники // Вестник Удмуртского университета. Серия «Экономика и право». 2020. Т. 30, № 3. С. 382-388.

ческого основания созданный в течение многовекового развития правовой науки юридический концепт действительности – юридическая личность в контексте нашего исследования, в научной среде именуемая феноменом «электронное лицо»[163].

Библиографический список

1. Архипов С.И. Субъект права (теоретическое исследование) : дис. … д-ра. юрид. наук. – Екатеринбург, 2005.

2. Брянцева О.В., Брянцев И.И. Проблема субъектности искусственного интеллекта в системе общественных отношений // Вестник Поволжского института управления. – 2023. – Т. 23, № 3.

3. Гаджиев Г.А. Является ли робот-агент лицом? (Поиск правовых форм для регулирования цифровой экономики) [Электронный ресурс] // Журнал российского права. – 2018. – № 1. – URL: https://cyberleninka.ru/ (дата обращения: 08.09.2023).

4. Дерябо С. Личность: от субъективности к субъектности [Электронный ресурс] // Развитие личности. – 2002. – № 3. – URL: http://rl-online.ru/articles/3-02/143.html (дата обращения: 08.09.2023).

5. Камалова Г.Г. Некоторые вопросы уголовно-правовой ответственности в сфере применения систем искусственного интеллекта и робототехники // Вестник Удмуртского университета. Серия «Экономика и право». – 2020. – Т. 30, № 3.

6. Мохат П.М. Юнит искусственного интеллекта как электронное лицо [Электронный ресурс] // Вестник Московского государственного областного университета. Серия «Юриспруденция». – 2018. – № 2. – URL: https://cyberleninka.ru/ (дата обращения: 08.09.2023).

7. Никитенко С.В. Трансформация субъекта права в связи с развитием искусственного интеллекта // Научно-практические исследования. – 2020. – № 5-2 (28).

---

[163] См.: *Мохат П.М.* Юнит искусственного интеллекта как электронное лицо // Вестник Московского государственного областного университета. Серия «Юриспруденция». 2018. № 2. URL: https://cyberleninka.ru/ (дата обращения: 08.09.2023).

8. Пройдаков Э.М. Современное состояние искусственного интеллекта // Науковедческие исследования. – 2018.

9. Радченко Е.В., Ранг К.А. Понимание субъектности в философии и языкознании [Электронный ресурс] // Вестник Южно-Уральского государственного университета. – 2012. – № 2. – URL: https://cyberleninka.ru/ (дата обращения: 08.09.2023).

10. Разин А.В. Этика искусственного интеллекта [Электронный ресурс] // Философия и общество. – 2019. – № 1. – URL: https://cyberleninka.ru/ (дата обращения: 08.09.2023).

11. Степаненко А.С. Социокультурные и технологические предпосылки искусственного интеллекта [Электронный ресурс] : автореф. дис. … д-ра. философских наук. – Ростов-на-Дону, 2007. – URL: https://www.dissercat.com/ (дата обращения: 08.09.2023).

Абашева Флюра Ахунзяновна,
к.ю.н., доцент, доцент кафедры уголовного процесса
и правоохранительной деятельности ФГБОУ ВО
«Удмуртский государственный университет»,
г. Ижевск

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ КАК УСЛОВИЕ ЭФФЕКТИВНОЙ ДЕЯТЕЛЬНОСТИ СУДОВ

Общие условия эффективной организации и деятельности судов как органов судебной власти связаны с факторами политического, экономического, общесоциального и информационного порядка. Информационно-аналитическая база как одна из предпосылок эффективной организации и деятельности судебной власти представляет собой систему необходимой и достаточной информации о самой судебной власти как одной из ветвей государственной власти, о судах, непосредственно осуществляющих реализацию судебной власти, о статусе судей, а также об эффективных процедурах ее реализации и совершенствовании процедуры осуществления

правосудия. Подготовленность реализации судебной деятельности, а именно степень организованности и скоординированности этой деятельности, наличие необходимых сил и средств, разработке современных научных рекомендаций и овладение ими. Используемая в реализации судебной деятельности информация включает в себя материалы статистики, нормативные документы и данные о практике их применения, научные обобщения. Большое количество разнообразных сведений циркулирует также внутри судебной системы, между судами и гражданами Потоки информации могут быть как целенаправленными, регулируемыми, так и складывающимися стихийно. По-разному решаются вопросы информационного обеспечения в разных субъектах Российской Федерации.

В условиях усиленного развития и усложнения социально-экономических отношений в большинстве правопорядков существенно возрастает нагрузка на судебные органы, в результате чего многие участники, при наличии формальной возможности обратиться в суд, оказываются лишенными реального доступа к правосудию. Научно-технический прогресс сегодня является одной из основных причин кардинальных изменений во всех сферах общественной жизни. Информационные технологии прочно укрепились в быту, проникли в банковскую деятельность, медицину, образование. Исключением не является и правосудие, причем в указанном русле развивается информатизация не только использования правовой базы, но и отдельных институтов всех видов судопроизводства. В основополагающих документах развития судебной системы последних лет ставится задача создания мобильного правосудия, электронного правосудия, внедрения программных средств аналитического обеспечения деятельности, осуществления всех поступающих в суды документов, формирования электронных дел, электронного архива суда. Для руководства судебных органов ставится в обязанность организовать разработку, внедрение и обеспечение программно-аппаратных средств, необходимых для ведения судопроизводства и делопроизводства, а также информационно-правового обеспечения судебной деятельности. Однако необходимо

отметить, использование судами новых инструментов не означает, что их природа и функция должны измениться.

С развитием информационных технологий рассмотрение многочисленных фактически бесспорных и (или) мелких дел может осуществляться при помощи специализированных алгоритмов без непосредственного участия судьи.

Внедрение информационных технологий способно ускорить судопроизводство, сократить нагрузку на аппарат суда и судей, снизить стоимость процедур, повысить уровень открытости судебной системы. При этом могут быть выделены два основных подхода к информатизации судебной системы – оптимизация процессов и трансформация самих судебных процедур.

При *оптимизации* существующие процедуры воспринимаются в качестве необходимых и согласованных. Внедрение информационных технологий в первую очередь позволит существенно сократить временные и трудовые затраты на выполнение повторяющихся, рутинных процессов, характерных для различных этапов судопроизводства.

Основными элементами данной оптимизации являются: внедрение систем электронной подачи документов и онлайн-взаимодействия сторон спора и судьи, расширение практики применения систем видео-конференц-связи, внедрение систем автоматического протоколирования судебных заседаний.

Трансформация судопроизводства, в свою очередь, предполагает внедрение новых технологий и процедур. Речь идет в том числе об отказе от проведения очных слушаний по широкому перечню мелких и бесспорных дел. Данная точка зрения является, по сути, развитием концепции письменного (заочного) производства, которое позволяет судам более эффективно расходовать финансовые и трудовые ресурсы в зависимости от значимости спора. На первом этапе очные судебные заседания могут быть заменены асинхронным взаимодействием сторон спора и судьи на базе специализированной интернет-платформы.

Наиболее значимым средством преодоления проблем является внедрение системы онлайн-заполнения исковых заявлений (хода-

тайств) независимо от инстанции, которая рассматривает спор. В общем объеме судебных споров определенной категории может быть разработана модель оптимального разрешения.

Такое структурирование процесса судебного разбирательства уже на начальном этапе может обеспечить отсечение наименее обоснованных споров. Также поступление информации в заданном формате и исключение необязательных документов снизит фактическую нагрузку на соответствующие органы.

Внедрение информационных технологий в процесс правоприменения позволяет сделать его интуитивно понятным и, как следствие, менее затратным – как минимум в силу возможности исключения излишних процедур и расходов на профессионального представителя.

В целом оценка уровня развития информационных технологий в сфере профилактики и уменьшения споров может осуществляться с использованием следующих механизмов:

– подача искового заявления в суд в электронном виде;

– разработанные формы подачи исковых требований, руководства по их заполнению, схемы, отражающие последовательность действий в процессе разрешения споров в судебном порядке;

– платформы для онлайн-переговоров или онлайн-посредничества;

– платформы для электронного обмена документами (доказательствами) между сторонами;

– наличие эффективно действующих онлайн-институтов внесудебного урегулирования споров.

Оптимизация судебных процедур рассмотрения судебных споров вследствие информатизации предполагает исключение хоть и традиционных, но в контексте цифровизации избыточных элементов судопроизводства.

Оптимизация судебных процедур рассмотрения спора в рамках так называемых длящихся онлайн-слушаний. При таких слушаниях судья и представители сторон в течение определенного периода времени имеют возможность знакомиться с имеющимися материалами дела, комментировать их, корректировать собственную

позицию, запрашивать и предоставлять недостающие доказательства, разрешать выявленные спорные ситуации. В настоящее время стороны спора по закону обязаны обмениваться соответствующими документами до начала судебного разбирательства. Однако на стадии судебного разбирательства взаимодействие участников спора и обмен документами происходит преимущественно во время предварительных судебных заседаний.

Внедрение возможности официального онлайн-взаимодействия сторон спора после начала судебного разбирательства должно стать логичным продолжением данной практики. Процедурное упрощение судопроизводства позволит обеспечить более высокий уровень осознанности совершаемых действий и, как следствие, более вероятным станет примирение сторон, а также снизится потребность в услугах профессиональных представителей.

Что касается оптимизации непосредственно объема судебной работы судей, то в данном случае выглядит актуальным и своевременным расширение применения при рассмотрении дела и вынесении решения систем, основанных на технологиях искусственного интеллекта.

Важно еще раз отметить, что при недостаточности предлагаемых процедур рассмотрение дела может осуществляться в традиционной форме, однако изначальное использование онлайн-процедур по умолчанию позволит сократить время, необходимое судье и сторонам спора для ознакомления с материалами дела и уточнения позиций.

Меры, предусмотренные обозначенными выше подходами к информатизации судебной системы, на практике могут рассматриваться как взаимодополняющие, как это предусмотрено, например, концепцией расширения судов. В рамках данной концепции расширение реального доступа к правосудию может быть достигнуто путем реформирования технологий правового просвещения граждан, стимулирования практики «избегания» (профилактики) и деэскалации споров на ранней стадии, оптимизации судебных процедур.

Исследования показывают, что в значительном числе случаев восстановлению нарушенных прав препятствует незнание лицами своих прав и доступных механизмов защиты. По статистике, менее

трети лиц способны осознать юридический характер возникающих споров – как правило, проблемные ситуации воспринимаются либо как нечто неизбежное, либо как результат «невезения».

Развитие информационных технологий, при условии обеспечения эффективных институциональных гарантий устранения возникающих ошибок и нарушений процессуальных прав, позволяет развивать практику дистанционного рассмотрения дел.

В России безусловным лидером по динамике развития систем электронного документооборота является система арбитражных судов, характеризующаяся использованием передовых разработок в области информационных технологий. Возможность подачи исков и размещения документов в электронной форме предусмотрена в арбитражном процессе, вне зависимости от типа судопроизводства и инстанции, и реализуется через специализированный сервис «Мой арбитр». При подаче документов происходит их предварительная проверка с возможностью повторной отправки отклоненных документов. В целях обеспечения безопасности подаваемые документы могут подписываться усиленной квалифицированной электронной подписью. Участникам споров также доступна опция подписки на уведомления об изменениях по делу. В качестве еще одной иллюстрации внедрения инноваций в данной сфере необходимо сказать, что с января 2020 г. в России проводится эксперимент по предоставлению сторонам возможности ознакомления с материалами дела в электронном виде. Доступ предоставляется не только к материалам, поступившим в электронном виде через систему «Мой арбитр», но и к печатным документам, отсканированным канцелярией суда, а также аудиозаписям судебных заседаний. В ближайшее время планируется запуск сервиса, облегчающего составление электронных документов, системы автоматизации стандартизированных функций сотрудников судебного аппарата, роботизации рассмотрения наиболее простых дел и др.

Однако следует отметить, что в последние годы наблюдается достаточно динамичное развитие электронных сервисов в судах общей юрисдикции. Наиболее успешным примером является

Официальный портал судов общей юрисдикции г. Москвы и Портал Единого информационного пространства мировых судей г. Москвы.

Библиографический список

1. Жукова Е.Н. Оптимизация судопроизводства в условиях развития информационных технологий // Актуальные проблемы организации правоохранительной и правозащитной деятельности : материалы Всерос. науч.-практ. конф., Тула, 06 февраля 2021 года. – Тула : Тульский ин-т (филиал) ФГБОУ ВО «Всерос. гос. ун-т юстиции» (РПА Минюста России), 2021. – С. 199-205.

2. Потапов Д.В., Потапова Л.В. Внедрение информационных технологий в современное судопроизводство // The Scientific Heritage. – 2021. – № 64-4(64). – С. 7-10.

3. Смецкой Р.Е. Информационные технологии в судопроизводстве // Молодой ученый. – 2023. – № 21(468). – С. 337-339.

Маслова Татьяна Николаевна,
старший помощник прокурора Вахитовского района города Казани прокуратуры Республики Татарстан, младший советник юстиции
г. Казань

НАДЗОРНАЯ ДЕЯТЕЛЬНОСТЬ ЗА ПРОЦЕССОМ РЕАЛИЗАЦИИ МЕЖОТРАСЛЕВОЙ СИСТЕМЫ МЕР БЕЗОПАСНОСТИ УЧАСТНИКОВ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Безопасность личности в современном уголовном процессе направлена на установление дополнительных гарантий защиты прав и законных интересов лиц, вовлекаемых в производство по уголовному делу[164]. Процесс обеспечения безопасных условий участия

[164] См.: *Епихин А.Ю.* Правовые основы безопасности личности и уголовного судопроизводства в отдельных международных документах //

в производстве по уголовному делу обусловлен многочисленными проблемными ситуациями, носит межотраслевой характер. Согласно положениям ст. 37 УПК РФ на прокурора возлагается 1) уголовное преследование и 2) прокурорский надзор за проведением дознания и предварительного следствия, то есть процессуальной деятельности, в которой могут применяться меры безопасности в отношении участников процесса (ч. 3 ст. 11 УПК РФ).

Прокурорский надзор, согласно разделу III ФЗ от 17.01.1992 «О прокуратуре Российской Федерации», осуществляется по четырём основным направлениям:

1. Надзор за исполнением законов.

2. Надзор за соблюдением прав и свобод человека и гражданина.

3. Надзор за исполнением законов органами ОРД, дознания и предварительного следствия.

4. Надзор за исполнением законов администрациями органов и учреждений, исполняющих наказание и назначаемые судом меры принудительного характера, администрациями мест содержания задержанных и заключенных под стражу[165].

Существует множество определений термина «прокурорский надзор». В рамках данной работы предлагается исходить из того, что под прокурорским надзором будет пониматься определённая законом деятельность органов и должностных лиц прокуратуры, направленная на создание и поддержание состояния законности, обнаружение и немедленное устранение нарушений закона, а также

Международное уголовное право и международная юстиция. 2012. № 2. С. 12-14; *Епихин А.Ю.* Концепция безопасности личности в уголовном судопроизводстве. Сыктывкар, 2004; *Епихин А.Ю.* Законодательство зарубежных стран, обеспечивающее безопасность участников уголовного судопроизводства : лекция. Сыктывкар, 2003; *Епихин А.Ю.* Общие условия эффективности функционирования безопасности личности в уголовном судопроизводстве // Уголовное право. 2003. № 4. С. 69-70.

[165] О прокуратуре Российской Федерации : Федеральный закон от 17.01.1992 № 2202-1 // Собрание законодательства РФ. 20.11.1995. № 47, ст. 4472.

на формирование условий для предупреждения возможных правонарушений.

Тематика мер безопасности является относительно молодой в истории правового развития России. Впервые на необходимость ограждения участников уголовного судопроизводства от негативного посткриминального воздействия на высшем уровне обратил внимание Закон СССР от 25.12.1958 «Об утверждении основ уголовного законодательства союза ССР и союзных республик»[166].

Другими значимыми актами, продолжившими развитие института мер безопасности в законодательстве нашей страны, являются Закон РФ от 18.04.1991 «О милиции»[167] и ФЗ РФ от 12.08.1995 «Об оперативно-розыскной деятельности в Российской Федерации»[168]. Вслед за ними стоит упомянуть ФЗ от 20.04.1995 «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»[169] и ФЗ от 20.04.2004 «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»[170]. Не стоит забывать и про Конституцию РФ 1993 г., УПК РФ, а также ряд иных федеральных законов, имеющих прямое отношение к реализации правового института мер безопасности. Прежде всего под этими федеральными законами подразумеваются правовые акты, регламентирующие правовой

---

[166] *Красавина Д.Д.* Формирование правовой основы обеспечения безопасности участников уголовного судопроизводства в российском законодательстве // Вестник юридического факультета Южного федерального университета. 2019. № 2.

[167] О милиции : Закон Российской Федерации от 18.04.1991 № 1026-1 // Ведомости СНД и ВС РСФСР. 18.04.1991. № 16, ст. 503. Утратил силу.

[168] Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ // Собрание законодательства РФ. 14.08.1995. № 33, ст. 3349.

[169] О государственной защите судей, должностных лиц правоохранительных и контролирующих органов : Федеральный закон от 20.04.1995 № 45-ФЗ // Собрание законодательства РФ. 24.04.1995. № 17, ст. 1455.

[170] О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства : Федеральный закон от 20.08.2004 № 119-ФЗ // Собрание законодательства РФ. 23.08.2004. № 34, ст. 3534.

статус и полномочия отдельных государственных органов, например полиции, прокуратуры, следственного комитета РФ и судов. Они особенно важны, поскольку вышеперечисленные структуры принимают непосредственное участие в процессе избрания и применения мер безопасности.

Вопрос о понятии и разновидностях мер безопасности участников уголовного судопроизводства вызывает определенные дискуссии[171]. Отметим, что в ч. 3 ст. 11 УПК РФ отсутствует легальное определение мер безопасности, однако сами меры перечислены:

1. Право следователя не приводить в протоколе следственного действия данные о личности некоторых участников уголовного процесса (ч. 9 ст. 166 УПК РФ).

2. Контроль и запись телефонных и иных переговоров по заявлению участников уголовного процесса или решению суда (ч. 2 ст. 186 УПК РФ).

3. Право следователя проводить предъявление для опознания в условиях, при которых опознающий остаётся вне пределов видимости опознаваемого (ч. 8 ст. 193 УПК РФ).

4. Закрытое судебное разбирательство при наличии определения или постановления суда (п. 4 ч. 2 ст. 241 УПК РФ).

5. Допрос свидетеля в условиях, при которых он остаётся вне пределов видимости других участников уголовного процесса, а данные о его личности не оглашаются (ч. 5 ст. 278 УПК РФ).

6. Иные меры безопасности, предусмотренные законодательством.

Приведённые меры ставят своей целью обеспечение безопасности участников уголовного судопроизводства, а также их защиту от угроз совершения против них и их близких опасных противоправных деяний, о чём говорится в тексте самих статей. Это правило распространяется и на иные меры безопасности, не указанные

---

[171] *Журба О.Л., Лысенко Я.В.* Понятие и сущность института обеспечения безопасности участников уголовного судопроизводства // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2020. № 2.

в этой норме. Например, для обеспечения безопасности участника процесса – возможность заключения под стражу, выделение уголовного дела в отдельное производство, изменение подсудности дела, проведение следственного действия с применением видео-конференц-связи и пр.

В настоящее время к иным мерам безопасности можно с уверенностью отнести меры, содержащиеся в ст. 6 ФЗ от 20.04.1995 «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и ст. 5 ФЗ от 20.04.04 «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», так как они прямо поименованы в качестве таковых.

Более дискуссионным является вопрос об отнесении к мерам безопасности мер пресечения[172]. С одной стороны, п. 3 ч. 1 ст. 97 УПК РФ даёт повод это сделать, ибо меры пресечения могут быть назначены подозреваемому и обвиняемому, если они угрожают участникам уголовного судопроизводства. С другой стороны, тот же п. 3 ч. 1 ст. 97 УПК РФ сводит применение мер пресечения только к случаям воспрепятствования производству по уголовному делу. То есть законодатель отдаёт предпочтение не безопасности участников уголовного процесса, а стабильному ходу расследования. Конечно, нельзя отрицать, что безопасность участников уголовного процесса этому не способствует, однако нужно помнить и об особенностях самих уголовных дел. Например, при расследовании дел об убийстве, когда личность умершего, его родственников и близких установить невозможно, а должностным лицам никто не угрожает, тяжело представить, безопасность какого участника судопроизводства будут обеспечивать меры пресечения.

---

[172] См.: *Епихин А.Ю.* Заключение под стражу как средство обеспечения безопасности участников уголовного судопроизводства // Судебная защита прав и свобод человека и гражданина при применении мер пресечения в виде заключения под стражу, залога и домашнего ареста : материалы Всерос. межведомственной науч.-практ. конф. Нижегородский областной суд ; отв. ред. В.Ф. Попов. Нижний Новгород, 2011. С. 88-94.

При анализе ч. 1 ст. 97 УПК РФ целесообразным видится вывод о том, что меры пресечения обладают смешанным характером. Бесспорно то, что при правовой регламентации мер пресечения законодатель предполагал их использование в качестве мер безопасности. Между тем очевидно, что основной акцент законодателем был сделан на обеспечение стабильности производства по уголовному делу. Думается, что теоретическая позиция о том, что меры пресечения являются наиболее строгой разновидностью мер государственного принуждения[173], подтверждает эту точку зрения.

Что касается взглядов учёных на терминологию в сфере мер безопасности, то они выглядят более конкретными, чем установки законодателя. Так, А.А. Юнусов утверждает, что обеспечение безопасности участников уголовного судопроизводства состоит в деятельности, создающей для них условия отсутствия угрозы жизни и здоровью или нивелирующей существующую опасность[174]. Л.В. Брусницын ссылается на то, что меры безопасности должны обеспечивать защиту лиц, содействующих правосудию, вместе с их родственниками на разных этапах уголовного судопроизводства, начиная от оперативно-розыскной деятельности, заканчивая исполнительным производством. При этом защищать упомянутых субъектов необходимо не только от уголовно наказуемых форм воздействия, но и от иных[175].

Перечисленные мнения ученых позволяют включить в список мер безопасности выделение уголовного дела в отношении несовершеннолетнего в отдельное производство (ст. 422 УПК РФ), а также заключение досудебного соглашения о сотрудничестве (гл. 40.1 УПК РФ). В первом случае несовершеннолетний, обладая

---

[173] *Тройнина И.С.* Понятие и система мер пресечения в российском уголовно-процессуальном законодательстве // Вестник ВГУ. Сер. «Право». 2010. № 1.

[174] *Юнусов А.А.* Обережение участников уголовного процесса и их ближних. URL: https://www.dissercat.com/content/ (дата обращения: 30.11.2022).

[175] *Брусницын Л.В.* Обеспечение безопасности лиц, содействующих уголовному правосудию: российский, зарубежный и международный опыт XX века (процессуальное исследование). М. : Юрлитинформ, 2001. 400 с.

повышенной внушаемостью в силу возраста, получает защиту от влияния на него совершеннолетних участников уголовного процесса. Во втором случае лицо, заключившее досудебное соглашение о сотрудничестве, может быть защищено от негативного влияния других фигурантов уголовного дела. Более того, ст. 317.9 УПК РФ предусматривает, что на лиц, заключивших данное соглашение, распространяются все меры защиты, предусмотренные Федеральным законом от 20.04.04 «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства». Фактически досудебное соглашение о сотрудничестве является документом, предваряющим применение мер безопасности к участнику уголовного процесса.

Кроме этого, к мерам безопасности допустимо относить отдельные нормы из УК РФ. С известной долей оговорок в качестве меры безопасности выступает условное осуждение. Согласно ч. 3-7 ст. 73 УК РФ условное осуждение подразумевает наличие для условно осуждённого испытательного срока и исполнение определённых обязанностей, за выполнением которых устанавливается контроль. В случае, если осуждённый не исполняет эти обязанности надлежащим образом, то, согласно ч. 2-5 ст. 74 УК РФ, суд может продлить испытательный срок или вовсе отменить его, вынеся решение об исполнении наказания. При наличии подобного механизма появляется реальная возможность воздействовать на поведение обвиняемого. Из-за неблагоприятных для него последствий нарушения норм об условном осуждении вероятность противоправного воздействия на других участников уголовного процесса снижается.

Продолжая ориентироваться на трактовки А.А. Юнусова и Л.В. Брусницына, к мерам безопасности также можно причислить меры принудительного медицинского характера. Так, ч. 1-2 ст. 97 УК РФ связывают случаи назначения данных мер с тем, что лица, к которым они применяются, опасны для себя и общества или потенциально могут создать иные существенные вредные последствия. В качестве одной из целей применения к лицам принудительных мер медицинского характера УК РФ в ст. 98 называет преду-

преждение совершения данными лицами последующих противоправных деяний. Исходя из этого, можно утверждать, что эта норма отвечает научным представлениям о сущности мер безопасности. Помимо перечисленных норм УК РФ содержит две «специальные» статьи, прямо направленные на уголовно-правовую превенцию разглашения сведений о мерах государственной защиты участников уголовного процесса (ст. 311 и 320 УК РФ).

Таким образом, институт безопасности личности в уголовном процессе имеет межотраслевой характер; меры защиты обусловлены возможным наличием противоречий. В процессуальной деятельности дознавателя, следователя, прокурора и суда возможность применения различных правовых средств обеспечения безопасности имеет важное значение.

Библиографический список

1. Брусницын Л.В. Обеспечение безопасности лиц, содействующих уголовному правосудию: российский, зарубежный и международный опыт XX века (процессуальное исследование). – М. : Юрлитинформ, 2001. – 400 с.

2. Епихин А.Ю. Заключение под стражу как средство обеспечения безопасности участников уголовного судопроизводства // Судебная защита прав и свобод человека и гражданина при применении мер пресечения в виде заключения под стражу, залога и домашнего ареста : материалы Всерос. межведомственной науч.-практ. конф. Нижегородский областной суд ; отв. ред. В.Ф. Попов. – Нижний Новгород, 2011. – С. 88-94.

3. Епихин А.Ю. Законодательство зарубежных стран, обеспечивающее безопасность участников уголовного судопроизводства : лекция. – Сыктывкар, 2003.

4. Епихин А.Ю. Концепция безопасности личности в уголовном судопроизводстве. – Сыктывкар, 2004.

5. Епихин А.Ю. Общие условия эффективности функционирования безопасности личности в уголовном судопроизводстве // Уголовное право. – 2003. – № 4. – С. 69-70.

6. Епихин А.Ю. Правовые основы безопасности личности и уголовного судопроизводства в отдельных международных документах // Международное уголовное право и международная юстиция. – 2012. – № 2. – С. 12-14.

7. Журба О.Л., Лысенко Я.В. Понятие и сущность института обеспечения безопасности участников уголовного судопроизводства // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2020. – № 2.

8. Красавина Д.Д. Формирование правовой основы обеспечения безопасности участников уголовного судопроизводства в российском законодательстве // Вестник юридического факультета Южного федерального университета. – 2019. – № 2.

9. Тройнина И.С. Понятие и система мер пресечения в российском уголовно-процессуальном законодательстве // Вестник ВГУ. Серия «Право». – 2010. – № 1.

10. Юнусов А.А. Обережение участников уголовного процесса и их ближних [Электронный ресурс]. – URL: https://www.dissercat.com/content/ (дата обращения: 30.11.2022).

Ибрагимова Алиса Мансуровна,
старший преподаватель кафедры основ организации и управления в органах прокуратуры Казанского юридического института (филиала) Университета прокуратуры Российской Федерации, г. Казань

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ОБЖАЛОВАНИЯ

Указом Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» закреплена система взглядов в информационной сфере, определяющих основные направления деятельности субъектов информационной сферы, в том числе в вопросах безопасности.

Анализ положений данного нормативно-правового акта позволяет сделать вывод, что информационная безопасность призвана обеспечить интересы государства, общества и отдельно взятой личности в различных сферах при работе субъектов информационной сферы с информацией, объектами информатизации, информационными системами, сайтами в сети Интернет, сетями связи, информационными технологиями.

В настоящее время ни одна сфера деятельности не осталась не затронутой достижениями в сфере информационных технологий. Не осталось в стороне и уголовное судопроизводство.

В юридической литературе идут бурные обсуждения о перспективах перехода к электронному уголовному делу, прорабатываются различные модели формирования электронных уголовных дел[176], а также предлагаются возможные варианты, используемые зарубежными странами[177].

Вместе с тем наше отечественное уголовно-процессуальное законодательство содержит небольшое количество норм, регламентирующих возможности использования информационных технологий в уголовном судопроизводстве (видео-конференц-связь, аудиопротоколирование, использование электронных документов).

Действующее уголовно-процессуальное законодательство закрепляет важнейшее средство реализации назначения уголовного процесса – возможность электронного обращения в судебные

---

[176] См., например: *Лебедев З.С.* Электронное уголовное дело как форма уголовного судопроизводства: способ реализации и перспективы внедрения // Научный дайджест Восточно-Сибирского института МВД России. 2020. № 2 (5). С. 41; *Каменев А.С.* Перспективы внедрения электронного уголовного дела и его влияние на осуществление функции защиты // Вестник Южно-Уральского гос. ун-та. Сер. «Право». 2022. Т. 22, № 4. С. 24; *Шереметьев И.И.* Электронное уголовное дело: что это такое и пути его создания // Lex Russica (Русский закон). 2020. Т. 73, № 10 (167). С. 87; *Гимазетдинова И.Н.* Уголовное дело как комплексный процессуальный акт и возможность его перевода в электронный формат // Вестник Волгоградской академии МВД России. 2023. № 2 (65). С. 74.

[177] Информационные технологии в уголовном процессе зарубежных стран : монография / под ред. д-ра. юрид. наук С.В. Зуева. М., 2020. С. 4-8.

органы по уголовным делам. Так, ст. 474.1 УПК РФ регламентирует подачу ходатайства, заявления, жалобы и представления в суд в форме электронного документа. В юридической литературе есть мнение, что возможность подачи жалоб, представлений и иных обращений в форме электронного документа допускается при условии соблюдения общих требований к порядку и срокам подачи документов в судебный орган[178].

Но следует обратить внимание, что статья конкретизирует условия правомерности такого обращения:

– отсутствие в документе сведений, составляющих охраняемую федеральным законом тайну. По нашему мнению, необходимость данного условия обусловлена принятием дополнительных правовых мер противодействия угрозам в информационной сфере, способным привести к хищению, уничтожению, блокированию, модификации содержащейся такого рода информации в жалобе, представлении и ином обращении в уголовном судопроизводстве в форме электронного документа;

– подача обращения, включая уголовно-процессуальную жалобу, через Единый портал государственных и муниципальных услуг (функций);

– подписание электронного документа усиленной квалифицированной электронной подписью, за исключением отдельных видов обращений.

В то же время ч. 3 ст. 474.1 УПК РФ допускает использование простой электронной подписи при подаче:

ходатайства об ознакомлении с материалами уголовного дела;

ходатайства о получении копий процессуальных документов, информации об участии в судебных заседаниях как очно, так и с использованием систем видео-конференц-связи;

---

[178] *Канунникова Н.Г.* К вопросу о современном состоянии реализации электронного документа в ходе уголовного судопроизводства // Интеграция мировой науки и техники: новые концепции и парадигмы : материалы II Междунар. науч.-практ. конф., Ставрополь, 28 февраля 2023 года. Ставрополь, 2023. С. 435.

гражданского иска, не содержащего ходатайства о принятии мер по обеспечению возмещения вреда, причиненного преступлением либо возможной конфискации имущества.

Тем самым УПК РФ допускает возможность подачи жалоб и представлений в форме электронного документа, подписанных усиленной квалифицированной электронной подписью.

Анализ норм уголовно-процессуального законодательства свидетельствует о том, что данная статья является одной из первых среди норм, которая закрепляет внедрение в уголовное судопроизводство современных достижений информационных технологий. Однако отсутствие правового регулирования применения возможностей информационных технологий в иных сферах уголовного судопроизводства, а также диспозитивности применения электронного документооборота в вопросах обжалования с оговоркой «при наличии технической возможности» говорит о фрагментарности правового регулирования вопросов электронного уголовного судопроизводства[179]. В то же время появление в УПК РФ нормы, регулирующей использование достижений информационных технологий, исключительно в вопросе подачи ходатайств, жалоб, заявлений, представлений, свидетельствует о широте использования этих инструментов в уголовном судопроизводстве и значимости возникающих в связи с их подачей правоотношений.

В настоящее время возможность подачи документов в электронной форме в суд активно используется среди населения.

Однако есть и факторы, наличие которых не позволяет говорить о полноценной реализации возможности подачи уголовно-процессуальных жалоб в форме электронного документа. Остановимся на основных недостатках.

Из содержания ст. 474.1 УПК РФ следует, что электронные жалобы и иные уголовно-процессуальные обращения подаются в суд. В то же время сама статья находится в разделе, посвященном

---

[179] *Долгополов К.А., Иванов С.А.* Цифровизация уголовного правосудия: проблемы и перспективы // International Law Journal. 2022. Т. 5, № 3. С. 34.

использованию в уголовном судопроизводстве электронных документов и бланков процессуальных документов. Справедливо будет сказано, что в приведенной ситуации наблюдается несовершенство законодательной техники.

На практике возможности электронного документооборота в несудебных органах уголовного судопроизводства широко внедряются. Возможности информационных технологий используются при подаче, приёме сообщений о преступлениях, жалоб на действия (бездействие) и решения несудебных органов и их должностных лиц в сфере уголовного судопроизводства.

Существуют ведомственные организационно-распорядительные документы, посвященные работе с электронными обращениями, являющимися и электронными уголовно-процессуальными жалобами. В Инструкции по делопроизводству в органах и организациях прокуратуры Российской Федерации, утвержденной приказом Генерального прокурора РФ от 29.12.2011 № 450[180] содержится раздел, посвященный особенностям работы с электронными документами.

Однако УПК РФ не содержит особенности работы с электронными документами в целом, как и с электронными обращениями, уголовно-процессуальными жалобами; не конкретизирует порядок направления жалоб и иных обращений уголовно-процессуального характера в органы предварительного расследования, прокуратуру в форме электронного документа, условия их приемлемости для приема и рассмотрения.

Вместе с тем актуальность такого способа «общения» в рамках уголовного судопроизводства объективна. Неоднократно отмечались позитивные факторы использования электронного документооборота[181]. Это и ускорение уголовного судопроизводства, и эко-

---

[180] О введении в действие Инструкции по делопроизводству в органах и организациях прокуратуры Российской Федерации : приказ Генпрокуратуры России от 29.12.2011 № 450 (ред. от 16.09.2022) (документ опубликован не был) // СПС «КонсультантПлюс» (дата обращения: 03.09.2023).

[181] См., например: *Макарова О.В.* Совершенствование судопроизводства путем внедрения электронной формы уголовного дела // Журнал

номия материально-технических ресурсов, и упрощение делопроизводства в органах государственной власти.

Отсутствие единого правового регулирования подачи электронных жалоб и иных обращений в уголовном судопроизводстве создает практику, при которой возникают ситуации невозможности их рассмотрения.

К примеру, в органы прокуратуры Российской Федерации электронные жалобы, которые относятся и к сфере уголовного судопроизводства, поступают по различным каналам связи, наиболее широко из которых используются специальный государственный интернет-портал (ЕПГУ); внедренный с мая 2020 года СПО ЕПП, через открытый контур которого граждане могут направлять электронные обращения и электронные жалобы уголовно-процессуального характера; электронная почта.

Отсутствие четкой правовой регламентации порядка и способа подачи обращений, в том числе уголовно-процессуальных жалоб, позволяет в настоящее время неинформированным лицам подавать их, используя электронную почту организации, иногда и без указания данных, позволяющих идентифицировать заявителя и связаться с ним при отсутствии недостающих сведений. Это также порождает угрозы информационной безопасности, так как электронная почта позволяет прикрепить любой файл, который может быть вредоносным, способным вывести из строя всю систему объектов информатизации. Более того, такое состояние может привести к хищению, уничтожению, модификации информации, находящейся в информационных базах и системах.

Таким образом, решение вопросов информационной безопасности в уголовно-процессуальном обжаловании напрямую зависит

российского права. 2019. № 2 (266). С. 162; *Алимова А.А.* Электронная форма уголовного дела // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : сб. материалов, Воронеж, 21 мая 2020 года. Том Часть 1. Воронеж, 2020. С. 11; *Пастухов П.С.* Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве // Пермский юридический альманах. 2023. № 6. С. 529.

от унификации требований к порядку использования электронного документооборота во всех инстанциях уголовного судопроизводства.

Отдельный аспект усиления конфиденциальности электронного документооборота может быть связан с применением мер безопасности участников уголовного судопроизводства. В документах могут содержаться сведения о защищаемых лицах, мерах безопасности и иных аспектах защитного процесса[182].

Именно поэтому считаем необходимым использование единого программно-технического решения для обеспечения информационной безопасности всей системы обжалования в уголовном судопроизводстве на всех его стадиях. Полагаем, что наиболее отвечающим этой задаче решением является Единый портал государственных и муниципальных услуг (функций).

Но для этого необходимо принятие дополнительных правовых мер.

В качестве первоочередной такой меры для обеспечения информационной безопасности считаем необходимым включить правило в гл. 16 УПК РФ, а именно в ст. 123 УПК РФ, которая позволяла бы обжаловать действия, бездействия, решения властных субъектов в уголовном судопроизводстве аналогично ст. 474.1 УПК РФ путем подачи электронного документа через Единый портал государственных и муниципальных услуг при наличии подтвержденных в системе персональных данных пользователя.

Библиографический список

1. Алимова А.А. Электронная форма уголовного дела // Преступность в СНГ: проблемы предупреждения и раскрытия преступ-

[182] См.: *Ефихин А.Ю.* Правовые основы безопасности личности и уголовного судопроизводства в отдельных международных документах // Международное уголовное право и международная юстиция. 2012. № 2. С. 13; *Ефихин А.Ю.* Концепция безопасности личности в уголовном судопроизводстве. Сыктывкар, 2004. С. 20; *Ефихин А.Ю.* Законодательство зарубежных стран, обеспечивающее безопасность участников уголовного судопроизводства : лекция. Сыктывкар, 2003. С. 9; *Ефихин А.Ю.* Общие условия эффективности функционирования безопасности личности в уголовном судопроизводстве // Уголовное право. 2003. № 4. С. 70.

лений : сб. материалов, Воронеж, 21 мая 2020 года. Том Часть 1. – Воронеж : Воронежский ин-т МВД РФ, 2020. – С. 10-12.

2. Гимазетдинова И.Н. Уголовное дело как комплексный процессуальный акт и возможность его перевода в электронный формат // Вестник Волгоградской академии МВД России. – 2023. – № 2 (65). – С. 70-75.

3. Долгополов К.А., Иванов С.А. Цифровизация уголовного правосудия: проблемы и перспективы // International Law Journal. – 2022. – Т. 5, № 3. – С. 31-37.

4. Епихин А.Ю. Законодательство зарубежных стран, обеспечивающее безопасность участников уголовного судопроизводства : лекция. – Сыктывкар, 2003.

5. Епихин А.Ю. Концепция безопасности личности в уголовном судопроизводстве. – Сыктывкар, 2004.

6. Епихин А.Ю. Общие условия эффективности функционирования безопасности личности в уголовном судопроизводстве // Уголовное право. – 2003. – № 4. – С. 69-70.

7. Епихин А.Ю. Правовые основы безопасности личности и уголовного судопроизводства в отдельных международных документах // Международное уголовное право и международная юстиция. – 2012. – № 2. – С. 12-14.

8. Информационные технологии в уголовном процессе зарубежных стран : монография / под ред. д-ра. юрид. наук С.В. Зуева. – М. : Юрлитинформ, 2020. – 216 с.

9. Каменев А.С. Перспективы внедрения электронного уголовного дела и его влияние на осуществление функции защиты // Вестник Южно-Уральского государственного университета. Серия «Право». – 2022. – Т. 22, № 4. – С. 21-26.

10. Канунникова Н.Г. К вопросу о современном состоянии реализации электронного документа в ходе уголовного судопроизводства // Интеграция мировой науки и техники: новые концепции и парадигмы : материалы II Междунар. научн.-практ. конф., Ставрополь, 28 февраля 2023 года. – Ставрополь : ООО «Ставропольское издательство «Параграф»», 2023. – С. 434-437.

11. Лебедев З.С. Электронное уголовное дело как форма уголовного судопроизводства: способ реализации и перспективы внедрения // Научный дайджест Восточно-Сибирского института МВД России. – 2020. – № 2 (5). – С. 37-41.

12. Макарова О.В. Совершенствование судопроизводства путем внедрения электронной формы уголовного дела // Журнал российского права. – 2019. – № 2 (266). – С. 159-168.

13. Пастухов П.С. Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве // Пермский юридический альманах. – 2023. – № 6. – С. 521-540.

14. Шереметьев И.И. Электронное уголовное дело: что это такое и пути его создания // Lex Russica (Русский закон). – 2020. – Т. 73, № 10 (167). – С. 81-90.

Семакина Алсу Валерьевна,
к.г.н., доцент, доцент кафедры экологии и природопользования
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск.
Зуев Альберт Марселевич,
ученик ЧУ СОШ «Столичный-КИТ»,
г. Москва

СЕРВИС ПО АВТОМАТИЧЕСКОЙ ЗАЩИТЕ ОТ ПРИСУТСТВИЯ НЕЖЕЛАТЕЛЬНЫХ БОТОВ В TELEGRAM-ГРУППАХ

Правила доступа к информации, сбора, распространения информации регламентированы Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). Наряду с проблемой несанкционированного доступа к информации[183], к проблемам

[183] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка)

информационной безопасности относятся и спам-атаки. Спам-атаки – телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя[184]. Косвенно регламентируют правила рассылки сообщений (в т.ч. телематических электронных сообщений) Федеральные законы № 38-ФЗ «О рекламе» от 13.03.2006 и № 152-ФЗ «О персональных данных» от 27.07.2006 (ред. от 06.02.2023). В обоих законах четко указано, что рассылка должна производиться только с согласия получателя. Распространение рекламы по сетям электросвязи в отсутствие предварительного согласия абонента на получение рекламных сообщений не допускается (ч. 1 ст. 18 закона № 38-ФЗ, п. 1 ст. 3 закона № 152-ФЗ).

Таким образом, в категорию спам попадают сообщения, которые относятся к одному или нескольким следующим критериям:

- направлены пользователю без его согласия;
- вводят его в заблуждение относительно характера таких сообщений;
- вводят его в заблуждение относительно отправителя сообщений.

На сегодняшний день социальные сети приобретают все большее значение в решении коммуникационных задач. Наряду с обычными пользователями, свои аккаунты регистрируют в социальных сетях (VK, Telegram и т.д.) компании, публичные лица, госструктуры (например ООО «Яндекс»[185], Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций[186], официальный канал заместителя председателя

(утв. ФСТЭК РФ 15.02.2008). URL: https://www.consultant.ru/ (дата обращения: 11.05.2023).

[184] Правила оказания телематических услуг связи (утв. Постановлением Правительства РФ от 31 декабря 2021 г. № 2607. URL: https://www.consultant.ru/ (дата обращения: 11.05.2023).

[185] URL: https://t.me/yandex (дата обращения: 11.05.2023).

[186] URL: https://t.me/rkn_tg (дата обращения: 11.05.2023).

Совета Безопасности РФ Медведева Д.А.[187]). Чем популярнее становятся такие ресурсы, тем большим угрозам подвергается информация, размещенная в социальных сетях[188]. Социальные сети – это интернет-площадки для общения, обмена информацией и контентом, прочих социальных взаимодействий[189].

Telegram – это мессенджер, появившийся в 2013 г., с помощью которого можно обмениваться текстовыми, видео- и аудиосообщениями, прикреплять к ним стикеры, медиафайлы и другие документы. Кроме указанного выше функционала, в Telegram можно создавать публичные и не публичные группы и каналы, организовывать групповые чаты-конференции, совершать звонки – голосовые и по видеосвязи[190,191]. В 2022 году количество активных пользователей Telegram превысило 700 млн чел. в месяц по всему миру[192]. Например, количество пользователей популярной в России социальной сети VK составляет 72,5 млн чел. в месяц[193].

Функционал Telegram предполагает использование следующей терминологии:

1. Аккаунт – личная страничка пользователя, зарегистрированная на определенный номер телефона. На один номер телефона может быть зарегистрирован один аккаунт.

---

[187] URL: https://t.me/medvedev_telegram (дата обращения: 11.05.2023).

[188] *Бадюк Д.С., Шрейнер И.Ю.* Информационная безопасность в социальных сетях : материалы VI Междунар. науч.-практ. конф. ; под общ. ред. Е.Ю. Тюменцевой. 2019. С. 494.

[189] *Кухаренко Ю.С.* Особенности распространения рекламных сообщений в социальных сетях (на примере социальной сети «вконтакте») // Знак: проблемное поле медиаобразования. 2018. № 1 (27). С. 171-177.

[190] linDEAL 2022 г. URL: https://lindeal.com/business/telegram-istoriya-sozda-niya-i-uspekha-kompani (дата обращения: 11.05.2023).

[191] *Рубина В.Б.* Telegram-каналы как основные слагаемые успеха менеджера Telegram // Идеи и новации. 2020. Т. 8, № 1. С. 73-84.

[192] Telegram (официальный сайт) 19.06.2022. URL: https://telegram.org /blog/700-million-and-premium/ru (дата обращения: 11.05.2023).

[193] «Вконтакте» подвела итоги 2021 г.: 72,5 млн пользователей в России и 1,2 млрд просмотров видео в день. 03.03.2022 10:43 https://www.cnews.ru/ (дата обращения: 11.05.2023).

2. Группа – это сообщество, включающее в себя до 200 тысяч пользователей, в котором пользователями осуществляется обмен сообщениями, файлами и проч. В группе могут быть администраторы, которые могут изменять настройки группы, удалять сообщения, блокировать пользователей, добавлять различных ботов и т.д.[194].

3. Канал – это сообщество с неограниченным количеством пользователей, в котором только администраторы могут публиковать сообщения. Они могут быть использованы для распространения информации широкой аудитории.

В социальных сетях пользователи общаются с другими пользователями или задают вопросы на сайте производителя сотруднику, но часто не понимают, что говорят с ботом. Бот – это программа, которая создана, чтобы выполнять однотипные и повторяемые задачи по определенному алгоритму[195]. По направлению использования ботов можно разделить на «функциональные» боты и «юзерботы». «Функциональные» боты имеют ограниченный круг функций, ограничены в правах рассылки, работают с разрешения пользователя. Они могут создавать опросы, предоставлять доступ к почте, искать информацию в онлайн-сервисах (например @QuizBot, @GMailBot, @wiki в Telegram). «Функциональные» боты развлекают, помогают и рассказывают. Публичная ссылка таких ботов почти всегда имеет окончание «bot». «Юзерботы» не имеют функциональных ограничений, могут отправлять сообщения пользователям без их согласия. «Юзерботы», в свою очередь, могут выполнять следующие действия:

1. Сбор данных о группе и ее участниках без их согласия.

2. Отправка нежелательных сообщений в группу и ее участникам (спам-рассылка).

3. Нежелательное (несогласованное) добавление пользователя в группу. Целью данного функционала является стартовая раскрутка группы или создание мошеннической группы, и добавление

---

[194] Лимиты Telegram. URL: https://limits.tginfo.me/ru-RU (дата обращения: 11.05.2023).

[195] Школа продвижения в социальных сетях. URL: https://smmplanner.com/blog/chto-takoie-bot-voobshchie-i-v-sotssietiakh-dlia-chiegho-nuzhien-i-kak-polzovatsia/ (дата обращения: 11.05.2023).

туда аудитории из официальной. В результате чего пользователи будут думать, что они состоят в официальной группе, в то время как они состоят в мошеннической группе – «двойнике». Примером может служить группа Чат Crypto Bot (@CryptoBotChatRu)[196], которая является двойником официальной группы Чат Crypto Bot (@CryptoBotRussian)[197].

4. Координированное засорение чата большим количеством сообщений (Flood)[198].

5. Координированное засорение видеозвонка (в Telegram – видеочата) ненужными звуковыми и видеосообщениями.

6. Массовая отправка жалоб на аккаунт, канал, группу, в результате чего они могут быть удалены из результатов поиска или заблокированы.

Несмотря на активную политику борьбы Telegram с юзерботами («флудвейт» (временное ограничение на выполнение определенного вида действий на период от нескольких секунд до 24 часов), спам-бан (временное или постоянное ограничение пользователей на отправку сообщений), полная блокировка аккаунта), на данный момент она недостаточна. Подтверждением данного утверждения являются зарегистрированные случаи спам-атак на аккаунты пользователей[199,200,201].

В дальнейшем в рамках данного исследования под термином «бот» будет пониматься «юзербот», являющийся нежелательным для присутствия в Telegram-группах. Целью данного исследования

---

[196] URL: https://t.me/CryptoBotChatRu (дата обращения: 11.05.2023).

[197] URL: https://t.me/CryptoBotRussian (дата обращения: 11.05.2023).

[198] Заработок в Интернете+. URL: https://work-in-internet.ru/chto-takoe-flud-v-chate-prostymi-slovami.html) (дата обращения: 11.05.2023).

[199] Способ атаковать любой чат в Telegram-мессенджере, или как на меня напали хакеры 22 авг 2021 в 19:53. URL: https://habr.com/ru/articles/574116/ (дата обращения: 11.05.2023).

[200] Атака ботов (Пикабу) 2021. URL: https://pikabu.ru/story/ataka_botov_7514181 (дата обращения: 11.05.2023).

[201] Ботом данный: как пользователей заваливают спамом // Известия 6 октября 2021 г., 10:00. URL: https://iz.ru/ (дата обращения: 11.05.2023).

является создание сервиса, который позволил бы отличать реальных пользователей от ботов в Telegram-группах.

На данный момент существуют следующие аналоги данного сервиса: Combot,[202], Group Help[203], Rose[204]. Все они являются ботами-модераторами (помощники чата) и обладают базовой защитой от нежелательных ботов в виде «капчи» (тест, который определяет, что пользователь не робот)[205]. Общей проблемой такого подхода является сложность для получения доступа в группу конечным пользователям. Разрабатываемый сервис будет требовать прохождения капчи только от некоторых аккаунтов на основании индивидуального рейтинга. Таким образом, реальные пользователи не будут получать требования прохождения «капчи», а боты – будут получать усложненные варианты «капчи», которые они не смогут пройти самостоятельно.

Методология исследования включает в себя выработку критериев и расчет индивидуального коэффициента. Данный коэффициент определяет индивидуальный рейтинг аккаунта, на основании которого будет производиться классификация аккаунтов по степени вероятности отнесения их к ботам. Чем выше значение рейтинга, тем больше вероятность того, что рассматриваемым аккаунтом управляет реальный пользователь.

Критерии, используемые для расчета индивидуального рейтинга, были условно разделены на «положительные» (для таких критериев коэффициент значимости будет устанавливаться со знаком «+») и «отрицательные» (для таких критериев коэффициент значимости будет устанавливаться со знаком «-»). К «положительным» критериям были отнесены следующие показатели:

1. Наличие платных элементов у аккаунта, таких как username в виде NFT, анонимный номер в виде NFT, подписки Telegram

---

[202] URL: https://t.me/combot (дата обращения: 12.05.2023).

[203] URL: https://t.me/GroupHelpBot (дата обращения: 12.05.2023).

[204] URL: https://t.me/MissRose_bot (дата обращения: 12.05.2023).

[205] CAPTCHA 26 марта 2023. URL: https://blog.skillfactory.ru/glossary/captcha/ (дата обращения: 12.05.2023).

Premium (наличие платных элементов у аккаунта удорожает стоимость потенциального бота и снижает вероятность его использования).

2. Дата регистрации аккаунта (чем больше «возраст» аккаунта, тем ниже вероятность, что это бот, поскольку средняя продолжительность жизни бота не превышает 2 месяцев).

3. Зарегистрированный факт блокировки и последующей разблокировки аккаунта (аккаунт прошел модерацию вручную и был разблокирован, что является гарантией реальности пользователя).

4. Количество групп, в которые вступил аккаунт.

5. Наличие аккаунта в базе номеров телефона, которая была сформирована в 2021 г.[206].

6. Наличие регистрации рассматриваемого username на других площадках (VK, Яндекс, Одноклассники и т.д.).

7. Наличие фотографии.

8. Наличие описания у аккаунта.

К «отрицательным» критериям были отнесены следующие показатели:

1. Наличие аккаунта в публичных антиспам – базах, таких как Combot Anti-Spam System[207].

2. Отличие языка пользователя от языка группы, в которую он вступил.

3. Наличие ссылок в описании пользователя.

Алгоритм расчета индивидуального рейтинга и отнесения его к определенной классификационной категории представлен в формуле *(1)*:

$$\sum Vi * Ki > P \qquad (1)$$

где

V_i – значение критерия i для аккаунта;

K_i – коэффициент значимости критерия i (вес);

[206] В Интернет слили базу данных 774 тыс. клиентов сервиса «Глаз Бога» // Коммерсант. 13.07.2021, 13:01. URL: https://www.kommersant.ru/ (дата обращения: 13.05.2023).

[207] Combot Anti-Spam System. URL: https://cas.chat/ (дата обращения: 13.05.2023).

P – пороговое значение для классификационной категории.

Расчет коэффициента значимости K_i производился автоматически на основании базовой выборки (100 аккаунтов реальных пользователей и 100 аккаунтов ботов, определенных ручным способом), подобно алгоритму обучения нейросети[208]. Программа расчета коэффициентов посредством использования математико-статистических методов (перебор вариантов, корреляционная связь и др.) автоматически подбирала коэффициенты, которые наиболее близко к реальности отражали классификацию выборки. Пороговые значения для классификационной категории P рассчитывались автоматически вместе с коэффициентами.

В дальнейшем в целях увеличения точности расчета коэффициентов K_i и пороговых значений для классификационных категорий P базовая выборка (100 аккаунтов реальных пользователей и 100 аккаунтов ботов, определенных ручным способом) будет ежедневно дополняться. Администратору (администраторам) сервиса будет отправляться определённое количество случайных аккаунтов, которые взаимодействовали с сервисом для ручного разделения аккаунтов на реальных пользователей и ботов с последующим дополнением их в базовую выборку. Таким образом, будет снижаться процент ошибки, связанный с автоматической работой сервиса.

В перспективе данный сервис можно использовать не только в группах Telegram, но и в Telegram-каналах, и в качестве модернизации «функциональных» ботов (как система защиты от мошеннических действий). Методологию создания сервиса можно перенести на другие социальные сети (например VK) с корректировкой классификационных критериев.

Библиографический список

1. Бадюк Д.С., Шрейнер И.Ю. Информационная безопасность в социальных сетях : материалы VI Междунар. науч.-практ. конф. ; под общ. ред. Е.Ю. Тюменцевой. 2019. – С. 494.

[208] Нейронные сети для начинающих. Часть 1 // Хабр. 12.10.2016, 16:48. URL: https://habr.com/ru/articles/312450/ (дата обращения: 13.05.2023).

2. Кухаренко Ю.С. Особенности распространения рекламных сообщений в социальных сетях (на примере социальной сети «вконтакте») // Знак: проблемное поле медиаобразования. – 2018. – № 1 (27). – С. 171-177.

3. Рубина В.Б. Telegram-каналы как основные слагаемые успеха менеджера Telegram // Идеи и новации. – 2020. – Т. 8, № 1 – С. 73-84.

Стяжкина Светлана Александровна,
к.ю.н., доцент, доцент кафедры уголовного права и криминологии ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обеспечение информационной безопасности является одним из главных направлений деятельности государства. Проблема защиты информации выходит на первый план. Динамично развивающиеся информационно-телекоммуникационные процессы и технологии требуют оперативного реагирования со стороны нормативного регулирования вопросов обеспечения информационной безопасности. Как указано в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646, «информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопас-

ность государства»[209]. Таким образом, одним из главных составляющих информационной безопасности выступает состояние защищенности личности, охрана ее информационных прав.

Необходимо отметить, что продолжается тенденция роста деяний, посягающих на персональные данные личности. По данным Positive Technologies «наблюдается прирост доли персональных данных среди украденной информации относительно итогов 2021 года: для организаций – 4 процентных пункта (с 32 до 36 %), для частных лиц – 8 п. п. (с 20 до 28 %)»[210]. Как отмечают эксперты: «В будущем такие объемы данных позволят злоумышленникам составлять цифровые портреты жертв и проводить более изощренные атаки с применением социальной инженерии».

Персональные данные все чаще и чаще выступают целью кибератак и, несомненно, представляют интерес для преступников. В связи с широко распространившимися случаями посягательств на персональные данные и возникающие угрозы информационной безопасности личности необходимо остановиться на проблемах уголовно-правовой охраны персональных данных.

В соответствии со ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» под персональными данными понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[211]. В научной литературе подобное определение вызывает критику. Многие авторы отмечают необходимость конкретизировать сведения, которые относятся к персональным данным. Как указывает А.А. Шутова: «Отсутствие конкретного перечня сведений, которые следует относить к персональным, приводит к тому, что в практической деятельности нередко возникают проблемы с определением того, какая информация будет относиться

---

[209] Указ Президента РФ от 5 декабря 2016 г. № 646 // СПС «Гарант».

[210] URL: https://www.ptsecurity.com/ru-ru/

[211] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ // СПС «Гарант».

к ним»[212]. Действительно, данное определение вряд ли может быть использовано при квалификации действий.

Но, говоря об уголовно-правовой защите рассматриваемых сведений, следует отметить, что предметом уголовно-правовой охраны будут не любые персональные данные, а только те, доступ к которым был ограничен или запрещен их владельцем, так как вышеназванный закон предусматривает такую разновидность персональных данных, как «персональные данные, разрешенные субъектом персональных данных для распространения».

Таким образом, определяющим критерием отнесения тех или иных сведений к числу защищаемых будет являться такой признак, как запрещенность субъектом данных их распространения. Речь идет об установлении режима конфиденциальности сведений. Само лицо определяет какие сведения не подлежат разглашению, а также перечень сведений, который может быть публично доступен. Следовательно, как справедливо отмечает С.И. Гутник, «вопрос о правовой охране персональных данных каждый раз зависит от стремлений самого человека защитить значимую для него информацию о себе путём установления соответствующего режима конфиденциальности персональной информации»[213].

Уголовный закон не предусматривает самостоятельную уголовно-правовую защиту персональных данных. Как справедливо отмечается в литературе, «персональные данные могут подпадать под различные правовые режимы конфиденциальности (личной и семейной тайны, коммерческой тайны, банковской тайны, налоговой тайны). Вследствие этого опасность угрожает только той разновидности персональных данных, которые являются конфиденциальными – сохранение тех или иных сведений в тайне является залогом

---

[212] *Шутова А.А.* Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные // Вестник Нижегородской академии МВД России. 2015. № 4 (32). С. 333.

[213] *Гутник С.И.* Уголовно-правовая характеристика преступных посягательств в отношении персональных данных : дис. … канд. юрид. наук. Красноярск, 2017. С. 108.

сохранения системы общественных отношений»[214]. Исходя из анализа действующих уголовно-правовых норм, можно сделать вывод, что персональные данные будут выступать предметом нескольких преступлений.

Во-первых, это ст. 137 УК РФ, предусматривающая ответственность за нарушение неприкосновенности частной жизни лица. Следует отметить, что предметом преступления, предусмотренного ст. 137 УК РФ, выступают сведения о частой жизни лица, составляющие его личную или семейную тайну. Ряд исследователей при анализе данного состава указывают на необходимость предусмотреть четкий перечень данных, раскрывающих понятие частной жизни лица, составляющих его личную или семейную тайну, относя к ним в том числе и персональные данные. Сложно согласиться с данным мнением. Представляется, что персональные данные могут быть личной или семейной тайной, например сведения о национальности, расе лица, политических взглядах, вероисповедании, о состоянии здоровья, о финансовом состоянии и т.д. Что касается сведений, позволяющих идентифицировать человека (ФИО, паспортные данные, адрес регистрации, номер телефона и т.д.), то отнести их к категории личной или семейной тайны не представляется возможным. Эти сведения не могут быть тайной в силу их общедоступности и обязательности предоставления. Следует согласиться с М.Ю. Авдеевым о том, что «персональные данные – лишь информация, позволяющая идентифицировать личность. Само по себе распространение этих данных не столько наносит ущерб личности, сколько создаёт возможность для причинения ущерба»[215].

Еще одним составом преступления, предметом которого могут выступать персональные данные, является ст. 183 УК РФ, где речь идет о незаконном собирании, распространении и использовании

---

[214] *Гутник С.И.* Указ. соч. С. 110.

[215] *Авдеев М.Ю.* Нормативное содержание права на неприкосновенность частной жизни // Новый юридический журнал. 2013. № 1. С. 233.

сведений, составляющих коммерческую, налоговую и банковскую тайну. Безусловно, персональные данные могут подпадать под определение банковской тайны, под которой понимаются сведения об операциях, о счетах и вкладах клиентов и корреспондентов банка.

Также персональные данные могут быть отнесены к коммерческой тайне. Речь идет о клиентских базах, где содержится информация о клиентах компаний и организаций. Здесь необходимо учитывать то обстоятельство, что рассматриваемые сведения можно отнести к сведениям, составляющим коммерческую тайну только при условии установления в отношении этих сведений режима коммерческой тайны (с соблюдением всех условий и правил, закрепленных законодательством). Хотя ряд исследователей придерживаются другой позиции. Как указывает С.И. Гутник, «любая клиентская база коммерческой организации или индивидуального предпринимателя, содержащая персональные данные лиц, которые пользовались услугами или работами указанных субъектов хозяйственной деятельности, подпадает под режим коммерческой тайны независимо от соблюдения или несоблюдения данным субъектом правил и режима коммерческой тайны»[216]. С данным мнением нельзя согласиться, так как Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ указывает, что «информация, составляющая коммерческую тайну, – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании, и в отношении которых обладателем таких сведений введен режим коммерческой тайны»[217]. То есть обязатель-

---

[216] *Гутник С.И.* Указ. соч. С. 66.

[217] О коммерческой тайне : Федеральный закон от 29.07.2004 № 98-ФЗ // СПС «Гарант».

ным признаком сведений, относимых к коммерческой тайне, является факт введения режима коммерческой тайны в отношении этих сведений.

Еще одним предметом преступления, предусмотренного ст. 183 УК РФ, выступают сведения, составляющие налоговую тайну. Не вызывает сомнений, что сведения о налогоплательщике относятся к персональным данным, в связи с чем подлежат уголовно-правовой охране по ст. 183 УК РФ.

В эпоху цифровизации и компьютеризации всех сфер жизнедеятельности общества, государства и отдельной личности все большую актуальность приобретает проблема защиты компьютерной информации. Быстрыми темпами развиваются информационно-телекоммуникационные системы и цифровые ресурсы. Большая часть персональных данных на сегодняшний день представлена в виде компьютерной информации и содержится на различного рода цифровых носителях. При посягательстве на персональные данные, представленные в виде компьютерной информации, квалификация будет осуществляться по преступлениям в сфере компьютерной информации. Универсальной нормой, предусматривающей ответственность за посягательства на сведения, отнесенные к персональным данным, которые представлены в виде электрических сигналов, и в отношении которых владельцем этих сведений или законным обладателем установлены меры безопасности и ограничен доступ, является ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Уголовная ответственность наступит только в случае, если в результате неправомерного доступа к компьютерной информации наступило одно из указанных в диспозиции неблагоприятных последствий в виде уничтожения, модификации или копирования рассматриваемых сведений. Таким образом, персональные данные могут выступать и предметом преступления, предусмотренного ст. 272 УК РФ. Если учесть, что большая часть сведений на сегодняшний день содержится на цифровых носителях, то и проблем с квалификацией действий лиц, скопировавших персональные данные из источников, доступ к которым был ограничен, не возникнет.

В качестве выводов можно отметить, что уголовно-правовая охрана персональных данных осуществляется в рамках нескольких статей Уголовного кодекса, которые предусматривают ответственность за посягательство на различные виды информации. В литературе высказывается предложение о необходимости предусмотреть уголовную ответственность за «незаконный сбор и (или) распространение персональных данных гражданина без его согласия». Как нам представляется, введение отдельной нормы, предметом которой выступали бы персональные данные, является излишним. Как справедливо отметил С.И. Гутник: «При введении специальной уголовно-правовой охраны преступных посягательств в отношении персональных данных неизбежно возникает избыточность криминализации. Это, в первую очередь, связано с тем, что соответствующие правовые режимы конфиденциальности персональных данных уже подпадают под уголовно-правовое воздействие посредством соответствующих норм Уголовного кодекса РФ (ст. 137, ст. 183)»[218].

Библиографический список

1. Авдеев М.Ю. Нормативное содержание права на неприкосновенность частной жизни // Новый юридический журнал. – 2013. – № 1.

2. Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных : дис. … канд. юрид. наук. – Красноярск, 2017.

3. Шутова А.А. Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные // Вестник Нижегородской академии МВД России. – 2015. – №4 (32).

[218] *Гутник С.И.* Указ. соч. С. 109.

Исхаков Роберт Ильгизович,
старший преподаватель кафедры
информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

ПРАКТИКА ПРИМЕНЕНИЯ СТЕНДА ВИРТУАЛИЗАЦИИ PROXMOX В УЧЕБНОМ ПРОЦЕССЕ СТУДЕНТОВ УГСН 10.00.00

В настоящее время в Удмуртском государственном университете осуществляется обучение студентов УГСН 10.00.00 по направлению «Информационная безопасность» и по специальности «Безопасность информационных технологий в правоохранительной сфере».

Большое количество ИТ-дисциплин, которые входят в учебный план, требуют закрепления теоретических знаний в ходе выполнения лабораторных работ[219].

Спецификой таких лабораторных работ является необходимость выполнения обучаемыми различных административных действий над системным и прикладным программным обеспечением, что требует предоставления прав администратора системы. Для решения этой задачи в процессе обучения используются технологии виртуальных машин.

Использование технологий виртуальных машин позволяет:

– выполнять полноценное администрирование программного обеспечения без необходимости его установки на персональный компьютер лабораторного класса;

– обеспечить индивидуальную среду обучения студента;

– использовать шаблоны сред обучения для различных дисциплин;

---

[219] *Васильева И.Н., Родин В.Н., Чернокнижный Г.М.* Использование средств виртуализации в преподавании ИТ-дисциплин // Вестник Санкт-Петербургского университета МВД России. 2013. № 1. С. 148-154.

– обеспечить хорошую степень отказоустойчивости среды обучения.

Среди большого количества программных сред виртуализации в учебном процессе используются гипервизор первого типа (требующий аппаратной поддержки) – Proxmox VE (далее – Proxmox) и гипервизор второго типа (работающий как приложение базовой операционной системы) – OracleVM VirtualBox (далее – VirtualBox)[220].

Гипервизор Proxmox установлен на сервере (стенде) виртуализации, а VirtualBox устанавливается на каждом персональном компьютере лабораторного класса[221].

Несмотря на ряд преимуществ использования технологии виртуальных машин на базе VirtualBox, которые перечислены выше, данный вариант использования виртуальных машин имеет ряд недостатков:

– количество одновременно используемых виртуальных машин ограничено вычислительными ресурсами персонального компьютера пользователя, а в рамках некоторых лабораторных работ требуется одновременное использование нескольких виртуальных машин;

– студенты имеют доступ к виртуальным машинам других пользователей, поэтому возникает проблема обеспечения целостности виртуальных машин;

– студенты получают возможность выполнения административных функций VirtualBox, в связи с чем возникает ситуация бесконтрольного клонирования (копирования) виртуальных машин, что приводит к исчерпанию дискового пространства персонального компьютера;

– студент фактически «привязывается» к рабочему месту, на котором установлены его виртуальные машины, что не позволяет ему выполнять лабораторные работы на других рабочих местах класса.

Гипервизор Proxmox – программный продукт для реализации серверной платформы виртуализации, которая способна поддерживать одновременную работу сотен виртуальных машин (гостевых хостов).

---

[220] VirtualBox. URL: https://www.virtualbox.org

[221] Proxmox – Powerful open-source server solutions URL: https://www.proxmox.com/

Определим ряд аргументов использования централизованного стенда виртуализации Proxmox в сравнении с автономным (на каждом персональном компьютере) использованием VirtualBox:

– работа со стендом строится по технологии клиент – сервер, поэтому на стороне клиента (персональный компьютер студента) для доступа к стенду используется веб-браузер, а вычислительные задачи выполняются на стороне сервера виртуализации Proxmox;

– обучаемый не «привязывается» к одному рабочему месту, доступ к его среде обучения возможен с любого рабочего места ЛВС университета, а при необходимости и из-за пределов университетской сети, например, с домашнего персонального компьютера;

– для студента создается индивидуальная среда обучения, к которой он получает доступ под собственной учетной записью;

– функции Proxmox позволяют организовать централизованный контроль работы студентов с возможностью ведения истории доступа студента к стенду;

– в рамках лабораторных работ возможно моделирование многокомпонентных сред и совместное их использование;

– возможно создание и использование тематических кластеров.

Тематический кластер – совокупность виртуальных машин и методического обеспечения кластера для решения определенных задач обучения студента.

Каждый из тематических кластеров предназначен для решения определенных задач обучения специалистов в области информационной безопасности: изучение технологий отечественных операционных систем, изучение инструментов поиска и закрытия уязвимостей информационных систем, изучение специализированного программного обеспечения и т.д.

Тематические кластеры имеют различную изолированность от внешней среды. В каких-то кластерах пользователи должны иметь доступ к сети Интернет, например, для установки пакетов программ из репозитория разработчика операционной системы, а другие должны быть изолированы от внешней среды, т.к. в них используются инструменты поиска уязвимостей информационной

системы, которые могут быть использованы обучаемыми для деструктивного воздействия на ресурсы Интернет.

Для развития тематического кластера за ним закрепляется специалист предметной области – это может быть преподаватель, который использует его для проведения своих дисциплин или инженер, выполняющий работу по администрированию сети университета.

Среди наиболее востребованных тематических кластеров отметим следующие: «Отечественные операционные системы и прикладное программное обеспечение», «Гетерогенная информационная сеть на базе Microsoft Windows AD, Samba DC и FreeIpa», «Стенд по поиску и закрытию уязвимостей информационной системы».

Тематический кластер *«Отечественные операционные системы и прикладное программное обеспечение»* используется для изучения технологий отечественных операционных систем на базе ядра Линукс и предлагает студентам три уровня обучения.

1. «Пользователь операционной системы». Уровень направлен на изучение базовых основ использования отечественных операционных систем.

2. «Базовое администрирование операционной системы». В рамках этого уровня студенты получают навыки администрирования операционных систем на базе ядра Линукс.

3. «Администрирование операционной системы специального назначения». На этом уровне обучаемые изучают операционные системы, которые могут быть использованы в информационных системах, где обрабатывается информация, относящаяся к государственной тайне.

В состав тематического кластера входят виртуальные машины с установленными операционными системами: Астра Линкус «Орел», Астра Линукс «Смоленск», Ред ОС, Альт Линукс.

Тематический кластер «*Гетерогенная информационная сеть на базе Microsoft Windows AD, Samba DC и FreeIpa»* используется для изучения технологий создания системы доверительных отношений в гетерогенных сетях.

Современные российские организации находятся на этапе перехода от иностранного программного обеспечения к отечественному ПО. Такой процесс предполагает поэтапную замену иностранного ПО, что приводит к необходимости создания гетерогенных информационных сетей, в которых используются доверительные отношения между доменами на основе Microsoft Windows AD, Samba DC или FreeIPA.

В состав тематического кластера входят следующие виртуальные машины:

– виртуальная машина с операционной системой MS Windows Server 2016 (контроллер домена Windows);

– виртуальная машина с операционной системой MS Windows 10 (рабочая станция домена Windows);

– виртуальная машина с операционной системой Астра Линукс Орел (контроллер домена FreeIPA);

– виртуальная машина с операционной системой Астра Линукс Орел (рабочая станция домена FreeIPA);

– виртуальная машина с операционной системой Альт Линкус сервер (контроллер домена Samba DC);

– виртуальная машина с операционной системой Альт Рабочая станция (рабочая станция домена Samba DC).

Тематический кластер *«Стенд по поиску и закрытию уязвимостей информационной системы»* используется в качестве стенда для изучения инструментов выявления уязвимостей программного обеспечения, практической демонстрации эксплуатации выявленных уязвимостей, а также для формирования рекомендаций по устранению выявленных уязвимостей.

Тематический кластер служит для выявления уязвимых мест в элементах информационной инфраструктуры, практической демонстрации возможностей использования уязвимостей, а также для формирования рекомендаций по устранению выявленных уязвимостей.

В состав тематического кластера входят следующие виртуальные машины:

– виртуальная машина с операционной системой Kali Linux (специализированная операционная система для проведения пентеста);

– виртуальная машина с операционной системой Metasploitable (операционная система с уязвимостями);

– виртуальная машина с операционной системой Ubuntu (операционная система с установленной системой моделирования EVE-NG);

– виртуальная машина с операционной системой Альт Рабочая станция (операционная система с установленным сканером уязвимости ScanOVAL).

Таким образом, в процессе обучения студентов направления «Информационная безопасность» и специальности «Безопасность информационных технологий в правоохранительной сфере» используются технологии виртуализации, среди которых приоритетной является технология на базе централизованного сервера (стенда) Proxmox.

Дальнейшее использование стенда предполагает развитие существующих и создание новых тематических кластеров.

Библиографический список

1. Васильева И.Н., Родин В.Н., Чернокнижный Г.М. Использование средств виртуализации в преподавании ИТ-дисциплин // Вестник Санкт-Петербургского университета МВД России. – 2013. – № 1. – С. 148-154.

2. Чернокнижный Г.М. Использование средств виртуализации пользовательских операционных сред в самостоятельной работе студентов // Инновационные методы уровневого образования в университете : материалы учеб.-метод. конф. проф.-преп. состава 20 января 2011 г. – СПб. : СПбГИЭУ, 2011. – С. 35.

3. VirtualBox [Электронный ресурс]. – URL: https://www.virtualbox.org

4. Proxmox – Powerful open-source server solutions [Электронный ресурс]. – URL: https://www.proxmox.com/

Дубовикова Ольга Викторовна,
старший преподаватель кафедры
информационной безопасности в управлении
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В УМНОМ ГОРОДЕ

Искусственный интеллект (далее – ИИ) – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека[222].

В настоящее время развитие ИИ оценивается как слабое и относится к классу «Narrow AI». Более высокие уровни могут быть достигнуты к 2070 году и значительно превысят творческие и другие человеческие способности.

Функции искусственного интеллекта:

- возможность решать задачи, выполняемые человеком;
- способность выполнять некоторые творческие функции, представленные в базе знаний ИИ;
- интерпретация и сбор внешних данных, их анализ и принятие решения о действиях;
- адаптация под определенные ситуации, самообучение в процессе работы.

[222] О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» : Федеральный закон от 24.04.2020 № 123-ФЗ, ст. 2.

Умный город – это город, в котором используются современные информационные технологии для оптимизации процессов управления, повышения безопасности и уровня жизни его жителей. Важную роль в развитии умного города играют технологии ИИ. Они применяются для управления транспортом, энергоснабжением, отходами, водоснабжением, городской инфраструктурой, здравоохранением и безопасностью города.

Рассмотрим области применения ИИ в умном городе:

1. Автоматизация управления транспортом, применение беспилотных автомобилей, улучшение безопасности дорожного движения, оптимизация дорожной инфраструктуры и потока транспорта.

2. Управление энергоснабжением с целью отслеживания энергопотребления, автоматизации контроля расходов энергии и поддержки использования возобновляемых источников энергии.

3. Мониторинг и оптимизация процессов сбора, переработки и утилизации отходов.

4. Управление водоснабжением для отслеживания качества воды, оптимизации расхода воды и предсказания сбоев в работе системы.

5. Управление городской инфраструктурой для наблюдения и оптимизации работы общественных транспортных средств, светофоров и дорожных знаков.

6. Управление здравоохранением для мониторинга состояния здоровья жителей города.

7. Управление общественной безопасностью и уровнем преступности города.

Примерами умных городов России, в которых успешно применяются технологии искусственного интеллекта, являются не только крупные города-миллионники (Москва, Санкт-Петербург, Казань, Екатеринбург и др.), но и небольшие города, например:

• Иннополис – молодой город в Республике Татарстан с населением 4,2 тыс. человек. У горожан есть виртуальная нейросеть и чат-бот в Telegram, с помощью которых можно узнать расписание автобусов и время работы городских учреждений, а также записаться на прием к врачу. Для быстрого передвижения в Иннополисе

используется бесплатное беспилотное такси, а доставку еды жителям осуществляют беспилотные колесные роботы – роверы.

• Дубна – небольшой город в Московской области с населением 74,5 тыс. жителей, является крупнейшим российским исследовательским центром в области ядерной физики. Развитие Дубны как умного города стало возможным благодаря современной технологической базе наукограда. В городе осуществляется контроль электроэнергии, используемой для уличного освещения, а также производится учет расхода горячей воды и тепловой энергии. Дорожное движение поддерживается умными светофорами, меняющими режимы своей работы в зависимости от загруженности городских дорог.

Изучим подробнее многоуровневую киберзащиту и уязвимые точки умного города, представленные на рис. 1 и 2.

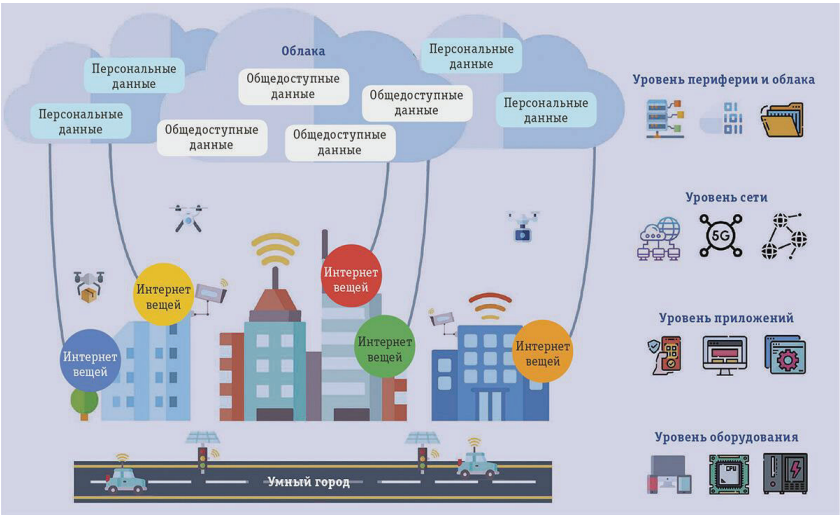


Рис. 1. Многоуровневая киберзащита умного города

Умный город должен повышать качество жизни с помощью ИТ-инфраструктуры, улучшающей различные аспекты повседневной деятельности горожан. Соответствующая архитектура такого города имеет много уровней, на каждом из которых имеется множество точек, требующих защиты от возможных атак. Обеспечение безопас-

ности и приватности должно быть приоритетом, учитывая наличие большого количества устройств, соединенных с Интернетом, которые обмениваются информацией друг с другом и накапливают данные в облаке. Кибератаки могут наносить большой ущерб, учитывая, что умный город работает на киберфизических системах, состоящих из взаимодействующих устройств и систем Интернета вещей[223].

Элементы умного города	Уровень устройств/датчиков	Уровень приложений	Уровень сети	Уровень периферии и облака
Транспорт	Умные автомобили Дорожные знаки Светофоры Уличные фонари Парковочные датчики	Веб-сайт Настольные приложения (Windows, macOS) Мобильные приложения (iOS, Android)	4G, 5G Wi-Fi ZigBee Z-Wave Bluetooth LoRA	Контроль передвижения Регистрация автомобилей Управление светофорами
Здравоохранение	Смарт-часы Фитнес-трекеры Кардиостимуляторы Автоматические инсулиновые помпы			Медицинские данные GPS Медицинские карты
Энергетика	Кондиционеры Датчики отопления Датчики утечки воды Датчики света Датчики температуры и влажности			Местонахождение клиента Температура Влажность Качество электропитания
Умные здания	Термостаты Камеры Умные колонки Умные дверные замки Радионяни			Поведение людей GPS, голос пользователя Заинтересованность пользователя Движение Снимки, видео

Рис. 2. Уязвимые точки умного города

Защита безопасности умного города состоит из нескольких аспектов:

1. Управление рисками кибербезопасности.

Градостроителям и городским администрациям необходимо заранее выбирать способы защиты инфраструктуры от угроз с учетом того, что в умных городах нужно обеспечить безопасность на нескольких уровнях. Необходимо проанализировать угрозы для каждого компонента и предусматривать меры защиты для всех уровней[224].

---

[223] *Чонхым Парк, Хенджи Чанг, Джоанна Дефранко.* Многоуровневая киберзащита для умного города // Открытые системы. СУБД. 2022. № 2. URL: https://www.osp.ru/os/2022/02/13056210?ysclid=li7g1qtv70847617183 (дата обращения: 10.06.2023).

[224] Умные города в России: концепция, интеграция, технологии, примеры [Электронный ресурс]. URL: https://mirdostupa.ru/umnye-goroda-v-rossii-koncepciya-integraciya-texnologii-primery/ (дата обращения: 10.06.2023).

2. Обнаружение аномалий и предотвращение кибератак.

Одним из ключевых аспектов защиты информации в умном городе является обнаружение аномального поведения и предотвращение кибератак. Искусственный интеллект позволяет анализировать большие объемы данных из различных источников, включая системы видеонаблюдения, датчики, социальные сети и другие, для выявления подозрительной активности. Алгоритмы машинного обучения и обработки данных позволяют ИИ распознавать необычные паттерны и предупреждать о возможных атаках на системы умного города.

3. Анализ больших данных для предсказания угроз.

Искусственный интеллект может анализировать огромные объемы данных о событиях, потоках людей, транспортном движении и других параметрах, чтобы выявлять паттерны и тренды, связанные с возможными угрозами. Это помогает городским властям принимать меры для предотвращения потенциальных проблем, таких как аварии, преступления или катастрофы.

4. Автоматизированная система безопасности.

Искусственный интеллект может быть использован для разработки автоматизированных систем безопасности в умном городе. Например, системы контроля доступа, видеонаблюдения и обнаружения лиц могут быть усилены с помощью ИИ. Искусственный интеллект способен распознавать лица, различать нормальное и подозрительное поведение, а также отслеживать людей или объекты, вызывающие опасение. Это обеспечивает более эффективную и надежную систему безопасности в умном городе.

5. Прогнозирование угроз и реагирование в реальном времени.

Искусственный интеллект, используя алгоритмы машинного обучения и обработку данных в реальном времени, может предсказывать потенциальные угрозы и помогать в принятии мер для их предотвращения или минимизации последствий. Например, система ИИ может определять опасные зоны в городе и предупреждать о возможных проблемах, таких как заторы, пожары или повреждe-

ния инфраструктуры. Реагирование в реальном времени на угрозы помогает обеспечить безопасность и эффективность умного города.

6. Прогнозирование потребностей безопасности.

Искусственный интеллект может использоваться для прогнозирования будущих потребностей безопасности и анализа рисков. Он может анализировать исторические данные, моделировать сценарии и предсказывать, какие меры безопасности будут необходимы в определенных условиях или в ответ на конкретные угрозы.

7. Управление данными и конфиденциальность.

Искусственный интеллект может помочь в управлении данными, особенно когда речь идет о персональной информации и конфиденциальных данных горожан. Использование ИИ для автоматизации процессов защиты и шифрования данных может помочь предотвратить несанкционированный доступ и утечку информации.

8. Анализ социальных медиа и общественного мнения.

Искусственный интеллект может мониторить социальные медиа и другие источники общественного мнения, чтобы выявлять потенциальные угрозы и предсказывать настроения или возможные протесты. Это может помочь городским властям принимать меры для предотвращения потенциальных конфликтов и обеспечения общественной безопасности.

9. Подготовка специалистов по кибербезопасности.

Для безопасности умных городов нужно учредить образовательные программы подготовки высококвалифицированных специалистов. Необходимо разработать факультативные дисциплины по киберфизическим системам и Интернету вещей для студентов, проходящих обучение в области ИТ-технологий. Возможно, стоит провести дополнительное обучение для действующих и отошедших от дел ИТ-специалистов, желающих взять на себя работу по защите города[225].

---

[225] Чонхым Парк, Хенджи Чанг, Джоанна Дефранко Многоуровневая киберзащита для умного города // Открытые системы. СУБД. – 2022. – № 2. URL: https://www.osp.ru/os/2022/02/13056210?ysclid=li7g1qtv70847617183 (дата обращения: 10.06.2023).

Библиографический список

1. Чонхым Парк, Хенджи Чанг, Джоанна Дефранко Многоуровневая киберзащита для умного города // Открытые системы. СУБД. – 2022. – № 2. URL: https://www.osp.ru/os/2022/02/13056210?ysclid=li7g1qtv70847617183 (дата обращения: 10.06.2023).

2. Умные города в России: концепция, интеграция, технологии, примеры [Электронный ресурс]. – URL: https://mirdostupa.ru/umnye-goroda-v-rossii-koncepciya-integraciya-texnologii-primery/ (дата обращения: 10.06.2023).

***Артамкин Кирилл Сергеевич**,*
аспирант 1 курса ФГБОУ ВО
«Удмуртский государственный университет»,
г. Ижевск

СПОРНЫЕ ВОПРОСЫ ПЕРЕХОДА ЦИФРОВОЙ ВАЛЮТЫ В ПОРЯДКЕ НАСЛЕДОВАНИЯ

Октябрь 2012 года ознаменовался признанием Европейским центральным банком существования цифровой валюты, когда он распространил доклад «Схемы виртуальных валют». В нём отмечается, что в некоторых случаях «виртуальные сообщества» создают и распространяют свою собственную цифровую валюту для обмена товарами (услугами) и единицы учёта[226]. В российском законодательстве под цифровой валютой, согласно ч. 3 ст. 1 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», признается совокупность электронных данных, содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации,

[226] Virtual Corrency Schemes. European Central Bank. Октябрь 2012. URL: https://www.ecb.europa.eu/ (дата обращения: 13.05.2023).

денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.

Ввиду вышеперечисленного цифровая валюта, признаваемая законодателем имуществом, может быть передана по наследству и в то же время может стать целью незаконного завладения со стороны злоумышленников, поэтому законодательно необходимо закрепление порядка наследования криптовалюты и способов её защиты. В настоящее время в России не существует законодательно регламентированного порядка принятия криптовалюты в порядке наследования, однако существует практика, когда суд признавал необходимость передать отдельный вид цифровых активов. Например, в 2018 году стала популярна такая криптовалюта, как «Bitcoin». На данный момент «Bitcoin», как и вся криптовалюта, признана объектом гражданских прав в соответствии со ст. 128 Гражданского кодекса Российской Федерации (далее – ГК РФ). Таковой её признал Девятый Арбитражный апелляционный суд. В деле о банкротстве арбитражный управляющий нашёл у лица, в отношении которого ведется процедура банкротства, криптокошелёк и заявил, что его необходимо включить в конкурсную массу, а также передать финансовому управляющему доступ к криптокошельку, логин и пароль. Истец возразил арбитражному управляющему и заявил, что криптовалюта не является объектом гражданских прав и имуществом в целом и поэтому не подлежит включению в конкурсную массу. Суд первой инстанции эти доводы не поддержал. Но суд апелляционной инстанции указал на то, что согласно ст. 128 ГК РФ к объектам гражданских прав относятся вещи, включая наличные деньги и документарные ценные бумаги, иное имущество. Также суд пояснил, что в Гражданском кодексе РФ отсутствует закрытый перечень

объектов гражданских прав, и действующее гражданское законодательство содержит понятие «иное имущество», упомянутое в ст. 128 ГК РФ, а с учетом современных экономических реалий и уровня развития информационных технологий допустимо максимально широкое его толкование. По мнению суда апелляционной инстанции, криптовалюта может быть расценена применительно к ст. 128 ГК РФ иначе как «иное имущество». Тем самым суд признал криптовалюту объектом гражданских прав[227].

Некоторые исследователи утверждают, что «применение к криптовалютам «традиционных» правил наследования активов (ценных бумаг, долей и т.д.) невозможно, что объясняется анонимностью криптокошельков»[228]. Решение этой проблемы исследователям видится в передаче ключа (пароля) и номера (логина) криптокошелька наследникам. В противном случае, если потенциальный наследодатель-владелец криптокошелька умрет раньше передачи такой информации – активы криптокошелька будут утеряны навсегда. На наш взгляд, на данный момент отсутствует возможность каким-либо образом повысить безопасность передачи криптовалюты по наследованию, поскольку внести изменения в действующее законодательство, введя в него процедуру передачи криптовалюты по наследству, невозможно из-за природы этого объекта. Криптовалюты, в отличие от цифровых валют центральных банков, не обладают такими свойствами денег, как эмитент, централизованная платежная система, обеспечивающая учёт расчётных единиц, возможность определения владельца счёта. «Такие особенности криптовалюты во многом идут вразрез с требованиями российского

---

[227] Постановление Девятого Арбитражного Апелляционного суда от 15 мая 2018 г. № 09АП-16416/2018 // СПС «КонсультантПлюс» (дата обращения: 08.05.2023).

[228] *Очирова П.И., Степаненко А.С.* Наследование криптовалюты: особенности и проблемы // Гуманитарные, социально-экономические и общественные науки. 2022. URL: https://cyberleninka.ru/ (дата обращения: 08.05.2023).

законодательства и тем самым значительно сужают сферу ее применения, поясняют эксперты»[229].

На проблемах наследования криптовалют также акцентируют внимание практикующие юристы стран СНГ: «Белорусское законодательство уже содержит достаточно много правовых норм, регулирующих цифровые права, но прецедентов с наследованием криптовалют у нотариусов еще не было, хотя эксперты уже прогнозируют возможные проблемы и вырабатывают пути их решения»[230]. В числе проблемных моментов юристы выделяют проблемы с собственностью на криптовалюты. Такая собственность обезличена, собственник не числится ни в каких реестрах; подтверждение собственности нельзя получить ни в каком виде, хотя оно требуется для вступления в права наследования. Возможность владеть и распоряжаться криптовалютой зависит только от владения номером специального электронного криптовалютного кошелька и наличия пароля к нему.

Таким образом, в настоящий момент владельцы криптовалюты не имеют возможности передать данные своих криптокошельков в порядке наследования, поскольку, во-первых, вопрос подтверждения принадлежности этого типа имущества конкретному лицу остается открытым; во-вторых, нотариус не может оформить наследственные права без идентификации и проверки факта принадлежности имущества наследодателю. Обезличенные виртуальные кошельки просто не позволяют этого сделать. Нет документа, который бы официально подтвердил, что тот или иной криптокошелек – это собственность покойного.

Кроме того, получить доступ к криптокошельку наследодателя после его смерти возможно через «изучение его электронной переписки, анализ банковских операций, записей в реестрах прав, которые отражают сделки с объектами, удостоверенными токена-

---

[229] *Куликов В.* Нотариусы сообщили о невозможности передать криптовалюту по наследству // Рос. газ. 23.05.2022. URL: https://rg.ru/ (дата обращения: 08.05.2023).

[230] *Ключевская Н.* Наследование цифровых активов: российский и зарубежный опыт. 2021 // СПС «Гарант» (дата обращения: 08.05.2023).

ми»[231]. Вместе с тем обеспечить принудительный доступ к выявленному наследниками цифровому кошельку наследодателя, при отсутствии у них кода, пока невозможно.

Для того, чтобы обеспечить сохранность цифрового имущества при наследовании, наследодатель может предпринять следующие шаги:

1. Создать список цифровых активов, в котором будут указаны все цифровые активы. Этот список должен быть доступен на случай смерти наследодателя и передан нотариусу или доверенному лицу.

2. Установить правила доступа, решить, кому наследодатель хочет передать свои цифровые активы, и как они будут иметь к ним доступ. Это могут быть наследники, друзья или доверенные лица.

3. Использовать надёжные пароли, которые никто не знает, кроме владельца кошелька. При использовании онлайн-банкинга применить двухфакторную аутентификацию, чтобы защитить счета.

4. Создание доверенности на доступ к цифровым активам, чтобы передать их наследникам или другим лицам. В этом случае субъект должен указать, какие активы он хочет передать и кому.

5. Создать резервные копии всех своих цифровых данных и хранить их в надежном месте. Это поможет сохранить имущество в случае потери или повреждения файлов.

Передача криптовалюты в порядке наследования предопределена созданным для нее правовым режимом как объекта права. Обеспечение сохранности цифрового имущества при наследовании – это важный процесс, который должен быть учтен при планировании наследования. Создание списка активов, установление правил доступа, использование паролей и учетных записей, создание доверенности на доступ к активам и резервное копирование данных – все эти меры помогут защитить цифровое имущество и передать его наследникам в безопасности.

---

[231] *Яценко Т.С.* Наследование цифровых прав. 2019. URL: https://urfac.ru/ (дата обращения: 08.05.2023).

Библиографический список

1. Очирова П.И., Степаненко А.С. Наследование криптовалюты: особенности и проблемы // Гуманитарные, социально-экономические и общественные науки. – 2022. – URL: https://cyberleninka.ru/ (дата обращения: 08.05.2023).

2. Куликов В. Нотариусы сообщили о невозможности передать криптовалюту по наследству // Российская газета. – 23.05.2022. – URL: https://rg.ru/ (дата обращения: 08.05.2023).

3. Ключевская Н. Наследование цифровых активов: российский и зарубежный опыт. 2021 // СПС «Гарант» (дата обращения: 08.05.2023).

4. Яценко Т.С. Наследование цифровых прав. – 2019. – URL: https://urfac.ru/ (дата обращения: 08.05.2023).

Уймин Антон Григорьевич,
старший преподаватель
РГУ нефти и газа (НИУ) им. И.М. Губкина.
Греков Владимир Сергеевич,
учебный мастер
РГУ нефти и газа (НИУ) им. И.М. Губкина,
г. Москва

СТРАТЕГИИ МОБИЛЬНОЙ РАЗРАБОТКИ С ИСПОЛЬЗОВАНИЕМ Qt ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОГРАММАХ ПОДГОТОВКИ 10.00.00

С развитием мобильных технологий и все большим распространением смартфонов и планшетов растет и количество мобильных приложений, а с ними и риски, связанные с безопасностью[232].

[232] *Ланецкая А.Ю., Александрова Е.Н.* Современные угрозы информационной безопасности // Международный журнал гуманитарных и естественных наук. 2022. № 7-2. С. 192-195.

Однако обеспечение информационной безопасности в мобильной разработке является важным и актуальным вопросом, который требует особого внимания и разработки эффективных методов и подходов[233]. В связи с этим актуальными вопросами являются использование платформы Qt для создания безопасных мобильных приложений, а также рассмотрение стратегий обеспечения безопасности на примере программ подготовки 10.00.00.

На факультете комплексной безопасности ТЭК в РГУ нефти и газа (НИУ) им. И.М. Губкина успешно осуществлена апробация 36-часового курса «Проектирование и разработка приложений для мобильных устройств на платформе Qt».

Цель данной работы – проанализировать подходы к мобильной разработке с использованием платформы Qt в контексте информационной безопасности, а также рассмотреть вопрос целесообразности обучения специалистов работе с платформой в рамках программ подготовки 10.00.00.

Мобильные приложения стали неотъемлемой частью жизни современного человека, однако это также привело к возникновению ряда проблем в области информационной безопасности[234], а применение безопасных подходов в мобильной разработке имеет первостепенное значение для обеспечения защиты пользовательских данных и предотвращения возможных атак[235]. В целом безопасные подходы в мобильной разработке помогают снизить риски атак и утечек данных, укрепить доверие пользователей к приложению и повысить его конкурентоспособность на рынке. Применение таких подходов является необходимым условием успешной и безопасной работы мобильных приложений, что особенно важно в условиях постоянно возрастающих киберугроз и требований к защите данных.

---

[233] *Баитов И.А., Человечкова А.В*. Недооцененная угроза мобильных приложений. 2022. С. 24.

[234] *Титаренко Д.В., Москалёв В.А.* Информационная безопасность мобильных приложений. 2022.

[235] *Сергеева О.А., Алексеева Е.С.* Повышение уровня защищенности программного обеспечения за счет внедрения процессов безопасной разработки.

Qt – это кросс-платформенный фреймворк для разработки приложений, который используется для создания графических интерфейсов, веб-приложений и многих других типов программного обеспечения. Qt обеспечивает единый интерфейс для разработки приложений на различных платформах, таких как Android, iOS, Windows, macOS и Linux[236]. Среди преимуществ платформы Qt для мобильной разработки стоит отметить кроссплатформенность, высокую производительность, гибкость и расширяемость, а также разработку с использованием модели компонентов.

Qt предоставляет ряд возможностей и инструментов для обеспечения информационной безопасности при разработке мобильных приложений:

- наличие встроенных криптографических функций;
- безопасное сетевое взаимодействие;
- управление доступом и авторизацией;
- интеграция с системами обеспечения безопасности;
- регулярное обновление и исправление уязвимостей;
- открытый исходный код.

Анализ уязвимостей (CVE) показывает, что разработчики оперативно и успешно справляются с их устранением[237].

В целом платформа Qt предоставляет разработчикам мощные инструменты и возможности для создания безопасных мобильных приложений[238]. При правильном использовании и соответствии рекомендациям по обеспечению безопасности, Qt может стать надежной основой для разработки мобильных приложений с высоким уровнем защиты информации и данных пользователей.

Безопасное проектирование и кодирование являются одним из ключевых факторов успешной разработки безопасных мобиль-

---

[236] Tools for Each Stage of Software Development Lifecycle. URL: https://www.qt.io/ (дата обращения: 09.05.2023).

[237] QT: Security Vulnerabilities // CVE Details. URL: https://www.cvedetails.com/vulnerability-list/vendor_id-6363/QT.html (дата обращения: 09.05.2023).

[238] *Potter L.* Hands-on mobile and embedded development with Qt 5: Build apps for Android, iOS, and Raspberry Pi with C++ and Qt. 2019.

ных приложений[239]. Примеры безопасного кода Qt модулей приложений могут включать различные аспекты, такие как защита от SQL-инъекций, безопасное хранение паролей и обеспечение безопасности при передаче данных. Ниже приведены некоторые примеры безопасного кода в приложениях, использующих Qt:

- Защита от SQL-инъекций с использованием подготовленных выражений (Prepared Statements):

```
#include <QSqlQuery>
#include <QVariant>

void addUser(const QString &username, const
QString &password) {
        QSqlQuery query;
        query.prepare(«INSERT INTO users (username,
password) VALUES (:username, :password)»);
        query.bindValue(«:username», username);
        query.bindValue(«:password», password);
        query.exec();
}
```

- Безопасное использование сетевых соединений с применением TLS/SSL:

```
#include <QSslSocket>
#include <QTcpSocket>
#include <QHostAddress>

void setupSecureSocket(QSslSocket *socket, const
QString &host, int port) {
        socket->setProtocol(QSsl::TlsV1_3);
        socket-
>setPeerVerifyMode(QSslSocket::VerifyPeer);
        socket->connectToHostEncrypted(host, port);
        if (!socket->waitForEncrypted()) {
            // Обработка ошибки
```

[239] *Исаев А.С., Луценко О.И., Симанович А.А.* Сравнительный анализ существующих методик разработки безопасного программного обеспечения // Научно-технический вестник Поволжья. 2020. №. 5. С. 109-112.

```
        }
    }
```

- Безопасное хранение паролей с использованием хеширования и соли:

```
    #include <QCryptographicHash>
    #include <QByteArray>
    #include <QRandomGenerator>

    QString hashPassword(const QString &password,
const QByteArray &salt) {
        QByteArray hash = QCryptographi-
cHash::hash(password.toUtf8() + salt, QCryptographi-
cHash::Sha256);
        return QString::fromUtf8(hash.toHex());
    }

    QByteArray generateSalt() {
        return QRandomGenerator::global()-
>generate();
    }
```

Эти примеры иллюстрируют некоторые подходы к безопасному программированию при использовании Qt. Важно учитывать принципы безопасного кодирования, такие как принцип наименьших привилегий, проверка входных данных и разделение контроля, для создания безопасных и надежных приложений.

Тестирование и аудит безопасности приложения являются важными этапами разработки, позволяющими обнаружить и устранить уязвимости и проблемы[240]. Рекомендуется проводить статический анализ кода, динамическое тестирование и аудит конфигурации и настроек. Защита пользовательских данных в мобильных приложениях должна быть обеспечена на всех этапах их обработки. Кроме того, при разработке безопасного мобильного приложения важно учитывать все уровни, на которых может возникнуть угроза.

---

[240] *Гуцель Н.В., Брюховецкий А.А.* Аудит процессов тестирования мобильных и web-приложений // Мир компьютерных технологий. 2021. С. 113-117.

Используя различные стратегии обеспечения безопасности на всех уровнях, разработчики могут создавать мобильные приложения, которые обеспечивают надежную защиту данных и информации пользователей, а также устойчивость к кибератакам и другим угрозам.

Предложения по реализации программ подготовки 10.00.00 с использованием Qt

Применение Qt в обучающих программах по информационной безопасности может включать в себя следующие практические аспекты:

- Организация курсов по основам разработки безопасных приложений с использованием Qt, охватывающих темы безопасного кодирования, тестирования и аудита безопасности, а также использования инструментов и возможностей Qt для обеспечения безопасности данных.
- Проведение воркшопов и практических занятий по использованию Qt в разработке защищенных приложений, где участники могут применять полученные знания на практике и получать обратную связь от экспертов.
- Разработка и внедрение сертификационных программ для специалистов по информационной безопасности, которые знакомы с использованием Qt в разработке безопасных приложений. Сертификация может подтверждать профессиональные навыки и знания, а также повышать конкурентоспособность специалистов на рынке труда.
- Использование Qt для разработки мобильных и настольных приложений может обеспечить возможность создания визуализаций сетевой инфраструктуры и симуляций различных сценариев атак, позволяя студентам лучше понять принципы работы сетей и методы обнаружения и предотвращения киберугроз[241].

[241] *Уймин А.Г., Мельников Д.А.* Обзор средств моделирования сетевой инфраструктуры при подготовке специалистов по укрупненным группам специальностей 09.00. 00, 10.00. 00 // Наука. Информатизация. Технологии. Образование. 2021. С. 392-405.

Таким образом, использование Qt в реализации программ подготовки 10.00.00 позволит создавать качественные и эффективные обучающие ресурсы в области информационной безопасности. Комбинация теоретических знаний и практических навыков, приобретаемых в процессе изучения Qt, способствует формированию квалифицированных специалистов, способных разрабатывать безопасные мобильные приложения и предотвращать киберугрозы.

В ходе работы над статьей были рассмотрены основные подходы к мобильной разработке с использованием Qt, а также способы обеспечения информационной безопасности приложений на этой платформе. Qt предоставляет мощные инструменты и возможности для создания надежных, безопасных и высокопроизводительных мобильных приложений. Применение принципов безопасного кодирования, тестирования и аудита безопасности, а также использование функций и библиотек Qt для обработки пользовательских данных и защиты от киберугроз являются основными стратегиями обеспечения безопасности приложений.

Необходима реализация обучающих программ и курсов в области информационной безопасности. Примеры включают разработку мобильных и веб-приложений для обучения, а также проведение воркшопов и сертификационных программ. Эти инициативы помогут подготовить квалифицированных специалистов, способных разрабатывать безопасные мобильные приложения и обеспечивать защиту от киберугроз.

Для дальнейшего развития и применения Qt в мобильной разработке и информационной безопасности рекомендуется:

1. Продолжать исследования и разработку новых инструментов и функций Qt для улучшения безопасности и защиты данных в мобильных приложениях.

2. Разрабатывать и проводить специализированные обучающие курсы и программы для разработчиков, акцентируя внимание на безопасности приложений и практиках защиты данных с использованием Qt.

3. Сотрудничать с профессиональными сообществами и организациями в области информационной безопасности для обмена

знаниями, опытом и лучшими практиками, а также для улучшения стандартов и методологий разработки безопасных мобильных приложений на базе Qt.

4. Внедрять и продвигать использование Qt в учебных заведениях и организациях, осуществляющих подготовку специалистов в области информационной безопасности.

Библиографический список

1. Ланецкая А.Ю., Александрова Е.Н. Современные угрозы информационной безопасности // Международный журнал гуманитарных и естественных наук. – 2022. – № 7-2. – С. 192-195.

2. Баитов И.А., Человечкова А.В. Недооцененная угроза мобильных приложений // ББК [16.2+ 16.8] я43 Н 34. – 2022. – С. 24.

3. Титаренко Д.В., Москалёв В.А. Информационная безопасность мобильных приложений. – 2022.

4. Сергеева О.А., Алексеева Е.С. Повышение уровня защищенности программного обеспечения за счет внедрения процессов безопасной разработки.

5. Tools for Each Stage of Software Development Lifecycle. – Текст: электронный // Qt: [сайт]. – URL: https://www.qt.io/ (дата обращения: 09.05.2023).

6. QT: Security Vulnerabilities . – Текст : электронный // CVE Details : [сайт]. – URL: https://www.cvedetails.com/vulnerability-list/vendor_id-6363/QT.html (дата обращения: 09.05.2023).

7. Potter L. Hands-on mobile and embedded development with Qt 5: Build apps for Android, iOS, and Raspberry Pi with C++ and Qt. – Packt Publishing Ltd, 2019.

8. Исаев А.С., Луценко О.И., Симанович А.А. Сравнительный анализ существующих методик разработки безопасного программного обеспечения // Научно-технический вестник Поволжья. – 2020. – № 5. – С. 109-112.

9. Гуцель Н.В., Брюховецкий А.А. Аудит процессов тестирования мобильных и web-приложений // Мир компьютерных технологий. – 2021. – С. 113-117.

10. Уймин А.Г., Мельников Д.А. Обзор средств моделирования сетевой инфраструктуры при подготовке специалистов по укрупненным группам специальностей 09.00. 00, 10.00. 00 // Наука. Информатизация. Технологии. Образование. – 2021. – С. 392-405.

Пашнина Татьяна Викторовна,
к.ю.н., доцент кафедры государственно-правовых дисциплин Уральского филиала ФГБОУ ВО «Российский государственный университет правосудия»,
г. Челябинск

О ВЛИЯНИИ СОЦИОКУЛЬТУРНЫХ ФАКТОРОВ НА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Третье десятилетие XXI века отмечено небывалым усилением геополитической напряженности, спровоцировавшим рост угроз информационной безопасности страны, что актуализировало вопросы, связанные с формированием эффективного механизма им противодействия, создаваемого с учетом факторов, традиционно находящихся за гранью правовых исследований. К таким компонентам, в частности, относятся факторы социокультурные, оказывающие существенное влияние на обеспечение информационной безопасности личности, общества, государства, и, в отличие, например, от вопросов информационно-психологической безопасности[242], не нашедших должного теоретического осмысления.

[242] См., например: *Смирнов А.А.* Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации : дис. … д-ра юрид. наук. М., 2022. 444 с.; *Федорова О.Н.* Информационно-психологическая безопасность личности в информационном обществе // Вестник ИШ ДВФУ. 2011. № 2 (7). С. 21-34.

В условиях интенсивных угроз национальным интересам российского государства одним из ключевых условий обеспечения суверенитета страны и национальной безопасности, в том числе в информационной сфере, становится феномен национальной (общероссийской) гражданской идентичности, поскольку, как справедливо было отмечено на площадках Петербургского международного юридического форума 2023, «в современных внешнеполитических условиях сохранить свою идентичность – значит сохранить Россию как единство правового пространства, истории и культуры, основанное на традиционных российских духовно-нравственных ценностях»[243].

Документы стратегического планирования под общероссийской гражданской идентичностью понимают «осознание гражданами Российской Федерации их принадлежности к своему государству, народу, обществу, ответственности за судьбу страны, необходимости соблюдения гражданских прав и обязанностей, а также приверженность базовым ценностям российского общества»[244]. Исходя из приведенного определения, можно говорить о том, что на общегосударственном уровне понятие общероссийской гражданской идентичности выступает базовой правовой категорией, включающей в себя иные, более частные формы идентичности.

При этом ряд форм идентичности (включая социальную, культурную, языковую, этническую, правовую и т.д.) охватывается понятием «социокультурная идентичность», которая, в свою очередь, в реалиях попытки «отмены» достижений российской культуры рядом западных стран становится важнейшим фактором сохранения единства российского общества и обеспечения национальной безопасности государства, поскольку «охватывает важнейшую часть

[243] Правовые контуры российской идентичности. URL: https://legal-forum.info/ programme/business-programme/2759/ (дата обращения: 11.05.2023).

[244] О Стратегии государственной национальной политики Российской Федерации на период до 2025 года : Указ Президента РФ от 19 декабря 2012 г. № 1666 (ред. от 06.12.2018) // СЗ РФ. 2012. № 52, ст. 7477.

социального бытия, а именно духовно-психологическую, политико-правовую и нравственную атмосферу в обществе»[245].

По обоснованному мнению Е.Н. Барсуковой и И.Б. Романенко, «социокультурная идентичность обеспечивает силу и крепость нации, ее способность противостоять силам распада, провокациям (внутренним и внешним), представляя собой связанную систему идей, чувств, стереотипов мировосприятия как в ретроспективе, так и в перспективе»[246].

Важность культурной компоненты в структуре национальной идентичности подчеркивает положения важнейшего стратегического документа Российской Федерации – «Стратегии государственной национальной политики Российской Федерации на период до 2025 г.»[247], назвавшей «русскую культурную доминанту», «единый культурный (цивилизационный) код», присущий всем народам нашей страны, основой общероссийской гражданской идентичности.

В силу этого, в современных условиях противостояния странам так называемого «коллективного запада» социокультурная идентичность, означающая признание гражданами государства уникального самобытного культурного достояния (наследия) народов России в качестве базовой, объединяющей ценности, может рассматриваться как ключевой элемент формирования культурного суверенитета страны.

Культурный суверенитет, в свою очередь, неразрывно связан с категорией информационной безопасности, поскольку под таковым согласно положениям «Основ государственной культурной политики» (2014) понимается «совокупность социально-культурных

---

[245] *Дряева Э.Д., Дубровский Д.И.* Социокультурная идентичность в условиях современных коммуникаций и базовая идентичность индивида // Философские науки. 2017. № 8. С. 64.

[246] *Барсукова Е.Н., Романенко И.Б.* Социокультурная идентичность и национальный менталитет: урбантропологический подход // Общество. Среда. Развитие (Terra Humana). 2012. № 4. С. 193.

[247] О Стратегии государственной национальной политики Российской Федерации на период до 2025 года : Указ Президента РФ от 19 декабря 2012 г. № 1666 (ред. от 06.12.2018) // СЗ РФ. 2012. № 52, ст. 7477.

факторов, позволяющих народу и государству формировать свою идентичность, … быть защищенными от деструктивного идеологического и информационного воздействия»[248].

Тесную связь культуры и национальной безопасности подтверждает и анализ положений «Стратегии национальной безопасности РФ» (2021)[249], среди задач обеспечения последней назвавшей «защиту традиционных российских духовно-нравственных ценностей, культуры и исторической памяти» (пп. 84-93).

Основополагающий документ в области информационной безопасности – «Доктрина информационной безопасности РФ» (2016)[250], не оперирует категориями «идентичность» и «культурный суверенитет», однако в абз. к) п. 23 одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности называет «нейтрализацию информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей».

В данном контексте формирование механизма противодействия угрозам национальным интересам в информационной сфере, хотя и осуществляется в рамках создания системы обеспечения информационной безопасности, связано, помимо прочего, с укреплением социокультурной идентичности российского общества, важнейшим средством формирования и защиты которой выступает культурный суверенитет государства.

В силу вышеназванных обстоятельств наблюдается значительное взаимопроникновение и взаимовлияние информационного и культурного пространства Российской Федерации. Наиболее

---

[248] Об утверждении Основ государственной культурной политики : Указ Президента РФ от 24 декабря 2014 г. № 808 (ред. от 25.01.2023) // СЗ РФ. 2014. № 52, ч. 1 ст. 7753.

[249] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 02 июля 2021 г. № 400 // СЗ РФ. 2021. № 27, ч. 2 ст. 5351.

[250] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50, ст. 7074.

показательно это подтверждает факт принятия в конце прошлого года важнейшего стратегического акта в области как культурной, так и информационной безопасности – Указа Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»[251], назвавшего накопленный культурно-исторический опыт народа России главным средством противостояния деструктивному информационно-психологическому воздействию, позволяющим «своевременно и эффективно реагировать на новые вызовы и угрозы, сохраняя общероссийскую гражданскую идентичность».

Вышесказанное позволяет сделать выводы о том, что:

1. Построение эффективной системы обеспечения национальной безопасности в реалиях современных вызовов и угроз требует учета всего комплекса факторов и средств ее обеспечения, включая и социокультурные, обуславливающие влияние культуры на сохранение и укрепление общероссийской гражданской идентичности.

2. В данном контексте считаем возможным говорить о необходимости выделения информационно-культурологической составляющей в структуре информационной безопасности, в первую очередь, – информационно-психологической безопасности личности, поскольку в условиях взаимопроникновения и взаимовлияния информационного и культурного пространства, укрепление культурного суверенитета с опорой на традиционные духовно-нравственные ценности становится одним из важнейших средств противодействия деструктивной идеологии как наиболее радикальной формы негативного информационно-психологического воздействия, и, следовательно, – обеспечения как информационной безопасности отдельного гражданина, так и российского общества и государства в целом, что должно найти нормативное закрепление в системе правового регулирования института информационной безопасности.

---

[251] СЗ РФ. 2022. № 46, ст. 7977.

3. В свете необходимости консолидации усилий не только органов публичной власти, но и всех институтов гражданского общества по обеспечению национальной безопасности в информационной сфере, считаем также необходимым теоретическое осмысление и нормативное отражение того вклада, который способны внести традиционные информационные и культурные институты – архивы, библиотеки, музеи и др., а также образовательные организации, способствующие сохранению и трансляции культурных достижений многонационального народа Российской Федерации как внутри страны, так за рубежом, в обеспечение информационно-психологической безопасности российского общества и информационной безопасности государства в целом.

Библиографический список

1. Барсукова Е.Н., Романенко И.Б. Социокультурная идентичность и национальный менталитет: урбантропологический подход // Общество. Среда. Развитие (Terra Humana). – 2012. – № 4. – С. 193–196.

2. Дряева Э.Д., Дубровский Д.И. Социокультурная идентичность в условиях современных коммуникаций и базовая идентичность индивида // Философские науки. – 2017. – № 8. – С. 63–75.

Уймин Антон Григорьевич,
старший преподаватель
РГУ нефти и газа (НИУ) им. И.М. Губкина.
Морозов Илья Михайлович,
учебный мастер
РГУ нефти и газа (НИУ) им. И.М. Губкина,
г. Москва

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ЭЛЕМЕНТОВ ПОВЕДЕНЧЕСКОЙ БИОМЕТРИИ

С развитием технологий и увеличением числа онлайн-транзакций мошенничество становится все более сложным и разнообразным. Для борьбы с ним используются различные методы идентификации, в том числе биометрические. В данной статье рассматривается поведенческая биометрия, ее преимущества и методы применения.

Поведенческая биометрия – это процесс автоматического распознавания индивидов на основе их поведенческих характеристик[252]. В отличие от статической биометрии, основанной на физических признаках (например отпечатках пальцев или сетчатке глаз), поведенческая биометрия анализирует динамические аспекты поведения пользователя, такие как скорость печати, паттерны движения мыши или стиль нажатия на экран смартфона. Большим преимуществом поведенческой биометрии является ее способность собирать и анализировать огромное количество разнообразных данных. Это позволяет создать более многогранный профиль пользователя, увеличивая точность идентификации и уменьшая вероятность мошеннических действий. Кроме того, такой подход сложнее подделать, поскольку имитировать уникальные поведенческие особенности гораздо труднее, чем статические биометрические данные.

---

[252] *Уймин А.Г., Морозов И.М.* Сравнительный анализ инструментов непрерывной онлайн-аутентификации и систем обнаружения аномалий для постоянного подтверждения личности пользователя // T-Comm. 2022. № 5. URL: https://cyberleninka.ru/ (дата обращения: 06.05.2023).

Смартфоны являются одним из основных устройств, использующих поведенческую биометрию для аутентификации пользователей[253]. Они собирают информацию о поведении пользователя, такую как движения при наборе текста или навигации, и используют ее для создания уникального профиля, позволяющего отличить владельца устройства от мошенников.

Банки и финансовые учреждения также активно применяют поведенческую биометрию для предотвращения мошенничества и улучшения безопасности своих клиентов[254]. Они могут анализировать поведение пользователя при проведении транзакций, взаимодействии с интернет-банком или мобильными приложениями, чтобы определить аномалии и своевременно предотвратить потенциальные угрозы.

Крупные корпорации также могут использовать поведенческую биометрию для защиты своих сотрудников и корпоративных данных. Системы безопасности могут мониторить поведение сотрудников при доступе к ресурсам компании, выявляя необычные действия и предотвращая внутренние угрозы.

При использовании поведенческой биометрии важно соблюдать баланс между безопасностью и приватностью пользователей. Сбор и анализ большого количества данных требует строгого соблюдения законодательства о защите персональных данных и получения согласия пользователей на обработку их информации.

Российские стандарты определяют следующие инструменты поведенческой биометрической аутентификации:

Анализ манеры набора текста: ГОСТ Р ИСО/МЭК 30107-2014 «Информационная технология. Биометрия. Системы и средства

---

[253] *Рассохин Д.К., Лукащик Е.П.* Двухфакторная биометрическая система аутентификации // Прикаспийский журнал: управление и высокие технологии. 2021. № 4 (56). URL: https://cyberleninka.ru/ (дата обращения: 06.05.2023).

[254] *Васильев Т.В.* Правовое регулирование использования биометрии в банковской сфере и проблемы по ее охране // Проблемы экономики и юридической практики. 2019. № 5. URL: https://cyberleninka.ru/ (дата обращения: 06.05.2023).

биометрической защиты информации. Требования к алгоритмам, параметрам и процедурам тестирования».

Анализ манеры письма: ГОСТ Р 57585-2017 «Информационная технология. Биометрия. Требования к функциональным возможностям биометрических систем и компонентов, применяемых в них».

Анализ манеры ходьбы: ГОСТ Р ИСО/МЭК 30144-2017 «Информационная технология. Биометрия. Системы биометрической идентификации. Характеристики производительности».

К сожалению, в них описываются не все современные типы поведенческой биометрии и не определены параметры применимости. Наиболее распространенные инструменты поведенческой биометрической аутентификации включают в себя:

Анализ манеры письма: используется для аутентификации почерка. Анализируется угол наклона букв, размер и форма символов, скорость и стиль письма.

Анализ манеры ходьбы: используется для аутентификации личности по характеру походки. Анализируется длина и ширина шага, скорость ходьбы, манера движения и другие параметры.

Анализ манеры набора текста: используется для аутентификации пользователей, использующих клавиатуру или мышь. Анализируются ударение на клавиши, скорость набора, паузы и другие факторы.

Анализ голоса: используется для аутентификации личности по голосу. Анализируются высота, скорость и интонация голоса.

Анализ устройства ввода: используется для аутентификации устройств ввода, таких как сенсорные экраны или мыши. Анализируется стиль и скорость ввода данных на устройство ввода.

На основе открытых источников[255,256,257,258] и собственной экспертизы можно сделать вывод, что при работе с клавиатурой

---

[255] *Kasprowski P., Harezlak K.* Fusion of eye movement and mouse dynamics for reliable behavioral biometrics // Pattern Analysis and Applications. 2018. Т. 21. С. 91-103.

[256] *Sarkar A., Singh B.K.* A review on performance, security and various biometric template protection schemes for biometric authentication systems // Multimedia Tools and Applications. 2020. Т. 79. С. 27721-27776.

или устройствами ввода, с одной стороны, мы получаем достаточный объем данных для принятия решения с относительно высокой скоростью, но при этом есть проблема в точности и вероятности подделки данных. Эту проблему могут решить нейронные сети. Нейронные сети являются одним из ключевых инструментов в этой области, поскольку они способны обрабатывать и анализировать большие объемы данных, обеспечивая высокую точность идентификации. В таблице приведено сравнение методов по применимости в них технологий нейронных сетей.

Характеристика	**Анализ манеры письма**	**Анализ манеры ходьбы**	**Анализ манеры набора текста**	**Анализ голоса**	**Анализ устройства ввода**
Количество доступных данных	Среднее	Среднее	Высокое	Высокое	Среднее
Разнообразие исходных данных	Низкое	Среднее	Высокое	Высокое	Низкое
Сложность обработки данных	Средняя	Высокая	Средняя	Высокая	Низкая
Необходимость предобработки данных	Высокая	Средняя	Низкая	Средняя	Низкая
Объем требуемых вычислительных мощностей	Средний	Высокий	Средний	Высокий	Низкий
Время разработки и обучения	Среднее	Долгосрочное	Среднее	Долгосрочное	Краткосрочное
Устойчивость к изменениям в данных	Низкая	Средняя	Высокая	Средняя	Высокая
Точность идентификации	Средняя	Средняя	Высокая	Высокая	Средняя
Масштабируемость	Средняя	Высокая	Высокая	Высокая	Низкая
Применимость в разных отраслях	Ограниченная	Широкая	Широкая	Широкая	Широкая

[257] *Ackerson J.M., Dave R., Seliya N.* Applications of recurrent neural network for biometric authentication & anomaly detection // Information. 2021. Т. 12, №. 7. С. 272.

[258] *Zulfiqar M.* et al. Deep face recognition for biometric authentication // 2019 international conference on electrical, communication, and computer engineering (ICECCE). IEEE, 2019. С. 1-6.

Таким образом, можно сделать вывод, что наиболее эффективными при вопросах непрерывной онлайн аутентификации пользователей являются «Анализ манеры набора текста» и «Анализ устройства ввода». При этом вопросы «Анализ устройства ввода», таких как манипуляторы, выходят на первый план ввиду смены парадигм управления большинством интерфейсов пользовательских систем.

Нам видится наиболее перспективным анализ поведенческой биометрии на основе данных манипулятора. В рамках эксперимента введем следующие переменные и параметры:

N – количество участников;

R – количество записей на каждого участника;

T_i – продолжительность i-й записи;

M(x, y, i) – движение мыши на позиции (x, y) в i-й записи;

C_k(i) – количество щелчков кнопки k в i-й записи, где k ∈ {left, right, middle, wheel_up, wheel_down}

Тепловая карта H(x, y, i) для i-й записи вычисляется следующим образом:

H(x, y, i) = M(x, y, i) / Σ M(x, y, i) по всем (x, y),

где Σ обозначает сумму по всем клеткам сетки 10x10.

Распределение щелчков мыши D_k(i) для i-й записи вычисляется следующим образом:

D_k(i) = C_k(i) / Σ C_k(i) по всем k ∈ {left, right, middle, wheel_up, wheel_down}, где Σ обозначает сумму по всем типам щелчков мыши.

Используя H(x, y, i) и D_k(i) как признаки, можно применить различные методы машинного обучения, такие как нейронные сети, для классификации участников на основе их движений мыши и распределения щелчков.

Тепловая карта (heatmap) – это графическое представление данных, в котором значения переменных представлены цветами. Это позволяет наглядно увидеть плотность или частоту некоторых событий в разных областях. В контексте эксперимента с движениями мыши и щелчками тепловая карта используется для визуализации плотности движений мыши и щелчков на сетке 10x10 клеток.

Для создания тепловой карты на основе данных движений мыши сначала разобьем область экрана на сетку 10x10 клеток. Затем, для каждой клетки (x, y) подсчитаем количество движений мыши M(x, y, i) в данной клетке для i-й записи.

Теперь можно создать тепловую карту H(x, y, i) для i-й записи, нормализуя количество движений мыши в каждой клетке по сумме движений мыши для всех клеток:

$H(x, y, i) = M(x, y, i) / \Sigma M(x, y, i)$ по всем (x, y),

где Σ обозначает сумму по всем клеткам сетки 10x10.

Таким образом, тепловая карта H(x, y, i) представляет собой нормализованное распределение движений мыши на сетке 10x10 клеток для i-й записи, где значения H(x, y, i) находятся в диапазоне [0, 1], и сумма всех значений равна 1.

В ходе эксперимента показана обработка средних результатов проверки на 5 блоках кросс-валидации. Задачей для различных классификаторов была классификация человека (60 человек в наборе данных) на основе тепловой карты или тепловой карты с распределением кликов. Мы оценили каждый метод с использованием 5-блочной кросс-валидации и рассчитали среднюю точность. В нашем тесте наибольшую точность показал FineKNN 98,082 %. Для всех процедур мы использовали параметры по умолчанию для Matlab и не выполняли поиск по сетке для оптимальных параметров. Если проанализировать результаты тепловой карты и результаты тепловой карты с распределением кликов, то можно увидеть, что распределение кликов в большинстве случаев оказывает скорее отрицательное влияние. Это, безусловно, связано с тем, что мало индивидуального поведения отражается в поведении кликов, так как люди ограничены в своих кликах, и левая кнопка мыши, и прокрутка, вероятно, являются наиболее часто используемыми функциями. Эта оценка показывает, что движения мыши являются очень хорошим способом биометрической аутентификации пользователей на основе их поведения.

Библиографический список

1. Уймин А.Г., Морозов И.М. Сравнительный анализ инструментов непрерывной онлайн-аутентификации и систем обнаружения аномалий для постоянного подтверждения личности пользователя // T-Comm. – 2022. – № 5. – URL: https://cyberleninka.ru/ (дата обращения: 06.05.2023).

2. Рассохин Д.К., Лукащик Е.П. Двухфакторная биометрическая система аутентификации // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 4 (56). – URL: https://cyberleninka.ru/ (дата обращения: 06.05.2023).

3. Васильев Т.В. Правовое регулирование использования биометрии в банковской сфере и проблемы по ее охране // Проблемы экономики и юридической практики. – 2019. – № 5. – URL: https://cyberleninka.ru/ (дата обращения: 06.05.2023).

4. Kasprowski P., Harezlak K. Fusion of eye movement and mouse dynamics for reliable behavioral biometrics // Pattern Analysis and Applications. – 2018. – T. 21. – C. 91-103.

5. Sarkar A., Singh B.K. A review on performance, security and various biometric template protection schemes for biometric authentication systems // Multimedia Tools and Applications. – 2020. – T. 79. – C. 27721-27776.

6. Ackerson J.M., Dave R., Seliya N. Applications of recurrent neural network for biometric authentication & anomaly detection // Information. – 2021. – T. 12, № 7. – C. 272.

7. Zulfiqar M. et al. Deep face recognition for biometric authentication // 2019 international conference on electrical, communication, and computer engineering (ICECCE). – IEEE, 2019. – C. 1-6.

Филичкин Сергей Андреевич,
аспирант ФГБОУ ВО «Ижевский государственный технический университет им. М.Т. Калашникова», г. Ижевск

АЛГОРИТМ ИНТЕЛЛЕКТУАЛЬНОГО РАСПОЗНАВАНИЯ ОПЬЯНЕННОГО СОСТОЯНИЯ ЧЕЛОВЕКА ПО ВИДЕОПОТОКУ ДАННЫХ

Решение задачи определения трезвости человека имеет огромную важность для общества. Ведь управление транспортными средствами в нетрезвом состоянии приводит к непоправимым последствиям, таким как дорожно-транспортные происшествия и гибель людей. Поэтому использование различных технологий для решения этой задачи помогает снизить количество трагических случаев на дорогах.

Кроме того, решение задачи определения трезвости может быть использовано не только в транспорте. Например, на производстве, при выполнении работ, связанных с опасными веществами, такая технология может предотвратить производственные несчастные случаи[259].

Таким образом, решение задачи определения трезвости является неотъемлемой частью общественной безопасности и помогает предотвратить множество негативных последствий как на дорогах, так и в других сферах жизнедеятельности[260].

Цель исследования решения задачи определения трезвости человека заключается в создании эффективного алгоритма, который

---

[259] *Филичкин С.А.* Применение нейронных сетей для распознавания поведенческих функций человека // Экология и безопасность жизнедеятельности : сб. ст. XXI Междунар. науч.-практ. конф. Пенза : Пензенский государственный аграрный университет, 2021. С. 206–210.

[260] *Iwamura M., Mori S., Nakamura K., Tanoue T., Utsumi Y., Makihara Y., Muramatsu D., Kise K., Yagi Y.* Individuality-preserving silhouette extraction for gait recognition and its speedup // IEICE Trans. Inf. Syst. 2021. No. 7. Pp. 992–1001.

позволит быстро и точно определять состояние человека. Используя этот алгоритм, можно повысить уровень безопасности на предприятиях, а также предотвратить производственные и другие несчастные случаи, вызванные нахождением людей в нетрезвом состоянии.

Обзор литературы показывает, что на предприятиях и рабочих местах также проводятся исследования в области обнаружения нетрезвых людей. Основной метод для определения нетрезвой степени человека на рабочих местах – это анализ специальных биологических и дыхательных показателей.

В одном из исследований устанавливали вентиляционные системы на рабочих местах для более точного определения состояния сотрудников. Воздух, выдыхаемый работниками, проходил через датчики вентиляционной системы, а затем проходил через датчики, измеряющие уровень алкоголя или наркотиков в выдыхаемом воздухе[261]. Если был обнаружен высокий уровень алкоголя или наркотиков, вентиляционная система автоматически оповещала руководство о возможном нахождении нетрезвых работников и блокировала доступ к опасным местам[262].

Помимо этого, проводились исследования с использованием анализа голоса, который может показать изменения в голосе нетрезвых людей. При проведении этих исследований использовались различные акустические параметры, такие как тональность, скорость, амплитуда, длина фразы и другие. Известно о разработке специальных устройств на основе шейных датчиков, которые могут измерять изменения в поведении и стиле походки, что может быть связано с нетрезвым состоянием человека. Также существует исследование, предлагающее использовать технологии бесконтактного

---

[261] *Филичкин С.А.*, *Вологдин С.В.* Применение нейронной сети YOLOv5 для контроля соблюдения регламентов персонала на предприятии // Информационные технологии в науке, промышленности и образовании : сб. трудов Всерос. науч.-технической конф., Ижевск, 26–27 мая 2022 года. Ижевск : ИжГТУ им. М.Т. Калашникова, 2022. С. 73-80.

[262] *Park S., Bae B., Kang K., Kim H., Nam M.S., Um J., Heo Y.J.* A Deep-Learning Approach for Identifying a Drunk Person Using Gait Recognition. Appl. Sci. 2023, 13. Pp. 1390-1391.

измерения температуры кожи для обнаружения состояния нетрезвости у человека.

Основные проблемы, которые решались в предыдущих работах – это снижение риска возникновения аварийных ситуаций на рабочих местах, связанных с нетрезвыми работниками, а также повышение качества производства и снижение несчастных случаев на рабочих местах.

Также проводилось исследование с использованием сверхточных нейронных сетей, где пытались определить состояние человека по длине шага, времени шага и скорости шага, однако набор данных был небольшим, и определять состояние человека получалось только имея данные о его обычной походке и нарушенной[263].

Алгоритм для решения задачи распознавания состояния человека будет состоять из следующих шагов (рис. 1):

1. Определение неуверенной походки: для этого необходимо провести анализ данных с видеокамеры. Система должна определить, насколько полученные данные соответствуют неуверенной походке. Это можно определить, учитывая скорость передвижения, используя сверточные нейронные сети.

2. Определение падения: система должна иметь программный модуль, который будет способен выявлять падения или нестандартные позы человека, что также требует использования сверточных нейронных сетей.

3. Определение шатания: для этого система должна анализировать данные с видеокамеры, которые позволят определить, насколько прямолинейно или в рамках допустимого коридора двигается человек.

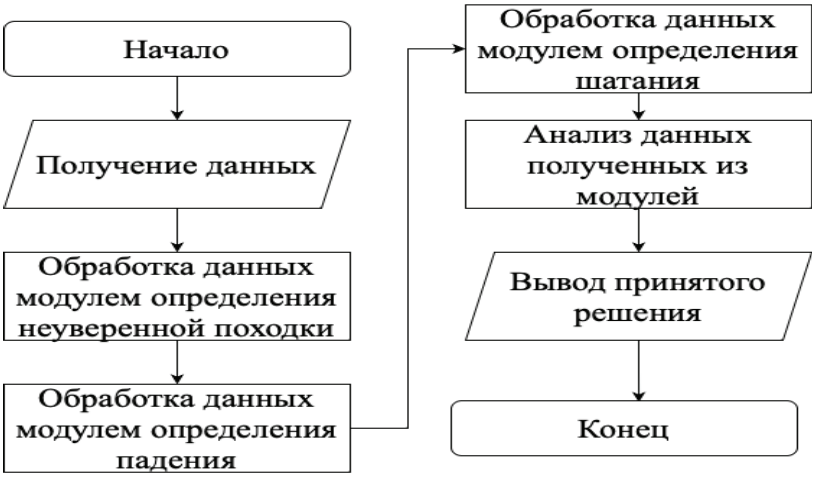
4. Обработка и анализ данных: система должна проанализировать данные, полученные на первых трех этапах, и определить, соответствует ли поведение человека признакам нетрезвости.

---

[263] *Prakash C.; Kumar R.; Mittal N.* Recent developments in human gait research: Parameters, approaches, applications, machine learning techniques, datasets and challenges // Artif. Intell. Rev. 2018. Pp. 1–40.

5. Вынесение решения: на основании анализа данных система должна вынести решение о нахождении человека в нетрезвом состоянии, используя рейтинг состояния, если он выше определенного порога, то сообщить об этом оператору.

Рис. 1. Алгоритм распознавания состояния человека



Оптимальной архитектурой нейронной сети для данной задачи может быть сверточная сеть с несколькими сверточными слоями, слоями Pooling, полносвязными слоями и dropout-слоями для регуляризации, например YOLOv8. Также необходимо использовать алгоритмы машинного обучения, такие как K-Nearest Neighbor (KNN), Support Vector Machines (SVM) и Random Forest.

В качестве метрик для оценки результатов будут использоваться Accuracy, Precision, Recall и F1-score. Accuracy определяет общую точность метода на тестовом наборе данных. Precision – отношение числа правильно обнаруженных объектов к числу всех обнаруженных объектов, Recall – отношение числа правильно обнаруженных объектов к числу всех объектов, которые следовало бы обнаружить, F1-score – среднее гармоническое между Precision и Recall.

Данные, необходимые для работы алгоритма, включают данные с видеокамеры и большой обучающий набор данных,

содержащий в себе сведения о различных походках человека, положение тела в пространстве, а также примеры передвижения человека на дистанцию[264].

Кроме того, для улучшения результатов можно использовать техники аугментации данных, такие как изменение яркости, перспективное преобразование и поворот изображений, а также fine-tuning модели на конкретных данных для улучшения ее точности для конкретной задачи. Также можно использовать различные оптимизаторы для улучшения обучения модели, например adaptive moment estimation (adam) или Stochastic gradient descent (SGD).

Алгоритм можно применять в следующих случаях:

1. Для контроля за состоянием работников, особенно за теми, которые занимаются опасными видами деятельности, такими как работа с машинами, вышками, электроустановками и т.п.

2. Для проверки водителей, которые работают с транспортными средствами компании[265].

3. Для обеспечения безопасности на производственных площадках и складах.

4. Для контроля за использованием алкоголя и наркотиков в рабочее время.

Преимущества использования алгоритма:

1. Повышение уровня безопасности на предприятии.

2. Снижение риска несчастных случаев и производственных травм[266].

---

[264] *Kao H.L., Ho B.J., Lin A.C., Chu H.H.* Phone-based gait analysis to detect alcohol usage. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing, Pittsburgh, PA, USA, 5–8 September, 2012. Pp. 661–662.

[265] *Park E., Lee S.I., Nam H.S., Garst J.H., Huang A., Campion A., Arnell M., Ghalehsariand N., Park S., Chang H.J.*, et al. Unobtrusive and continuous monitoring of alcohol-impaired gait using smart shoes. Methods Inf. Med. 2017. Pp. 74–82.

[266] *Ворожцова Н.А., Вологдин С.В.* Подготовка набора данных для распознавания показаний с фотографий лицевых панелей приборов учета электроэнергии // Вестник Российского нового университета. Сер. «Сложные системы: модели, анализ и управление». 2020. № 4. С. 121–126.

3. Возможность снижения затрат на охрану труда, за счет автоматизации некоторых процессов.

4. Предотвращение неэффективного использования ресурсов, так как нетрезвые работники могут снижать производительность работы.

5. Оптимизация управления рисками[267].

Полученные результаты такого исследования имеют большую важность для современных технологий, связанных с разработкой систем безопасности, так как могут быть использованы для создания программных и аппаратных комплексов, обеспечивающих безопасность на предприятиях[268]. Разработка подобных комплексов и систем является актуальной задачей современного мира, где все больше внимания уделяется защите прав и безопасности людей, работающих на производстве.

Библиографический список

1. Филичкин С.А. Применение нейронный сетей для распознавания поведенческих функций человека // Экология и безопасность жизнедеятельности : сб. ст. XXI Междунар. науч.-практ. конф. – Пенза : Пензенский гос. аграрный ун-т, 2021. – С. 206–210.

2. Iwamura M., Mori S., Nakamura K., Tanoue T., Utsumi Y., Makihara Y., Muramatsu D., Kise K., Yagi Y. Individuality-preserving silhouette extraction for gait recognition and its speedup // IEICE Trans. Inf. Syst. – 2021. – No.7. – Pp. 992–1001.

3. Филичкин С.А., Вологдин С.В. Применение нейронной сети YOLOv5 для контроля соблюдения регламентов персонала на предприятии // Информационные технологии в науке, промышленности и образовании : сб. трудов Всерос. науч.-технической

[267] *Saleh A.M., Hamoud T.* Analysis and best parameters selection for person recognition based on gait model using CNN algorithm and image augmentation // J. Big Data. 2021. Pp. 1–20.

[268] *Arnold Z., Larose D., Agu E.* Smartphone inference of alcohol consumption levels from gait. In Proceedings of the 2015 International Conference on Healthcare Informatics, Dallas, TX, USA, 21–23 October 2015. Pp. 417–426.

конф., Ижевск, 26–27 мая 2022 года. – Ижевск : ИжГТУ им. М.Т. Калашникова, 2022. – С. 73-80. – EDN YERSAG.

4. Park S., Bae B., Kang K., Kim H., Nam M.S., Um J., Heo Y.J. A Deep-Learning Approach for Identifying a Drunk Person Using Gait Recognition. Appl. Sci. – 2023, 13. – Pp. 1390-1391.

5. Prakash C.; Kumar R.; Mittal N. Recent developments in human gait research: Parameters, approaches, applications, machine learning techniques, datasets and challenges // Artif. Intell. Rev. – 2018. – Pp. 1–40.

6. Kao H.L., Ho B.J., Lin A.C., Chu H.H. Phone-based gait analysis to detect alcohol usage. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing, Pittsburgh, PA, USA, 5–8 September, 2012. – Pp. 661–662.

7. Park E., Lee S.I., Nam H.S., Garst J.H., Huang A., Campion, A., Arnell M., Ghalehsariand N., Park S., Chang H.J., et al. Unobtrusive and continuous monitoring of alcohol-impaired gait using smart shoes. Methods Inf. Med. – 2017. – Pp. 74–82.

8. Ворожцова Н.А., Вологдин С.В. Подготовка набора данных для распознавания показаний с фотографий лицевых панелей приборов учета электроэнергии // Вестник Российского нового университета. Сер. «Сложные системы: модели, анализ и управление». – 2020. – № 4. – С. 121–126. DOI 10.25586/RNU.V9187.20.04. pp. 121.

9. Saleh A.M., Hamoud T. Analysis and best parameters selection for person recognition based on gait model using CNN algorithm and image augmentation // J. Big Data. – 2021. – Pp. 1–20.

10. Arnold Z., Larose D., Agu E. Smartphone inference of alcohol consumption levels from gait. In Proceedings of the 2015 International Conference on Healthcare Informatics, Dallas, TX, USA, 21–23 October 2015. – Pp. 417–426.

Дубень Андрей Кириллович,
научный сотрудник Института государства
и права Российской академии наук,
г. Москва

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРАВОВОЙ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ

В условиях глобальной цифровой трансформации всех сфер жизнедеятельности, а также обострившихся геополитических противоречий и усиления межгосударственного информационного противоборства особенно актуально обеспечение информационной безопасности государства, общества и гражданина. В связи с этим чрезвычайно важно правовое обеспечение информационной безопасности как на национальном, так и международном уровнях. Это определяет приоритетность государственной политики Российской Федерации в области обеспечения национальной безопасности в информационной сфере, требующей научного осмысления правовых проблем информационной безопасности в условиях новых вызовов и угроз.

По результатам диссертационного исследования следует отметить, что в настоящее время правовое обеспечение информационной безопасности занимает особое место не только в системе информационного права, но и является одним из приоритетных направлений в системе обеспечения национальной безопасности Российской Федерации. В этой связи в условиях динамичного роста информационно-телекоммуникационных технологий важными представляются задачи противодействия угрозам и рискам в информационной сфере, которые сегодня определены стратегическими правовыми актами, базирующимися на комплексном подходе.

Значение правового обеспечения информационной безопасности определено целым рядом документов стратегического планиро-

вания, таких как Стратегия национальной безопасности[269], Стратегия комплексной безопасности детей в Российской Федерации[270], Основы государственной политики в области международной информационной безопасности[271], утвержденных указами Президента Российской Федерации и актами Правительства Российской Федерации. Эти нормативные правовые акты являются базовыми в системе документов стратегического планирования, которые требуют научного осмысления с позиции информационного права, поскольку сегодня в эпоху активных процессов цифровой трансформации, общемирового кризиса и геополитических рисков остро ощутимо их влияние и на систему права.

Вместе с тем в условиях трансформации права и цифровизации всех сфер жизнедеятельности решение задач обеспечения национальной безопасности требует разработки теоретико-методологических вопросов информационной безопасности[272]. Так, в Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации указано, что одним из механизмов реализации повышения уровня культуры информационной безопасности граждан является создание условий для системной работы по включению в образовательную программу

---

[269] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 2 июля 2021 г. № 400 // СЗ РФ. 2021. № 27 (ч. 2). Ст. 5351.

[270] О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года : Указ Президента РФ от 17 мая 2023 года № 358 // СЗ РФ. № 21. Ст. 3696.

[271] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 2 июля 2021 г. № 400 // СЗ РФ. 2021. № 27 (ч. 2). Ст. 5351.; Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : Указ Президента РФ от 12 апреля 2021 г. № 213 // СЗ РФ. 2021. № 16 (ч. 1). Ст. 2746.

[272] *Полякова Т. А., Камалова Г. Г.* Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. 2022. № 2 (68). С. 114.

уроков по повышению грамотности по вопросам информационной безопасности[273].

Вместе с тем в Доктрине информационной безопасности Российской Федерации одной из угроз информационной безопасности является отсутствие на должном уровне развития конкурентоспособных информационных и компьютерных технологий, а также обеспечение кадрового резерва специалистов информационных систем[274].

Таким образом, важное значение для сферы обеспечения информационной безопасности имеет подготовка компетентных кадров, включая как специалистов в сфере собственно информационных технологий (программистов, тестировщиков, системных администраторов и других), так и специалистов по защите информации. При этом следует отметить, что кадровая подготовка на уровне бакалавриата, специалитета и магистратуры, имея комплексный характер, требует совершенствования учебно-методических материалов, направленных на формирование правовых знаний и правовой культуры. Однако, как правило, подготовка квалифицированных кадров в сфере обеспечения информационной безопасности осуществляется техническими вузами, которые не имеют достаточный профессорско-преподавательский состав в области права.

Вместе с тем на сегодняшний день в условиях нарастающей сложности геополитической обстановки и увеличения количества кибератак на информационные ресурсы при предотвращении угроз информационной безопасности и обеспечения национальных интересов в информационной сфере проводится работа по подготовке и переподготовке кадров в информационной сфере, проведение бето-тестирования программного оборудования по выявлению

---

[273] Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации : распоряжение Правительства РФ от 22.12.2022 № 4088-р // СЗ РФ. 2022. № 52. Ст. 9726.

[274] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

уязвимости информационных рисков и угроз. Формирование единого обучения специалистов в сфере информационных технологий потребовало создание единого центра Национального киберполигона. В Совете безопасности Российской Федерации особо отмечается: «В текущей ситуации для нас особенно важно оперативно обучать специалистов компетенциям, обеспечивающим кибербезопасность страны в Национальных киберполиганах, в которых не только студенты, а также сотрудники региональных IT-компаний смогут отрабатывать практические навыки защиты от киберугроз»[275].

Банк России в соответствии с документом «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов» отметил, что в сфере информационной безопасности наблюдается дефицит кадров и недостаточно высокий уровень их подготовки. В целях совершенствования организационных мер обеспечения информационной безопасности предлагается совместно с федеральными органами исполнительной власти развивать государственные образовательные стандарты высшего образования для подготовки специалистов по информационной безопасности посредством формирования требований к образованию и направлениям подготовки специалистов по информационной безопасности и разработки методических рекомендаций по подготовке соответствующих специалистов. Тем самым разработка обучающих программ для образовательных учреждений позволит сформировать единые стандарты качества подготовки практико-ориентированных специалистов в области информационной безопасности[276].

В этой связи следует отметить, что для снижения вероятности проявления угроз информационной безопасности требуется

---

[275] Чернышенко: в РФ в 2022 году создадут два новых центра Национального киберполигона // Информационное агенство «Интерфакс». URL: https://academia.interfax.ru/ru/news/articles/8136/ (дата обращения: 10.06.2023).

[276] Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов (Документ опубликован не был) // СПС «КонсультантПлюс».

принятие организационно-правовых мер, включая совершенствование кадрового потенциала и образовательной системы по подготовке специалистов в сфере обеспечения информационной безопасности, разработки и применения современных цифровых технологий. Ученые-исследователи констатируют тот факт, что сегодня отсутствует металогическая основа правовых и организационных решений при выделении образовательных стандартов, при этом важность данной темы определена тем, что в условиях трансформации системы права важная роль отнесена образовательному процессу[277].

Как справедливо отмечают Т.А. Полякова, Н.А. Троян, на современном этапе развития высшего образования создаются специальные образовательные модули по информационной безопасности в технических вузах, которые направлены на формирование профессиональных компетенций по защите информационных ресурсов, включая защиту критически важных информационных объектов[278].

Все указанное ранее позволяет делать вывод о том, что для развития организационно-правовых мер информационной безопасности необходимо формирование единых концептуальных подходов к обеспечению состояния защищенности от внутренних и внешних угроз в информационной сфере, в котором немаловажную роль в организации защиты информации играет кадровое обеспечение, непосредственно связанное с прогнозированием потребности в специалистах и повышения качества подготовки соответствующих научных и технических кадров.

На основе проведенного анализа государственной информационно-правовой политики в рассматриваемой сфере полагаем,

---

[277] *Полякова Т. А.* Правовое обеспечение информационной безопасности в системе юридического образования в условиях цифровизации // Юридическое образование и юридическая наука в России: современные тенденции и перспективы развития: (к 15-летию юридического факультета Курского государственного университета) : сб. материалов Всерос. науч.-практ. конф., Курск, 24–25 мая 2019 года. Курск : Курский гос. ун-т, 2019. С. 67.

[278] *Полякова Т. А., Троян Н. А.* Образование и культура информационной безопасности граждан Российской Федерации: научно-правовые аспекты // Образование и право. 2023. № 3. С. 315.

что ее реализация тесно связана с развитием и совершенствованием законодательства в области обеспечения информационной безопасности в России. Это позволяет сделать вывод о том, что правовое обеспечение информационной безопасности будет реализовываться посредством соблюдения Конституции Российской Федерации, российского законодательства, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению национальной информационной безопасности, развитие международного сотрудничества в сфере обеспечения информационной безопасности и развитие цифровых технологий, правовое равенство всех участников процесса информационного взаимодействия; приоритетное развитие отечественных современных цифровых технологий и их компонентов, формирование цифровой доверенной среды и обеспечение доступа к достоверной информации, цифрового и технологического суверенитета России.

Библиографический список

1. Полякова Т. А. Правовое обеспечение информационной безопасности в системе юридического образования в условиях цифровизации // Юридическое образование и юридическая наука в России: современные тенденции и перспективы развития: (к 15-летию юридического факультета Курского государственного университета) : сб. материалов Всерос. науч.-практ. конф., Курск, 24–25 мая 2019 года. – Курск : Курский гос. ун-т, 2019. – С. 64-70.

2. Полякова Т. А., Камалова Г. Г. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. – 2022. – № 2 (68). – С. 112-121.

3. Полякова Т. А., Троян Н. А. Образование и культура информационной безопасности граждан Российской Федерации: научно-правовые аспекты // Образование и право. – 2023. – № 3. – С. 310-317.

Яковлева Елена Александровна,
ведущий специалист-эксперт группы информационного обеспечения и оказания государственных услуг в электронном виде Управления по вопросам миграции МВД по Удмуртской Республике, г. Ижевск

РОЛЬ ЦИФРОВОЙ ДОВЕРЕННОЙ СРЕДЫ В ФЕДЕРАЛЬНОМ ОРГАНЕ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Вопрос создания цифровой доверенной среды в государственных учреждениях Российской Федерации на сегодняшний день является одним из приоритетных, поскольку трансформация цифровых технологий происходит во всех областях и отраслях современного общества. Обществу со стороны государства гарантируется обеспечение прав и свобод гражданина, свободный поиск и передача информации, обеспечение целостности, доступности и конфиденциальности информации, а также правовое регулирование, направленное на построение здорового информационного общества.

Преимущественным видом обработки информации являются персональные данные, в связи с чем возникающие информационные отношения в цифровой доверенной среде между федеральным органом исполнительной власти[279] и гражданином подлежат нормативному правовому регулированию со стороны государства.

Взаимодействие в цифровой доверенной среде между участниками информационных отношений должно строиться на доверии, минимизируя риски, снижая неопределенность выбора во взаимоотношениях в цифровой среде, где регулятором информационных правоотношений становится федеральный орган, отвечающий за приём, обработку и передачу информации по защищенным каналам. В цифровой доверенной среде стратегически главное обстоятельство, требующее регуляторного влияния, – укрепление доверия

[279] Далее – ФОИВ.

к информационному ресурсу, к информационному процессу и организации, участвующей в информационном взаимодействии. Совокупность правовых механизмов и практических механизмов, направленных на обеспечение защиты информации и информационных систем в цифровом пространстве, представляет собой правовую защиту информации цифровой доверенной среды.

В результате цифровая доверенная среда – цифровое пространство, обеспечивающее безопасный приём, обработку и передачу информации по защищенным каналам, созданное комплексом мер и средств защиты для обеспечения безопасности конфиденциальной информации и информационных систем[280].

Этапами создания цифровой доверенной среды в ФОИВ являются: правовой, организационный, инженерно-технический, программно-аппаратный.

Правовая защита информации представляет собой нормы действующего законодательства, регулирующие целостность, доступность и конфиденциальность информации от внешних и внутренних угроз в цифровой доверенной среде: международные договоры и соглашения, конституция РФ, федеральные законы, законы субъектов, указы и распоряжения, локальные акты, обеспечивающие информационную безопасность в ФОИВ.

Приведенный выше перечень регулирует отношения между участниками информационного процесса, защищает информацию от несанкционированного доступа, накладывает ограничения на распространение конфиденциальной информации, предотвращает использование критичного программного обеспечения в цифровой доверенной среде ФОИВ.

Правовая защита информации цифровой доверенной среды ФОИВ – это совокупность правовых норм, регулирующих цифровые отношения, возникающие и реализующиеся как в информационной среде, так и в различных сферах общественной жизни.

---

[280] *Яковлева Е.А.* Правовое обеспечение цифровой доверенной среды учетов по вопросам миграции // Информационное право. 2022. № 3(73). С. 22-24.

Правовая защита обусловлена необходимостью изучения процессов цифровизации и правовой природы цифровых технологий, цифровых данных и складывающихся цифровых отношений. Правовое регулирование отношений в цифровой доверенной среде выступает в виде совокупности правовых регуляторов, использующих потенциально определенный набор методов, приёмов и средств, способных контролировать и развивать отношения в ней.

Цифровая доверенная среда формирует круг общественных цифровых правоотношений и направлена на разработку и принятие регуляторных решений в виде правил и требований, адресованных участникам, регулируемых и контролируемых контрольно-надзорными органами, с целью их реализации и выявления последствий применения к субъектам соответствующих правоотношений.

Организационная защита цифровой доверенной среды ФОИВ представляет собой «установление особого режима конфиденциальности; ограничение доступа к конфиденциальной информации; использование организационных мер защиты информации; осуществление контроля за соблюдением установленного режима конфиденциальности»[281].

Организационная защита информации позволит установить специальный режим, включающий в себя охрану помещений, правила обработки информации, содержание носителей информации, а также обеспечить контроль за соблюдением требований норм технической эксплуатации цифровой доверенной среды ФОИВ. Стадия организационной защиты информации позволит определить источники угроз защищаемой информации, виды конфиденциальной информации, обрабатываемой в цифровой доверенной среде ФОИВ; основные каналы утечки информации; организовать допуск и доступ к конфиденциальной информации, организацию работы персонала и т.д.

---

[281] *Петухов К.В., Стригунов Ю.В., Сырвачев П.Р.* Организационные меры по защите информации при использовании средств криптографической защиты информации // Современные проблемы и пути их решения в науке, производстве и образовании. 2016. № 1. С. 90-93.

Как верно отмечает Л.А. Домбровская: «Организационная защита информации на предприятии – регламентация производственной деятельности и взаимоотношений субъектов (сотрудников пред-приятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию»[282], тем самым организуя мероприятия по обеспечению безопасности цифровой доверенной среды ФОИВ.

Основная цель инженерно-технического этапа – комплекс мер защиты информации в цифровой доверенной среде, обеспечивающий передачу информации по техническим каналам. Согласно организационно-правовым методам защиты выбираются технические средства защиты цифровой доверенной среды, в основном отечественное программное обеспечение, сертифицированное по требованиям безопасности. Установка такого программного обеспечения производится только на аттестованное рабочее место во исполнение требований Приказа Федеральной службы по техническому и экспортному контролю от 29 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

С учетом приведения в соответствие с действующим законодательством требований необходимого помещения производится установка основных технических средств и систем и вспомогательных технических средств и систем.

К основным техническим средствам защиты информации относятся: устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.); устройства для шифрования информации.

---

[282] *Домбровская Л.А., Васютина Т.Л.* Организационные средства защиты информации как элемент общей системы защиты информации // European Science. 2016. № 11(21). С. 21-25.

Постановлением Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» определено понятие технической защиты конфиденциальной информации – «выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней».

К техническим средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств компьютерных систем[283] и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности[284]. Критерием отнесения устройства к техническим, а не к инженерно-техническим средствам защиты, является обязательное включение в состав технических средств компьютерных систем.

Таким образом, инженерная защита информации представляет собой набор средств защиты информации выделенного помещения путем недопущения утечки информации через акустические видовые (окна, двери, стены и т.д.) каналы с целью обеспечения защиты информации в цифровой доверенной среде ФОИВ.

Программно-аппаратные средства защиты информации цифровой доверенной среды ФОИВ призваны обеспечить противодействие злоумышленнику при возможности его физического доступа к автоматизированным рабочим местам.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного

---

[283] *Хлыстова Д.А., Коробчинская В.А.* Методика построения инженерно-тех-нической защиты информации на примере объекта информатизации // Символ науки: международный научный журнал. 2016. № 12-2(24). С. 118-120.

[284] Программные и технические средства защиты информации. URL: https://specialitet.ru/lekcyi/eb/lekcyy_modul_7_vopros_6.pdf.

обеспечения компьютерных систем исключительно для выполнения защитных функций[285].

К основным программным средствам защиты информации относятся: программы идентификации и аутентификации пользователей компьютерных систем; программы разграничения доступа пользователей к ресурсам компьютерных систем; программы шифрования информации; программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т.п.) от несанкционированного изменения, использования и копирования.

Таким образом, цифровая доверенная среда в ФОИВ осуществляет минимизацию рисков реализации информационных угроз и контроль за их показателями, усиление роли защиты прав граждан, повышение удобства и качества предоставляемых услуг, повышение доверия к федеральным органам исполнительной власти, увеличение значимости информационной безопасности, а также внедрение постоянно возникающих прорывных и перспективных цифровых технологий, позволяющих создать условия для безопасного оборота цифровых услуг, посредством установления соразмерных требований к информационной безопасности и защите информации в этой сфере.

Библиографический список

1. Яковлева Е.А. Правовое обеспечение цифровой доверенной среды учетов по вопросам миграции // Информационное право. – 2022. – № 3(73). – С. 22-24.

2. Петухов К.В., Стригунов Ю.В., Сырвачев П.Р. Организационные меры по защите информации при использовании средств криптографической защиты информации // Современные проблемы и пути их решения в науке, производстве и образовании. – 2016. – № 1. – С. 90-93.

[285] Программные и технические средства защиты информации. URL: https://specialitet.ru/lekcyi/eb/lekcyy_modul_7_vopros_6.pdf.

3. Домбровская Л.А., Васютина Т.Л. Организационные средства защиты информации как элемент общей системы защиты информации // European Science. – 2016. – № 11(21). – С. 21-25.

4. Хлыстова Д.А., Коробчинская В.А. Методика построения инженерно-технической защиты информации на примере объекта информатизации // Символ науки: международный научный журнал. – 2016. – № 12-2(24). – С. 118-120.

Осетров Станислав Леонидович,
аспирант ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

РИСКИ И ПРОБЛЕМЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЦИФРОВИЗАЦИИ СУДОПРОИЗВОДСТВА

Электронные технологии коренным образом меняют современный мир. Не является исключением и сфера отправления правосудия. Развитие информатизации происходит настолько быстро, что даже специалисты могут потерять представление о последних изменениях и об их общем масштабе.

Внедрение электронного правосудия, то есть использование цифровых технологий для повышения его прозрачности, эффективности и доступности, стало необходимым условием модернизации любой судебной системы. В последние годы электронные технологии судопроизводства активно применяются и в России, что привело к технологизации гражданского и уголовного процесса по всей стране.

Существенный толчок в развитии цифрового судопроизводства произошел по вынужденной причине – в связи с последствиями новой коронавирусной инфекции. По причине введенных карантинных мер, обусловленных высокими темпами распространения пандемии, российскому судебному сообществу пришлось принять исключительные меры. Временная приостановка личного приема граждан кратно увеличила нагрузку на электронные сервисы правосудия.

Несмотря на то, что цифровизация судебной системы, как правило, представляется как безусловно позитивный процесс, возникают отдельные риски и проблемы, в том числе связанные с информационной безопасностью, не являвшиеся актуальными при традиционном способе отправления правосудия.

Постановление X Всероссийского съезда судей от 01.12.2022 № 1 «О развитии судебной системы Российской Федерации» определило: «Несмотря на то, что Российская Федерация занимает одно из ведущих мест в Европе по внедрению судами современных технологий ... одной из приоритетных задач дальнейшего развития судебной системы на современном этапе является технологическая модернизация судов, активное внедрение цифровых технологий и расширение сферы применения электронного правосудия. Необходима правовая база, разработка которой уже началась, включающая необходимость создания единой электронной платформы базы данных всех органов власти и управления»[286].

Эксперты «Центра развития современного права» в 2020 году подготовили аналитический доклад о состоянии и перспективах информационных технологий в правосудии[287]. По мнению авторов доклада, завышенные требования к степени защиты информации могут стать существенным препятствием для внедрения дистанционного правосудия. Указывается, что « …избыточные и не вполне обоснованные требования к защите информации при использовании системы веб-конференции по отношению к участникам судебных процессов (например шифрование данных, передача их исключительно по закрытым ведомственным каналам, создание изолированных «доверенных кабинетов» и т.п.) способны полностью

---

[286] О развитии судебной системы Российской Федерации : Постановление X Всероссийского съезда судей от 01.12.2022 № 1 // СПС «КонсультантПлюс».

[287] Информационные технологии в правосудии: состояние и перспективы. Россия и мир. Аналитический доклад // НИУ «ВШЭ». URL: http://цpсп.рф/wp-content/uploads/2020/07/tezis-informacionnie-tehnologii-v-pravosudii.pdf (дата обращения: 12.05.2023).

дезавуировать преимущества дистанционного правосудия … практика продемонстрировала надуманность проблем, связанных с недостаточной защитой информации. На данный момент отсутствуют сведения о каких-либо случаях злоупотреблений, свидетельствующих о критической уязвимости применяемой в настоящее время системы с точки зрения обеспечения процессуальных гарантий сторон либо защиты информации. Требования по защите информации должны быть оправданными с учетом вида процесса и конкретных обстоятельств дела, предъявляться не по принципу «чем больше, тем лучше», а быть сбалансированными с принципом доступности судопроизводства»[288].

Эксперты отмечают, что при оценке рисков необходимо учитывать уже имеющийся реальный опыт отечественных и зарубежных судов. Так, практика свидетельствует о том, что эффективность ограничения участия посторонних лиц в процессах путем применения таких технологий, как использование электронной подписи, верификации посредством порталов ЕСИА, визуальной проверки удостоверяющих личность документов, а также базового использования средств криптографии, является достаточной. Удобной стала бы автоматическая синхронизация данных об участниках процесса со сведениями государственных информационных систем. При этом, по мнению авторов доклада, более строгие методы защиты информации могут допускаться в отдельных случаях, таких как уголовное судопроизводство, заседания в закрытом режиме, процессы с участием несовершеннолетних[289].

Однако не все специалисты полностью разделяют изложенную позицию. Отмечается, что вопросы информационной безопасности при отправлении правосудия являются чувствительной и требующей особого внимания темой. Определение эффективных

---

[288] Информационные технологии в правосудии: состояние и перспективы. Россия и мир. Аналитический доклад // НИУ «ВШЭ». URL: http://црсп.рф/wp-content/uploads/2020/07/tezis-informacionnie-tehnologii-v-pravosudii.pdf (дата обращения: 12.05.2023).

[289] Там же.

методов и степени достаточности применяемых мер по защите данных невозможно без привлечения высококвалифицированных специалистов по информационной безопасности. Следует презюмировать небезопасность интернет-пространства для любых загружаемых и передаваемых цифровых данных. В случае необходимости выбора приоритет следует отдавать именно безопасности информации, а не удобству использования сервисов для пользователей[290]. Существуют опасения, что «для значительного числа IT-специалистов не составляет труда подменить вложения, направляемые по обычным незащищенным каналам связи. Подделать электронный документ и направить его в суд не представляет сложности»[291]. Не стоит исключать и другие последствия злонамеренного использования «слабых мест» цифровых технологий. Не всегда возможным является также сохранение баланса между высоким уровнем конфиденциальности и требованиями к открытости судебных заседаний.

Отдельные недобросовестные разработчики ПО не обеспечивают приемлемый уровень защиты персональных данных пользователей. Так, компания Zoom Video Communications, продукты которой относятся к числу наиболее используемых при проведении онлайн-заседаний в судах зарубежных стран, была замечена в передаче личных данных пользователей сторонним компаниям, включая социальные сети, без информирования об этом клиентов[292].

Прогрессивной, но достаточно спорной является тема использования искусственного интеллекта при отправлении правосудия. Часть авторов видит положительные стороны применения технологий машинного интеллекта в судебных процессах, утверждая, что их использование даст возможность снизить нагрузку на судей при выполнении рутинной работы. Другие эксперты отмечают такие

---

[290] Цифровизация правосудия: преимущества и риски // Адвокатская Газета. 2020. 29 июля. URL: https://www.advgazeta.ru/mneniya/tsifrovizatsiya-pravosudiya-preimushchestva-i-riski/ (дата обращения: 12.05.2023).

[291] Там же.

[292] Zoom sued for allegedly sharing users' personal data // CBS.NEWS. 2020. URL: https://www.cbsnews.com/news/ (дата обращения: 12.05.2023).

риски внедрения искусственного интеллекта, как технологические проблемы с обеспечивающими программами и системами, возможный взлом серверов и баз данных. Дискуссионным является также вопрос ответственности за действия искусственного интеллекта, в том числе при осуществлении правосудия.

X Всероссийский съезд судей сформулировал позицию по применению искусственного интеллекта в нашей стране следующим образом: «В настоящее время встает вопрос об использовании систем искусственного интеллекта, принимающего на себя обширную часть аналитической работы судьи. Съезд, не отрицая использования его отдельных элементов в судопроизводстве и дальнейшего развития в этой части процессуального законодательства, исходит из невозможности полной замены судьи искусственным интеллектом. Ряд оценочных категорий, таких как справедливость, соразмерность и др., не могут быть доверены компьютерному алгоритму»[293].

Представляется разумным определить границы применения технологий искусственного интеллекта в судебной деятельности. Вряд ли целесообразным является применение таких технологий в судопроизводстве по уголовным делам, поскольку судьи при вынесении приговора руководствуются не только законом, но и внутренним убеждением; уголовный закон содержит отдельные понятия, носящие оценочный характер и устанавливаемые судьей в каждом конкретном случае. К числу исключений для автоматизации судебного процесса предлагается также отнести отдельные категории дел, такие как семейные споры и дела о компенсации морального вреда, в которых важно участие реального судьи для «человеческой» оценки обстоятельств дела. В то же время с бесспорной категорией дел, рассматриваемых в порядке приказного и особого производства, с делами об административных правонарушениях на основании

[293] О развитии судебной системы Российской Федерации : Постановление X Всероссийского съезда судей от 01.12.2022 № 1 // СПС «КонсультантПлюс».

информации, полученной в автоматическом режиме, в обозримой перспективе смог бы справиться и искусственный интеллект[294].

Безусловно, непрекращающееся развитие современных технологий обуславливает дальнейший прогресс в сфере судопроизводства, и ярким примером здесь могут стать зарубежные страны. Так, в Китае уже действуют специальные суды, организованные с целью рассмотрения заседаний исключительно по видеосвязи; судебный аппарат в своей работе активно использует технологии блокчейн для верификации данных. Также в этой стране начинается внедрение искусственного интеллекта при отправлении правосудия, и, хотя полная замена судей программами случится еще не скоро, уже сейчас машинный разум помогает в рассмотрении дел, выполняя такие вспомогательные функции, как распознавание речи для составления протоколов и автоматическое уведомление суда о наличии схожих судебных дел[295]. Перспективным является китайский проект интернет-судов «Smart courts», предполагающий разработку программного продукта, в рамках которого дело рассматривается виртуальным судьей. Несмотря на то, что в интернет-судах используются технологии искусственного интеллекта, судьи следят за процессом и принимают наиболее важные решения. Количество рассмотренных интернет-судами дел уже измеряется сотнями тысяч[296].

Преимущества информатизации судов в целом очевидны. Использование современных технологий способно обеспечить ускорение судопроизводства, повышение его прозрачности и механизма «обратной связи» между властью и обществом, значительно повысить доступность судов, что особенно важно для лиц с ограниченными возможностями здоровья.

---

[294] *Анисимова А.С., Спиридонова М.П.* К вопросу о возможностях использования технологий искусственного интеллекта в правосудии // Юридический вестник ДГУ. 2021. Т. 39, № 3. С. 161–165.

[295] *Wang Z.* China's E-Justice Revolution // Judicature. 2021. № 1. P. 37-47.

[296] Аватар вместо мантии: какое будущее ждет судебную систему в эпоху инноваций // Рос. газ. 2020. URL: https://rg.ru/ (дата обращения: 12.05.2023).

Для успешного развития информатизации судебной деятельности необходимы согласованные действия государства и общества, затрагивающие решение целого ряда задач, лежащих в диапазоне от формальных и технических ограничений до трудностей, связанных с инертностью правового мышления и неприятием цифровизации в целом.

Представляется, что известные преимущества цифровизации судебной власти значительно превосходят возможные недостатки, а имеющиеся риски, при условии должной проработки нормативной базы и надлежащего контроля за обеспечением информационной безопасности, можно считать несущественными.

Библиографический список

1. Анисимова А.С., Спиридонова М.П. К вопросу о возможностях использования технологий искусственного интеллекта в правосудии // Юридический вестник ДГУ. – 2021. – Т. 39, № 3. – С. 161–165.

2. Информационные технологии в правосудии: состояние и перспективы. Россия и мир. Аналитический доклад [Электронный ресурс] // НИУ «ВШЭ». – URL: http://црсп.рф/wp-content/uploads/2020/07/tezis-informacionnie-tehnologii-v-pravosudii.pdf (дата обращения: 12.05.2023).

3. Wang Z. China's E-Justice Revolution // Judicature. – 2021. – № 1. – P. 37-47.

СОДЕРЖАНИЕ

Научное издание

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Сборник статей

Редактор: И. А. Бусоргина

Подписано в печать 26.09.2023. Формат 60x84 1/16
Усл. печ. л. 11,08. Уч. изд. л. 7,63.
Тираж 27 экз. Заказ № 1611.

Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, 4Б, каб. 021
Тел.: + 7 (3412) 916-364, E-mail: editorial@udsu.ru

Типография Издательского центра
«Удмуртский университет»
426034, Ижевск, ул. Университетская, 1, корп. 2.
Тел. 685-718