ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Ижевск
2025

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

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Сборник статей
Всероссийской научно-практической конференции
с международным участием

28 марта 2025 г.

Ижевск
2025

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

Рекомендовано к изданию редакционно-издательским советом УдГУ

Рецензенты: д-р юрид. наук, профессор, зав. каф. информ. права и цифровых технологий ФГАОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)» **А.В. Минбалеев**;
канд. юрид. наук, доцент, доцент каф. уголовного права и криминологии ФГБОУ ВО «Удмуртский государственный университет» **Г.А. Решетникова**.

Научные редакторы: *Г.Г. Камалова*, д-р юрид. наук, профессор, зав. каф. информационной безопасности в управлении ИПСУБ ФГБОУ ВО «Удмуртский государственный университет»;
В.Г. Ившин, канд. юрид. наук, доцент, профессор каф. уголовного права и криминологии, директор Института права, социального управления и безопасности ФГБОУ ВО «Удмуртский государственный университет».

О-136 Обеспечение информационной безопасности: вопросы теории и практики : сб. ст. Всерос. науч.-практ. конф. с междунар. участием / науч. ред.: Г.Г. Камалова, В.Г. Ившин. – Ижевск : Удмуртский университет, 2025. – 223 с.

ISBN 978-5-4312-1302-1
DOI:10.35634/978-5-4312-1302-1-2025-1-223

Сборник содержит статьи участников Всероссийской научно-практической конференции «Обеспечение информационной безопасности: вопросы теории и практики», проведенной Институтом права, социального управления и безопасности Удмуртского государственного Университета 28 марта 2025 года. В статьях рассматриваются актуальные вопросы теории и практики обеспечения информационной безопасности.

УДК 34:004.056(063)
ББК 67.401.114я431

ISBN 978-5-4312-1302-1
DOI:10.35634/978-5-4312-1302-1-2025-1-223

СОДЕРЖАНИЕ

Камалова Гульфия Гафиятовна,

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

ПЕРСПЕКТИВЫ РАЗВИТИЯ РЕГУЛИРОВАНИЯ СФЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ФОРМИРОВАНИЯ ЭКОНОМИКИ ДАННЫХ И ЦИФРОВОЙ ТРАНСФОРМАЦИИ ГОСУДАРСТВА

Одним из ключевых факторов развития современных общества и государства является революционная динамика цифровых технологий, что признается многими исследователями[1]. Это имеет как позитивные, обусловленные повышением уровня и качества жизни граждан и общества в целом в результате активизации применения информационно-коммуникационных технологий во всех областях деятельности, так и негативные аспекты. Последние выражены прежде всего в усилении проблем, связанных с обеспечением информационной безопасности личности, общества и государства. Это диктуется трендами развития цифровых технологий и общественных отношений в условиях дальнейшей эволюции информационного общества, цифровой трансформации и формирования многополярного мира. При этом проблемы обеспечения информационной безопасности весьма разнообразны и требуют глубокого исследования в отношении дальнейших перспектив в этой области. Указанное усугубляется фактически ведущейся

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

недружественными по отношению к России гибридной войной, важной составляющей которой является активное информационное и технологическое противостояние.

Указом президента РФ «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»[2] национальными целями развития России определены: формирование безопасной среды для жизни, технологическое лидерство, цифровая трансформация системы публичного управления, экономики и социальной сферы. При этом, полагаем, формирование безопасной среды для жизни граждан и общества предполагает достижение высокого уровня кибербезопасности во всех ее проявлениях, информационно-психологической личности и общества, а также технологического суверенитета России в отношении цифровых технологий[3].

В связи с этим Национальный проект «Экономика данных и цифровая трансформация государства»[4] в состав подлежащих реализации федеральных проектов включает разнообразные проекты, связанные с развитием информационно-коммуникационных технологий, в том числе инфраструктуры доступа к информации через информационно-телекоммуникационную сеть «Интернет» и социальных цифровых платформ, отечественных решений на основе технологии искусственного интеллекта, дальнейшей цифровизации государственного управления и подготовки кадров для цифровой трансформации. Особое место среди таких проектов занимает проект, направленный на дальнейшее развитие российской инфраструктуры кибербезопасности. В рамках этого проекта при повышении

---

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

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

[4] URL: https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva (дата обращения: 30.04.2025).

уровня кибербезопасности в России важное внимание планируется уделить проблемам противодействия преступлениям в информационном пространстве, совершаемым с использованием цифровых технологий, усилению механизмов снижения ущерба от таких правонарушений, а также достижению сетевого суверенитета и информационной безопасности при использовании информационно-коммуникационной сети «Интернет». Кроме того, необходимо выстроить эффективную систему противодействия угрозам безопасности обработки персональных данных.

В рамках реализации Программы «Информационное общество» также поставлены цели развития экономического потенциала России на основе использования новейших цифровых технологий, сохранения традиционных духовно-нравственных ценностей, а также защита личности, общества и государства от внутренних и внешних информационных угроз для обеспечения государственной защиты интересов российских граждан в информационной сфере[5].

Указанные векторы государственной политики в информационной сфере ставят перед научным правовым сообществом задачи осмысления происходящих социальных процессов и формирования теоретико-методологической основы процессов развития правового обеспечения информационной безопасности, соответствующих современным вызовам и угрозам, дальнейшего развития правового регулирования в этой сфере.

По оценкам экспертов в области информационной безопасности трендами в этой области в настоящее время являются:

– расширение системы ролей и компетенций специалистов информационной безопасности;

– переход от модели обеспечения безопасности функционирующей информационной инфраструктуры и цифровых сервисов

[5] Об утверждении государственной программы Российской Федерации "Информационное общество" : постановление Правительства РФ от 15.04.2014 № 313 (ред. от 25.12.2024) // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru, 24.04.2014.

к модели безопасности на всех этапах жизненного цикла продукта и сервиса, в том числе обеспечения безопасной разработки;

– перенос приоритета с защиты системы на защиту управленческих и бизнес-процессов;

– развитие киберразведки;

– активное внедрение технологий искусственного интеллекта, с одной стороны, как инструмента злоумышленников, а с другой – в систему обеспечении кибербезопасности;

– развитие киберполигонов и SOC-центров;

– влияние потенциала квантовых технологий;

– сохраняется недостаток кадров в области информационной безопасности;

– продолжается движение по достижению технологического суверенитета в отношении применяемых средств защиты информации;

– дальнейшее развитие идентификации и аутентификации, а также доверенных систем в цифровой среде;

– и другие[6].

Существенное значение в развитии системы информационной безопасности Российской Федерации имеет, безусловно, совершенствование законодательства и правовой доктрины. При этом повышение требований к процессам и состоянию защищенности информации в целях защиты прав и свобод и усиления национальной безопасности является важнейшим фактором значимых позитивных изменений для системы деятельности в области обеспечения информационной безопасности. В настоящее время основными трендами развития российского законодательства и права информационной безопасности являются усиление контроля, организационно-правовое обеспечение технологической независимости и созда-

[6] Тенденции в ИБ на 2025 год // Securitylab.ru by Positive Technologies. URL: https://www.securitylab.ru/blog/company/Rubikon/355166.php?ysclid=mal2t5z66m83313170 (дата обращения: 02.06.2025); Что ждёт сферу кибербезопасности в 2025 году: тренды, технологии и ключевые скиллы // Хабр. URL: https://habr.com/ru/companies/netologyru/articles/900718/ (дата обращения: 02.06.2025).

ние правовых условий развития сквозных цифровых технологий, включая технологию искусственного интеллекта, усиление защиты персональных данных граждан. Еще одним вектором развития углубления регуляторной политики обеспечения информационной безопасности является углубление технического регулирования этой области. Вместе с тем развитие правового обеспечения информационной безопасности и технического регулирования по-прежнему значительно отстает от динамики организационных и технических средств и мер защиты информации.

Следует отметить, что к настоящему времени информационное право и законодательство прошли немалый путь развития и уже сформированы нормативно-правовые основания обеспечения информационной безопасности России. Вместе с тем дальнейшая цифровая трансформация влечет активизацию гонки за динамично развивающимися технологиями и новыми механизмами защиты информационных прав и свобод граждан, информационных ресурсов и информационной инфраструктуры Российской Федерации. Происходящие изменения ведут к активному дальнейшему развитию системы информационного права в рамках публично-правовых отраслей права, включая формирование новых институтов права, совершенствование понятийного аппарата, системы принципов. Следует отметить, что динамика развития в области правовых средств информационной безопасности в настоящее время в большей мере связана с отдельными правовыми институтами: идентификации, информации ограниченного доступа, критической информационной инфраструктуры, противодействия компьютерным преступлениям и др.

Один из ключевых факторов в настоящее время – безопасность критической информационной инфраструктуры как совокупности защищаемых объектов критически важных для государства и общества. Для субъектов критической информационной инфраструктуры в 2025 году становятся обязательными требования по переходу на отечественное программное обеспечение и радиоэлектронную продукцию, что будет способствовать как усилению

состояния защищенности объектов критической информационной инфраструктуры, так и положительно повлияет на российский рынок средств защиты информации. Кроме того, наблюдается тенденция по усилению мониторинга и контроля в этой области, что позволит обеспечить гарантированность действий субъектов по повышению уровня защищенности объектов такой инфраструктуры и, соответственно, их устойчивости к кибератакам и иным неправомерным воздействиям.

Однако переход на отечественные решения для обеспечения безопасности объектов критической информационной инфраструктуры в настоящее время наталкивается на проблемы, связанные с тем, что пока не по всем направлениям защиты информации есть полноценные российские аналоги иностранных решений, не умаляя вместе с тем отечественные достижения. Это ставит задачи дальнейшего развития государственной политики в данной области в целях стимулирования рынка средств защиты информации России.

Значение, которое невозможно переоценить, продолжает иметь эффективная защита персональных данных. В отношении совершенствования системы правовой охраны персональных данных и правового обеспечения безопасности их обработки следует отметить нормы, направленные на выявление и противодействие киберинцидентам и конкретизацию требований к обработке биометрических данных, а также усиление юридической ответственности посредством введения уголовной ответственности ст. 272.1 УК РФ за незаконные использование, передачу (распространение, предоставление, доступ), сбор и (или) хранение персональных данных в форме компьютерной информации, полученных посредством неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путем. Кроме того, криминализировано «Создание и (или) обеспечение функционирования информационного ресурса (сайта в сети "Интернет" и (или) страницы сайта в сети "Интернет", информационной системы, программы для электронных вычислительных машин), заведомо предназначенного для незаконных хранения,

передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, полученной незаконным путем»[7]. Все указанные изменения российского законодательства о персональных данных непосредственно связаны с ростом проблем утечки из информационных систем персональных данных, которые еще более усугубились в последние три года. Интерес в части формирования и совершенствования понятийного аппарата информационного права, полагаем, представляет примечание к ст. 272.1 УК РФ, конкретизирующее понятие трансграничного перемещения носителей информации, содержащих компьютерную информацию.

Усиливается также административно-правовая ответственность в области защиты информации, включая персональные данные. Это требует со стороны операторов информационных систем и владельцев информационной инфраструктуры проведения аналитики существующих у них процессов для выявления потенциальных рисков нарушения законодательства, регулярных аудитов информационной безопасности и совершенствование организационных и технических мер защиты информации посредством контроля доступа и защиты цифровых данных. В связи с усложнением процессов защиты информации и требований в этой области многие организации сегодня переходят на модель «информационная безопасность как сервис», в том числе в области защиты персональных данных[8].

---

[7] О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 30.11.2024 № 421 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru, 30.11.2024.

[8] Безопасность в облаке: как защищать данные и соответствовать законодательству // Ведомости. Технологии. URL: https://www.vedomosti.ru/technologies/special/2025/06/02/bezopasnost-v-oblake-kak-zaschischat-dannie-i-sootvetstvovat-zakonodatelstvu (дата обращения: 20.05.2025); Камалова Г.Г. Некоторые проблемы правового обеспечения конфиденциальности информации в условиях цифровизации и геополитических рисков // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции : в 6 т. Казань, 2023. С. 178-185.

В рамках противодействия распространению информации, которая имеет деструктивный характер, в конце 2024 года внесены изменения в Федеральный закон «Об информации информационных технологиях и о защите информации»[9], которые предусматривают соблюдение требований пользователем социальной сети и при определенных условиях ограничение доступа к его персональной странице. Вместе с тем решение задачи противодействия распространению противоправной информации, в том числе в социальных сетях, полагаем, необходимо строить комплексно и важную роль в этом, наряду с ограничительными мерами, играет повышение культуры информационной безопасности граждан[10].

Развитие отечественных решений на базе технологии искусственного интеллекта в настоящее время имеет приоритетное значение среди новейших цифровых технологий ввиду его интеграционного потенциала. Правовое регулирование отношений в связи с искусственным интеллектом представляется сегодня одним из вызовов праву, которое должно учитывать, с одной стороны, возможности этих технологий и потребности развития рынка, а с другой – существующие и формирующиеся риски. Учитывая международный и зарубежный опыт, сегодня следует в поле российского права встраивать регуляторные механизмы, обеспечивающие условия развития цифровых продуктов на базе технологий искусственного интеллекта при одновременном обеспечении гарантий соблюдения прав, свобод и законных интересов граждан. При этом следует учитывать, что технологии искусственного интеллекта используются

[9] Федеральный закон от 23.11.2024 № 411.

[10] Полякова Т.А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы / Т.А. Полякова, А.В. Минбалеев, Н.А. Троян // Государство и право. 2023. № 5. С. 131-144; Полякова Т.А. Формирование культуры информационной безопасности: правовые векторы // Обеспечение информационной безопасности: вопросы теории и практики : сборник статей Всероссийской научно-практической конференции / науч. редакторы: Г.Г. Камалова, В.Г. Ившин, Г.А. Решетникова. Ижевск, 2023. С. 3-10.

и в различных программных и программно-аппаратных решениях в области защиты информации. Однако эти технологии активно осваиваются и применяются и в противоправных целях.

В настоящее время для России остро стоит вопрос обеспечения безопасности в финансово-кредитной сфере, что особенно ощутимо в части кибератак на информационные ресурсы и расширения мошенничеств с применением информационно-коммуникационных технологий. В связи с этим в отношении возможностей и рисков для российского финансового рынка значимо не только усиление кибербезопасности финансово-кредитных институтов, но и защита прав потребителей финансовых услуг, а также повышение уровня доверия граждан к цифровым технологиям, применяемым в этой сфере. Для современности важно создание условий для безопасного внедрения цифровых платежных технологий, контроля рисков информационной безопасности и операционной надежности для непрерывного оказания банковских и финансовых услуг. Внедрение цифрового рубля формирует новые возможности для финансово-кредитной системы, однако это предполагает конкретизацию условий использования платформы цифрового рубля и усиление мер информационной безопасности в банковской сфере.

Следует отметить, что в рамках статьи сложно охватить все тренды развития правового обеспечения информационной безопасности. Вместе с тем необходимо отметить, что в настоящее время активно ведутся работы по разработке Цифрового кодекса РФ, который позволит системно регулировать сферу применения информационно-коммуникационных технологий. В этой связи важным представляется совершенствование понятийного аппарата информационного права и его системы. Безусловно, новые цифровые технологии обостряют и существовавшие проблемы баланса публичного и частного права. В этих условиях в аспекте иерархии правовых актов информационного законодательства, несомненно, важна кодификация, учитывающая динамику цифровых изменений в отраслях права и риски, возникающие в отношении основных прав и свобод граждан. Достойное место в будущем цифровом кодексе следует

отвести правовым нормам, регулирующим вопросы обеспечения информационной безопасности. При этом в центре происходящих процессов должны оставаться ценностные аспекты права[11].

Библиографический список

1. Механизмы и модели регулирования цифровых технологий / А.В. Минбалеев, А.В. Мартынов, Г.Г. Камалова, С.Г. Чубукова, О.В. Сушкова, М.В. Бундин, В.М. Жернова, И.С. Бойченко, К.Ю. Никольская. – Москва, 2023.

2. Камалова Г.Г. Некоторые проблемы правового обеспечения конфиденциальности информации в условиях цифровизации и геополитических рисков // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции : в 6 т. – Казань, 2023. – С. 178–185.

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

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

5. Полякова Т.А. Формирование культуры информационной безопасности: правовые векторы // Обеспечение информационной безопасности: вопросы теории и практики : сборник статей Всероссийской научно-практической конференции / науч. редакторы: Г.Г. Камалова, В.Г. Ившин, Г.А. Решетникова. – Ижевск, 2023. – С. 3–10.

6. Ценность права в условиях цифровой реальности : монография / О.Ю. Рыбаков, М.А. Беляев, Ю.Ю. Ветютнев [и др.]. – Москва, 2024.

[11] Ценность права в условиях цифровой реальности : монография / О.Ю. Рыбаков, М.А. Беляев, Ю.Ю. Ветютнев [и др.]. М., 2024.

Татьянина Лариса Геннадьевна,

д-р юрид. наук, профессор, зав. кафедрой уголовного процесса и криминалистики ИПСУБ ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДВАРИТЕЛЬНОМ СЛУШАНИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Развитие технологий порождает проблемы безопасности, оно привело к возможности их использования сторонами в уголовном судопроизводстве, что поставило под угрозу обеспечение сохранности информации, полученной как в досудебном, так и судебном производстве. Обеспечение информационной безопасности в уголовном судопроизводстве связано непосредственно с обеспечением безопасности личности, вовлеченной в уголовное судопроизводство, независимо от ее процессуального статуса, а также обеспечением сохранения доказательств в целях воспрепятствования оказанию противодействия процессу производства предварительного расследования и судебного разбирательства.

«Информационная безопасность – состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам)»[12]. Следовательно, информационная безопасность представляет собой комплекс мер, направленных на защиту от утечки или взлома программ, компьютерных систем и данных. Учитывая, что в настоящее время огромный массив информации по уголовным делам хранится и проходит через различные информационные системы, то ее безопасность находится под постоянной угрозой.

[12] См.: Вострецова Е.В. Основы информационной безопасности : учебное пособие // Екатеринбург : Изд-во Урал. ун-та, 2019. С. 15.

Информационная безопасность направлена на обеспечение безопасности информации, которая представляет собой « …защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования»[13].

Авторами выделяются по различным критериям и основаниям различные категории угроз информационной безопасности[14]. Применительно к уголовному судопроизводству представляется обоснованным выделение двух категорий угроз информационной безопасности: внутренние и внешние.

К числу внутренних угроз относятся те, которые идут изнутри системы. Данные угрозы связаны с утечкой данных или их повреждением. Указанные ситуации возникают в случае, когда сотрудник, имеющий доступ к информации, передает ее другому лицу за определенную плату или по иным причинам, либо когда злоумышленником является авторизованный пользователь. Наиболее распространенной является ошибка, в результате которой конфиденциальные сведения оказываются в открытом доступе или повреждаются, что связано с некачественной подготовкой следователей, дознавателей, прокуроров и судей к работе с компьютерами, в кото-

---

[13] См.: Вострецова Е.В. Указ. соч. С. 15.

[14] См.: Киргизова Е.В., Рубцов А.В., Ахтамова С.С. Информационная безопасность : учеб. пособие. Красноярск : Сибирский федеральный университет, 2018. С. 30-66; Вострецова Е.В. Основы информационной безопасности : учебное пособие. Екатеринбург : Изд-во Урал. ун-та, 2019. С. 68-90; Фалеев М.И., Черных Г.С. Угрозы национальной безопасности государства в информационной сфере. 2024. Т. 4., № 1 (6). С. 24; Гафнер В.В. Информационная безопасность : учебное пособие : в 2 ч. / ГОУ ВПО «Урал. гос. пед. ун-т». Екатеринбург, 2009. Ч. 1. С. 107-118; Хорев А.А. Техническая защита информации : учеб. пособие для студентов вузов : в 3 т. Т. 1. Технические каналы утечки информации. М. : НПЦ «Аналитика», 2008. 436 с.; Хорев А.А. Угрозы национальной безопасности // Журнал «Специальная Техника». 2010. № 1; и др.

рой они чаще всего являются банальными пользователями. Необходимо, чтобы лицо, допущенное к ознакомлению с информацией, не могло бы нарушить работу системы даже случайно, а информация оставалась защищена.

К внешним относятся угрозы, которые приходят извне, что порождает их разнообразие. Сюда следует отнести попытку взлома системы через найденную уязвимость, когда злоумышленник проникает в сеть, чтобы украсть или повредить информацию; DDoS-атаку, в результате которой сервер не выдерживает, что приводит к прекращению работы сайта; деятельность компьютерных вирусов, действия которых очень разнообразны: от рассылки спама от имени взломанного адреса до полной блокировки системы и повреждения файлов; форс-мажоры и несчастные случаи, в результате которых хранилище данных оказывается поврежденным (например: пожар, авария и т.п.).

Бесспорно, что в уголовном судопроизводстве существует возможность возникновения основных угроз безопасности, в качестве которых выступают: « …раскрытие конфиденциальной информации; компрометация информации; несанкционированное использование информационных ресурсов; ошибочное использование ресурсов; несанкционированный обмен информацией; отказ от информации; отказ от обслуживания»[15].

Производство предварительного слушания в суде первой инстанции, в соответствии с ч. 1 ст. 234 УПК РФ, проводится в закрытом судебном заседании, учитывая, что на порядок его проведения распространяются положения гл. 35 УПК РФ, то в соответствии с положениями ст. 241.1 УПК РФ допустимо использование видеоконференц-связи, в связи с чем возникают вопросы по обеспечению недопустимости распространения информации, полученной в процессе проведения предварительного слушания.

[15] См.: Фалеев М.И., Черных Г.С. Угрозы национальной безопасности государства в информационной сфере. 2014. Т. 4, № 1 (6). С. 24.

Угроза распространения информации существует в течение всего досудебного и судебного процесса, поскольку противодействие процессу расследования и судебного разбирательства имеет место практически по всем уголовным делам, но от их особенностей зависит уровень противодействия. Право участников процесса копировать информацию, с учетом развития технологий, привело к использованию различных технических средств для получения информации, в частности копируются на телефоны протоколы следственных и процессуальных действий, заключения экспертов и т.д., следователи передают копии звуко-видео-записи следственных действий в целях экономии времени. При ознакомлении с материалами уголовного дела представители конфликтующих сторон получают практически всю информацию, имеющуюся в материалах уголовного дела, вопрос о возможности ее использования для оказания противодействия процессу производства по уголовному делу остается открытым.

На предварительном слушании суд должен решить только те вопросы, которые указаны в ст. 229 УПК РФ, соответственно, информация, которая может быть исследована, ограничивается вопросами, входящими в предмет судебного рассмотрения предварительного слушания. Суд вправе исследовать те доказательства, на основании которых он будет принимать решение, распространение информации, их составляющей является недопустимым в целях исключения возможности оказания воздействия на участников процесса в целях изменения информации.

Закрытость судебного заседания на предварительном слушании исключает возможность разглашения информации. В связи с чем возникает вопрос о возможности использования видео-конференц-связи при его проведении. Учитывая вопросы, подлежащие рассмотрению, заинтересованность конкретной стороны-заявителя в их разрешении, представляется нецелесообразным использование указанной процедуры на предварительном слушании. Проведение судебного заседания предварительного слушания предполагает четкое исследование конкретного вопроса, занимает непродолжительное

время и исключает в связи с закрытостью процедуры распространение информации. Использование видео-конференц-связи предполагает дополнительную подготовку к его проведению, вовлечение представителей другого суда, технических работников, производство записи заседания, что не обеспечивает эффективность деятельности суда и обеспечение сохранения информации. В связи с чем полагаю, что при проведении предварительного слушания необходимо отказаться от использования видео-конференц-связи, а также осуществлять его только в закрытом судебном заседании, что обеспечит недопустимость разглашения информации, исследуемой и полученной при его проведении.

Решетнева Татьяна Васильевна,

канд. юрид. наук, доцент, зав. кафедрой теории и истории государства и права ИПСУБ ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

ПОНЯТИЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДОКУМЕНТАХ СТРАТЕГИЧЕСКОГО ПЛАНИРОВАНИЯ И МЕЖДУНАРОДНЫХ ДОГОВОРАХ РОССИЙСКОЙ ФЕДЕРАЦИИ

Современное состояние общественной жизни сложно представить без информационно-коммуникационных технологий (далее – ИКТ), расширяющегося информационного пространства, оказывающих значительное влияние на прогрессивное развитие всего человечества. В силу того, что в «информационной сфере практически отсутствуют географические и геополитические границы, временные

рамки и часовые пояса»[16], возрастают риски и угрозы, связанные с возможным использованием информационно-коммуникационных технологий в целях, которые не совместимы с обеспечением международного мира, правами человека и их защитой, с суверенными правами и интересами государств, и, как следствие, актуализируется вопрос, связанный с созданием эффективных правовых, организационных, институциональных механизмов, позволяющих обеспечить информационную безопасность, в том числе международную, что побуждает государства на национальном и международном уровнях предпринимать соответствующие усилия.

Ключевым вопросом при правовой регламентации отношений в сфере обеспечения международной информационной безопасности (далее – МИБ) является выработка унифицированного понятийного аппарата. В настоящее время в юридической литературе ведутся активные дискуссии относительно выработки дефиниции «международная информационная безопасность».

Сложность в выработке на международном уровне универсальной дефиниции обусловлена разным подходом государств к проблеме информационной безопасности, различиями в используемой терминологии (наряду с термином «информационная безопасность» как эквивалент используется термин «кибербезопасность»). По мнению А. Бедрицкого, сформировались 2 основных подхода: «1) США и Европа сосредоточили свое внимание на отдельных проблемах международной информационной безопасности, выбрав в качестве приоритетного направления противодействие угрозам террористического и криминального характера, что привело к созданию на европейском уровне конвенции о борьбе с преступлениями в киберпространстве. Вопрос разоружения серьезно не рассматривался ввиду скептического отношения к идее «информационного оружия» и «информационной войны» в целом.

[16] Дубень А.К. Опыт международного сотрудничества в сфере информационной безопасности: проблемы и перспективы // Международное право и международные организации. 2023. № 3. Режим доступа: СПС «Консультант Плюс».

2) Иной путь выбрали для себя Россия, ее партнеры по ШОС и представители развивающихся стран, настаивающие на комплексном анализе проблемы международной информационной безопасности, определяя в качестве основной цели предотвращение опасности развязывания информационной войны. Они также настаивали на назревшей необходимости разработки международно-правовой основы универсального режима МИБ»[17]. Широкое понимание МИБ предложено Е.В. Калининой: международная информационная безопасность – это одновременно «1) и состояние защищенности субъектов международного права (МП) от информации, носящей вредный или противоправный характер, а также оказывающей негативное воздействие на сознание населения; 2) и состояние защищенности информационной инфраструктуры субъектов МП; 3) и система организационно-правовых средств, обеспечивающая защиту сетей, компьютеров, программ, устройств от атак, повреждения или несанкционированного доступа, призванная обеспечить эффективное сотрудничество акторов в международном информационном пространстве»[18].

В документах стратегического планирования Российской Федерации содержатся легальные дефиниции информационной безопасности и международной информационной безопасности. Согласно подп. «в» п. 2 Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ № 646 от 5 декабря 2016 г., под информационной безопасностью РФ понимают «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором

[17] Бедрицкий А. Международные договоренности по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. – ПЕРСПЕКТИВЫ: Фонд исторической перспективы : [Электронный ресурс]. URL: http://www.perspektivy.info/print.php?ID=232592 (дата обращения: 10.04.2019). Цит. по: Калинина Е.В. Становление идеи международной информационной безопасности. Прогнозы на ближайшее будущее. С. 10. URL: http://www.zakipp.unn.ru/wp-content/uploads/sites/16/2020/02/2. - Kalinina.pdf?ysclid=mbncd0yah7347417951 (дата обращения: 30.04.2025).

[18] Калинина Е.В. Указ. соч. С. 9.

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 безопасность государства», а в п. 6 «Основ государственной политики Российской Федерации в области международной информационной безопасности», утвержденных Указом Президента РФ от 12.04.2021 № 213 (далее – Основы), под международной информационной безопасностью понимается «такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности». В Основах, как документе стратегического планирования Российской Федерации, отражены официальные взгляды на сущность международной информационной безопасности, определены основные угрозы международной информационной безопасности, цель, задачи, направления государственной политики Российской Федерации в области международной информационной безопасности[19]. Согласно положениям Основ, государственная политика России в области международной информационной безопасности представляет собой «совокупность скоординированных мер, направленных на формирование с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности»[20], представленной международными и национальными институтами, регулирующими деятельность в глобальном информационном пространстве в целях предотвращения (минимизации) угроз международной

[19] Пункт 1 «Основ государственной политики Российской Федерации в области международной информационной безопасности», утв. Указом Президента Российской Федерации от 12.04.2021 № 213 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

[20] Пункт 2 «Основ государственной политики Российской Федерации в области международной информационной безопасности», утв. Указом Президента Российской Федерации от 12.04.2021 № 213 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

информационной безопасности[21], «содействия установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности»[22]. Исходя из указанных выше документов, подход России к международной информационной безопасности видится в обеспечении при помощи национальных и международных инструментов состояния защищенности личности, общества, государства в глобальном информационном пространстве, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности, создаются условия для предотвращения (урегулирования) межгосударственных конфликтов. Российский подход к вопросу о международной информационной безопасности находит свое отражение в инициативах Российской Федерации относительно содержания международных документов, посвященных вопросам международной информационной безопасности.

Россия совместно с дружественными ей государствами выступила инициатором разработки и принятия целого ряда международных документов. Так, на площадках Организации Объединенных Наций «Российская Федерация последовательно выступает за формирование системы международной информационной безопасности на прочной правовой основе, с опорой на принципы суверенного равенства государств и невмешательства в их внутренние

[21] Пункт 7 «Основ государственной политики Российской Федерации в области международной информационной безопасности», утв. Указом Президента Российской Федерации от 12.04.2021 № 213 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

[22] Пункт 9 «Основ государственной политики Российской Федерации в области международной информационной безопасности», утв. Указом Президента Российской Федерации от 12.04.2021 № 213 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

дела»[23] и исходит из того, «что только коллективными усилиями всего мирового сообщества можно обеспечить мир и стабильность в глобальном информационном пространстве и эффективно противодействовать всему комплексу существующих и потенциальных угроз в данной сфере. В этих целях ежегодно – на протяжении 25 лет Россия – вносит проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»»[24]. В ходе 70-й сессии Генассамблеи ООН Первым комитетом принята российская резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Как отмечено выше, этот документ принимается консенсусом на протяжении целого ряда лет и с каждым годом привлекает все больше активных сторонников»[25]. Согласно положениям преамбулы данной резолюции было констатировано, что «ИКТ являются технологиями двойного назначения, которые могут использоваться как в законных, так и в злонамеренных целях», и их использование «в будущих конфликтах становится все более вероятным», при этом было определено, что «все государства заинтересованы в поощрении использования ИКТ в мирных целях с целью создания для человечества сообщества общего будущего в киберпространстве и <…> заинтересованы в предотвращении конфликтов, возникающих в результате использования ИКТ». Именно Организации Объединенных Наций отводится ведущая роль «в поощрении диалога между государствами-членами для выработки общего понимания в отношении

[23] Выступление заместителя руководителя российской делегации А.И. Белоусова по российскому проекту резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» в ходе голосования по разделу «Другие меры разоружения и международная безопасность» в Первом комитете 78-й сессии ГА ООН. Постоянное представительство Российской Федерации при ООН. URL: https://russiaun.ru/ru/news/611123 (дата обращения: 20.04.2025).

[24] Там же.

[25] О принятии Первым комитетом Генассамблеи ООН резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://www.mid.ru/ru/foreign_policy/news/1518395/ (дата обращения: 20.04.2025).

обеспечения безопасности при использовании ИКТ и самих ИКТ, а также в выработке единого понимания в вопросах применимости международного права и норм, правил и принципов ответственного поведения государств в этой сфере, поощрять региональные усилия, меры по укреплению доверия и повышению транспарентности, а также способствовать наращиванию потенциала и распространению передового опыта». При этом в документе подчеркивается, что главную ответственность за поддержание безопасной и мирной ИКТ-среды несут прежде всего государства.

15 мая 2023 г. «Россия в соавторстве с Белоруссией, КНДР, Никарагуа и Сирией внесла концепцию конвенции ООН об обеспечении международной информационной безопасности (МИБ) в качестве официального документа 77-й сессии Генеральной Ассамблеи ООН»[26]. В рамках обновленной концепции конвенции ООН обозначено, что «растет необходимость заключения государствами в рамках ООН юридически обязательного многостороннего международного договора… Конвенции ООН об обеспечении международной информационной безопасности (далее – Конвенция), регулирующей отношения государств по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий»[27]. Необходимо подчеркнуть, что в обновленной концепции Конвенции ООН об обеспечении международной информационной безопасности отражен широкий подход к сущности международной информационной безопасности, что проявляется в закреплении перечня основных угроз обеспечения МИБ[28].

---

[26] О концепции конвенции ООН по международной информационной безопасности (сайт МИД РФ). URL: https://www.mid.ru/ru/foreign_policy/news/1870609/ (дата обращения: 11.05.2025).

[27] Обновленная концепция конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности (сайт Совета Безопасности РФ). URL: www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf

[28] См. Раздел II Обновленной концепции конвенции Организации Объединенных Наций об обеспечении международной информационной

Россия принимает активное участие в региональных, субрегиональных международных объединениях и организациях. Министрами иностранных дел – членов ОДКБ (Организации Договора о коллективной безопасности) было принято совместное заявление[29], в котором стороны подтвердили необходимость принятия скоординированных мер по обеспечению МИБ на всех международных площадках (ООН, МСЭ, ОДКБ и др.) и выразили намерение об активизации политического взаимодействия в рамках вступившего в силу Соглашения о сотрудничестве в области обеспечения информационной безопасности 2017 года и повышения координации продвижения согласованных подходов к вопросам информационной безопасности на международной арене. На площадке СНГ было принято Решение Совета глав государств СНГ «О Совместном заявлении глав государств – участников Содружества Независимых Государств о сотрудничестве в области обеспечения международной информационной безопасности», вступившее в силу 18.12.2020, в котором главы государств акцентировали внимание на повышение «уровня межгосударственного сотрудничества, направленного на предотвращение и мирное урегулирование конфликтов, которые могут возникнуть в результате неправомерного и деструктивного использования информационно-коммуникационных технологий» в целях обеспечения национальных и международных интересов в условиях глобальных кризисных ситуаций, а также на усиление обмена положительным опытом и практиками противодействия угрозам международной информационной безопасности[30]. О необходимости «формирования общего будущего в информационном

безопасности (сайт Совета Безопасности РФ). URL: www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf

[29] Совместное заявление министров иностранных дел государств – членов Организации Договора о коллективной безопасности об активизации сотрудничества в области обеспечения международной информационной безопасности (г. Ереван, 23.11.2022; договаривающиеся стороны: Армения, Беларусь, Казахстан, Киргизия, Россия, Таджикистан) // Сайт Организации Договора о коллективной безопасности. URL: https://odkb-csto.org/

[30] См. Единый реестр правовых актов и других документов СНГ. URL: http://cis.minsk.by/

пространстве», основанном на предотвращении конфликтов, возникающих в результате использования ИКТ, об обеспечении использования ИКТ в интересах социального и экономического развития и повышения благосостояния народов говорится в Заявлении Совета глав государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 10.11.2020[31]. В этом же документе подчеркнуто, что разработка и использование ИКТ, международное сотрудничество в данной сфере должны основываться на общепризнанных принципах международного права, «включая Устав ООН, в частности, государственного суверенитета, политической независимости, территориальной целостности, суверенного равенства государств, урегулирования споров мирными способами, невмешательства во внутренние дела других государств, а также уважения основных свобод и прав человека, в том числе неприкосновенность частной жизни, которые имеют первостепенное значение для формирования мирного, безопасного, открытого и стабильного глобального информационного пространства»[32]. В рамках ШОС правительствами государств-членов организации (Казахстан, Киргизия, Китай, Россия, Таджикистан, Узбекистан) был заключен международный договор о сотрудничестве в области обеспечения международной информационной безопасности[33].

Российская Федерация активно сотрудничает с государствами в направлении заключения двусторонних международных договоров по вопросам обеспечения МИБ. В частности, Россия заключила

[31] Источник публикации: сайт Шанхайской организации сотрудничества. URL: http://rus.sectsco.org/

[32] Источник публикации: сайт Шанхайской организации сотрудничества. URL: http://rus.sectsco.org/

[33] Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (г. Екатеринбург, 16.06.2009, вступило в силу 02.11.2011) // Бюллетень международных договоров. 2012. № 1. С. 13–21 ; официальный сайт МИД России. URL: http://www.mid.ru

двусторонние договоры о сотрудничестве в области обеспечения международной информационной безопасности с Республикой Мьянма (Бирма)[34], Эфиопией[35], Зимбабве[36], Таджикистаном[37], Азербайджанской Республикой[38], Индонезией[39], Республикой Узбекистан[40], Республикой Никарагуа[41], Киргизской Республикой[42], Турк-

[34] Соглашение между Правительством Российской Федерации и о сотрудничестве в области обеспечения международной информационной безопасности (г. Нейпьидо, 05.12.2023) (Вместе с «Перечнем основных понятий... »), вступило в силу 17.05.2024. Опубликовано: официальный сайт МИД РФ. URL: http://www.mid.ru

[35] Соглашение между Правительством Российской Федерации и Правительством Федеративной Демократической Республики Эфиопии о сотрудничестве в области обеспечения международной информационной безопасности (г. Санкт-Петербург, 28.07.2023). Опубликовано: официальный сайт МИД РФ. URL: http://www.mid.ru

[36] Соглашение между Правительством Российской Федерации и Правительством Республики Зимбабве о сотрудничестве в области обеспечения международной информационной безопасности (г. Санкт-Петербург, 27.07.2023), вступило в силу 20.12.2023. Опубликовано: официальный сайт МИД РФ. URL: http://www.mid.ru

[37] Соглашение между Правительством Российской Федерации и Правительством Республики Таджикистан о сотрудничестве в области обеспечения международной информационной безопасности (г. Москва, 19.06.2023), вступило в силу 16.02.2024. Опубликовано: официальный сайт МИД РФ. URL: http://www.mid.ru

[38] Соглашение между Правительством Российской Федерации и Правительством Азербайджанской Республики о сотрудничестве в области обеспечения международной информационной безопасности (г. Баку, 24.06.2022), вступило в силу 19.10.2022 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

[39] Соглашение между Правительством Российской Федерации и Правительством Республики Индонезии о сотрудничестве в области обеспечения международной информационной безопасности (г. Джакарта, 14.12.2021, вступило в силу 28.05.2022) // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

[40] Соглашение между Правительством Российской Федерации и Правительством Республики Узбекистан о сотрудничестве в области обеспечения международной информационной безопасности (г. Москва, 18.11.2021) // Официальный сайт МИД РФ. URL: http://www.mid.ru

менистаном[43], Вьетнамом[44], ЮАР[45], Китайской Народной Республикой[46], Кубой[47], Республикой Беларусь[48], Бразилией[49]. Все двусто-

---

[41] Соглашение между Правительством Российской Федерации и Правительством Республики Никарагуа о сотрудничестве в области обеспечения международной информационной безопасности (г. Москва, 19.07.2021, вступило в силу 08.10.2021) // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

[42] Соглашение между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудничестве в области обеспечения международной информационной безопасности (г. Москва, 25.02.2021, вступило в силу 12.02.2022) // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

[43] Соглашение между Правительством Российской Федерации и Правительством Туркменистана о сотрудничестве в области обеспечения международной информационной безопасности (г. Москва, 05.04.2019, вступило в силу 12.06.2019) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

[44] Соглашение между Правительством Российской Федерации и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности (г. Сочи, 06.09.2018, вступило в силу 29.04.2019) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

[45] Соглашение между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности (г. Сямэне, 04.09.2017) // Официальный сайт МИД РФ. URL: http://www.mid.ru/

[46] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности (г. Москва, 08.05.2015, вступило в силу 10.08.2016) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

[47] Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности (г. Гавана, 11.07.2014, вступило в силу 02.01.2015) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

[48] Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности (г. Москва, 25.12.2013, вступило в силу 27.02.2015) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

[49] Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в обла-

ронние договоры о сотрудничестве в области обеспечения МИБ отражают единый подход к обозначению угроз, связанных с использованием ИКТ, а также направлений и форм международного сотрудничества. Однако только некоторые из них в качестве неотъемлемой части договора содержат «Перечень основных понятий в области обеспечения международной информационной безопасности» (далее – Перечень), где закреплена современная терминология в рассматриваемой сфере. В договорах РФ с Кубой, Республикой Беларусь, ЮАР, КНР, а также в Перечне договора ШОС в области обеспечения МИБ содержится единая дефиниция информационной безопасности, под которой понимают «состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве». В договоре же с Бразилией дается расширенная дефиниция информационной безопасности, включающая в себя также и коммуникационную безопасность. В частности, в п. 1 Перечня закреплено, что «информационная и коммуникационная безопасность – состояние защищенности личности, общества, государства и их интересов от существующих и потенциальных угроз в сфере информационных и коммуникационных средств и технологий, включая меры, направленные на обеспечение доступности, целостности, конфиденциальности и подлинности информации». При этом только в договоре России с Республикой Беларусь, в договоре ШОС раскрывается понятие международной информационной безопасности, под которой понимают «состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве», а в договоре России с Бразилией установлено, что «международная информационная и коммуникационная безопасность – состояние международных отношений, исключающее

сти обеспечения международной информационной и коммуникационной безопасности (г. Москва, 14.05.2010) // СПС Консультант Плюс (дата обращения: 21.04.2025).

нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в сфере информационных и коммуникационных средств и технологий». Можно констатировать, что существующая международно-правовая регламентация отношений в сфере МИБ характеризуется фрагментацией, в международных договорах и официальных международных документах не всегда присутствуют дефиниции понятий «информационная безопасность», «международная информационная безопасность», имеются расхождения в части использования терминологии, что демонстрирует договор России с Бразилией. Хотя, исследуя содержание договоров в сфере МИБ, можно прийти к выводу, что международная информационная безопасность, является частью информационной безопасности, а в глобальном аспекте – частью международной безопасности, имеющей своей основной целью обеспечение международного мира, суверенитета и безопасности государств, недопущение дестабилизации внутриполитической и социально-экономической обстановки, пресечение разжигания межнациональной и межконфессиональной вражды, защиту прав человека и недопущение нарушения неприкосновенности частной жизни индивида.

Эффективное правовое регулирование международной информационной безопасности невозможно достичь без согласованной позиции государств относительно содержания понятия «международная информационная безопасность», единства в понимании угроз, как потенциальных, так и реальных, международных и внутригосударственных инструментов и механизмов, позволяющих обеспечить международную информационную безопасность. В связи с чем возрастает роль и значение норм международного права в регулировании отношений, складывающихся в трансграничном информационном пространстве. При этом реализация норм международного права невозможна без создания эффективных внутригосударственных механизмов и принципиальной согласованности международного и внутригосударственного права относительно понимания международной информационной безопасности.

Гафурова Эльмира Равилевна,

канд. юрид. наук, доцент, доцент кафедры теории и истории государства и права ИПСУБ ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

ЮРИДИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В условиях стремительного развития цифровых технологий и возрастающей роли информационных ресурсов, обеспечение информационной безопасности Российской Федерации приобретает первостепенное значение. Это подтверждается как Указом Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[50], подчеркивающим необходимость защиты национальных интересов в информационной сфере, так и Указом Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»[51], где информационная безопасность признана одним из ключевых факторов национальной безопасности. Обеспечение этой безопасности требует не только совершенствования технических средств защиты, но и адекватного правового регулирования, особенно в контексте бурного внедрения искусственного интеллекта (далее – ИИ).

[50] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 12.12.2016. № 50, ст. 7074.

[51] О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 02.07.2021 № 400 // Собрание законодательства РФ 05.07.2021. № 27 (часть II), ст. 5351.

Использование ИИ в обеспечении информационной безопасности открывает новые возможности: от автоматизированного выявления угроз и предотвращения кибератак до повышения эффективности мониторинга и анализа больших данных. Однако внедрение ИИ в сферу информационной безопасности порождает ряд сложных юридических вопросов, требующих внимательного анализа и решения.

Так, Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[52] определяет цели, задачи и меры по реализации внутренней и внешней политики страны в сфере применения информационных и коммуникационных технологий, указывая в качестве приоритетного направления – ИИ.

Рассматривая ИИ как возможность обеспечения информационной безопасности, отметим, что в Указе Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» закреплено: «ИИ – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их». Сам комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений[53].

---

[52] О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы : Указ Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. 15.05.2017. № 20, ст. 2901.

[53] О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») : Указ Президента РФ от 10.10.2019 № 490 // Собрание законодательства РФ. 14.10.2019. № 41, ст. 5700.

В случае использования такого комплекса технологических решений в целях обеспечения информационной безопасности возникает вопрос об определении ответственности за действия и решения, принимаемые им. В случае причинения ущерба в результате сбоя или ошибочного действия ИИ, кто несет ответственность: разработчик, владелец системы, пользователь или сам ИИ?

Существующее законодательство, ориентированное на действия физического лица, часто оказывается недействительным для подобных ситуаций. Например, если автономная система кибербезопасности ошибочно блокирует доступ к критическим ресурсам, кто компенсирует потери? Владением является прежде всего фактическое обладание вещью, в то время как использование подразумевает под собой извлечение полезных свойств. В частности, не каждый владелец ИИ является его пользователем, тем самым не является возможным осуществление контроля за действиями, выполняемыми ИИ. Соответственно, нести юридическую ответственность в рассматриваемой ситуации должен пользователь. Вопрос привлечения к юридической ответственности разработчика ИИ является также неоднозначным. С одной стороны, разработчик конструирует основные алгоритмы программы. С другой стороны, данные технологии являются совокупностью процессов, которые контролировать крайне сложно. Разработчик зачастую не способен предвидеть негативные последствия применения программного продукта.

Для урегулирования данного вопроса необходимо разработать новые правовые механизмы, четко распределяющие ответственность в зависимости от уровня автономности ИИ и характера причиненного вреда, круга лиц (разработчик, владелец, пользователь и т.д.). При этом законодателю следует учитывать тонкости деятельности разработчика и привлекать его к ответственности только в случае создания ИИ в целях совершения правонарушений. Вид ответственности должен определяться исходя из тяжести содеянного и причиненного ущерба.

ИИ-системы, особенно те, что используются для анализа больших данных, часто обрабатывают огромные объемы персональной информации, это особенно важно для обеспечения информационной

безопасности. Соответственно, возникают вопросы о соблюдении законодательства о защите данных. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»[54] необходимо обеспечить согласованность обработки данных принципам законности, добросовестности и целевого назначения. Особое внимание требует использование биометрических данных, которые могут быть использованы для идентификации личности и требуют особого уровня защиты. Важно разработать механизмы обеспечения прозрачности обработки данных ИИ-системами, позволяющие пользователям понимать, как используется их информация и какие решения принимаются на ее основе. В этих целях следует разработать специальное положение, которое установит перечень информации, подлежащей обработке ИИ, основания ее использования и решения, принимаемые на основе этой информации. Также необходимо обеспечить направление копий согласий на обработку персональных данных, подписанных пользователем, на электронную почту. Поскольку согласия на обработку персональных данных зачастую являются достаточно объемным для чтения и восприятия документом, то пользователи, как правило, подписывают не читая. В данном случае пользователь сможет в любое время ознакомиться с подписанным им согласием на обработку личных данных. Разумным решением также будет допустить на законодательном уровне отзыв согласия на обработку персональных данных в течение установленного времени.

Развитие ИИ в сфере информационной безопасности – это глобальный вызов, который требует международного сотрудничества. Поскольку киберпреступность не знает границ, и мошенники осуществляют свои преступные действия, используя VPN-сервисы находясь в любой стране, то необходимо разработать международные стандарты и правовые рамки, которые будут регулировать использование ИИ в этой области, обеспечивая согласованность

[54] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ // Российская газета. 29.07.2006. № 165.

и эффективность борьбы с киберугрозами. Это включает в себя разработку общих определений, критериев ответственности и механизмов международного сотрудничества в области кибербезопасности[55].

К тому же существующее законодательство часто не учитывает специфику использования ИИ, а также различные формы его проявления. Необходимо разработать новые правовые нормы, которые будут регулировать разработку, внедрение и использование ИИ-систем, учитывая риски и вызовы, связанные с этой технологией. Это включает в себя разработку новых понятий, определений и стандартов (для ИИ на базе браузеров, мессенджеров и т.д.), а также уточнение существующих норм с учетом особенностей ИИ. Целесообразно к тому же возложить на Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации функции по ведению реестра систем ИИ.

Совершенствование Кодекса этики в сфере ИИ, который был принят на I Международном форуме «Этика искусственного интеллекта: начало доверия» в 2021 году, также является значимым правотворческим решением. На сегодня Кодекс устанавливает общие этические принципы и стандарты поведения, которыми следует руководствоваться участникам отношений в сфере ИИ, и предназначен для создания среды доверенного развития технологий ИИ в России[56]. Для совершенствования Кодекса можно рассмотреть следующие предложения: добавить условие о том, что ИИ должен выступать в качестве помощника. Это относится к ключевым отраслям, где вопросы морально-этического выбора стоят наиболее остро (например: финансовая сфера, судопроизводство, трудоустройство). Добавить порядок обжалования решений. Он может быть полезен, когда у человека возникает сомнение в отношении того, принимала ли система решение по важному вопросу самостоятельно или нет.

---

[55] Кудряшова П.А. Правовое регулирование использования искусственного интеллекта // Вестник науки. 2023. № 6 (63). С. 181-187.

[56] Кодекс этики в сфере искусственного интеллекта // СПС «КонсультантПлюс».

В заключение следует отметить, что эффективное использование ИИ в обеспечении информационной безопасности требует комплексного подхода, сочетающего технологические инновации с адекватным правовым регулированием. Только сбалансированный подход позволит реализовать потенциал ИИ для повышения уровня кибербезопасности, при этом минимизируя риски и обеспечивая соблюдение прав и свобод граждан.

Шевченко Екатерина Валерьевна,

канд. юрид. наук, доцент кафедры гражданского права и процесса Северного института (филиала) ФГБОУ ВО «ВГУЮ (РПА Минюста России)»,

Смирнов Вячеслав Максимович,

обучающийся 3 курса Северного института (филиала) ФГБОУ ВО «ВГУЮ (РПА Минюста России)»,
г. Петрозаводск

ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЦЕЛЯХ ЗАЩИТЫ ИНФОРМАЦИИ

Неотъемлемой частью жизни человека является обмен значимой информацией. Рассматривая «эволюцию» передачи данных, можно выделить пять основных, на наш взгляд, этапов. Первый характеризуется личной передачей информации «из уст в уста», второй – появлением письменности и возможностью хранения такой информации на первичных письменных носителях. Третьим этапом можно выделить появление печатных станков – тиражирование информации. Четвертый этап, на наш взгляд, можно охарактеризовать как период «информационной эволюции» – это связано с появлением

технологий радиопередач. Пятый этап характеризуется появлением персональных компьютеров, с помощью которых информация стала наравне с материальными ценностями. Сейчас же практика социальной и государственной жизни доказывает нам, что мы переходим на новый этап – период цифровизации и применения технологий нейронных сетей. Вопрос является дискуссионным, и ряд ученых считают, что нельзя назвать данный переход новым этапом, так как он дополняет пятый. Мы же считаем, что обе точки зрения имеют место быть. Искусственный интеллект стал составной частью нашей повседневной жизни, трансформируя различные сферы деятельности – от образования и медицины до безопасности государства. Главным достоинством технологии нейронных сетей является способность хранения, обработки, анализа огромных массивов данных, прогнозирование событий, что делает такую технологию мощным инструментом повышения эффективности и оптимизации процессов.

Защита информации является одним из важнейших аспектов национальной безопасности Российской Федерации. В условиях глобализации и цифровизации общества задачи по защите информации выходят на новый уровень. Проанализировав статистику, мы пришли к выводу, что с каждым годом количество кибератак на Российскую Федерацию увеличивается. По данным из открытых источников «Лаборатории Касперского» «за 12 месяцев 2024 года в России было зафиксировано 1 811 562 707 кибератак»[57]. Также важно отметить нарушение правил конфиденциальности и утечку данных. Требуется не только внедрение современных технологий нейронных сетей, которые могут повысить устойчивость организаций к таким угрозам, но и создание надежной правовой базы для обеспечения защиты прав и законных интересов субъектов, что могло бы привести к безопасному использованию искусственного интеллекта в такой деятельности. Представляется возможным

[57] В «Лаборатории Касперского» посчитали все кибератаки на Россию за 2024 год : [Электронный ресурс] // Газета.ru. URL: https://www.gazeta.ru/tech/news/2025/01/16/24840404.shtml (дата обращения: 04.03.2025).

использовать такую инновацию, как искусственный интеллект, для защиты информации в сфере информационной безопасности. Однако стоит отметить, что применение технологий нейронных сетей не исключает возможность «стороннего» влияния на технологию, что может привести к несанкционированному доступу третьих лиц к информации. Поэтому одной из важнейших является задача правового регулирования общественных отношений, складывающихся в связи с развитием и использованием технологий искусственного интеллекта.

Прежде всего, представляется необходимым формирование национальной системы стандартизации и оценки соответствия в области технологий искусственного интеллекта и робототехники. Для решения поставленной задачи мы должны структурировать работу, подойти к решению комплексно и поэтапно. В частности, утвержден Национальный стандарт Российской Федерации ГОСТ Р 59277-2020 «Системы искусственного интеллекта. Классификация систем искусственного интеллекта» (далее по тексту – СИИ). Целью указанного стандарта является «установление принципов классификации ССИ. Внедрение данного стандарта необходимо для повышения эффективности использования систем *искусственного интеллекта* при решении прикладных задач. Установление классификации СИИ позволит сравнивать различные решения по таким параметрам, как вид деятельности, структура знаний, функции контура управления, безопасность, конфиденциальность, степень автоматизации, методы обработки информации, интеграция/интероперабельность, комплексность системы, архитектура, специализация»[58].

Был принят Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», который ввел общий механизм установления экспериментальных правовых режимов, позволяющих

[58] ГОСТ Р 59277-2020. Системы искусственного интеллекта. Классификация систем искусственного интеллекта : дата введения 01.03.2021. URL: http://gost.gtsever.ru/Data/754/75406.pdf (дата обращения: 05.03.2025).

заинтересованным лицам (прежде всего юридическим лицам) не применять отдельные обязательные требования, устанавливаемые государством, т.е. законом были допущены некоторые послабления в правовом регулировании в течение определенного периода времени по некоторым направлениям, а именно по 8 сферам разработки, апробации и внедрения цифровых инноваций. В частности, в медицинской деятельности санкционировано применение телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан с помощью искусственного интеллекта. В сфере проектирования с помощью нейронных сетей стали решаться вопросы производства и эксплуатации транспортных средств, в том числе высокоавтоматизированных транспортных средств и беспилотных воздушных судов, аттестации их операторов, предоставление транспортных и логистических услуг и организации транспортного обслуживания.

Данные решения требовали соответствующего правового регулирования внедряемых технологий искусственного интеллекта, в том числе в целях защиты информации, а как следствие, приказом Федерального агентства по техническому регулированию и метрологии от 28 июня 2022 г. № 545-ст утверждается национальный стандарт РФ ГОСТ Р 59921.1-2022 «Системы искусственного интеллекта в клинической медицине. Часть 1. Клиническая оценка».

Приказом Росстандарта от 11 октября 2024 года № 1436-ст утвержден ГОСТ Р 71686-2024 «Искусственный интеллект. Модели машинного обучения для проведения косвенных измерений свойств материалов. Общие положения». Стандарт устанавливает общие положения к разработке (обучению и тестированию), верификации и эксплуатации моделей машинного обучения для косвенных измерений свойств материалов, применим для измерений, в которых функция преобразования (функция измерений) средства измерений неизвестна априори и/или не может быть определена в силу ее сложности. Стандарт предназначен для использования организациями и специалистами, занимающимися разработкой, испытаниями

и эксплуатацией средств измерений на основе искусственного интеллекта и машинного обучения для определения свойств материалов, используемых в различных отраслях промышленности и исследованиях. Стандарт не распространяется на модели машинного обучения для проведения прямых измерений свойств материалов или для других целей, не связанных с измерениями[59].

Анализ представленных правовых актов показывает, что существует положительный опыт правового регулирования применения технологий искусственного интеллекта. Представляется возможным и апробация технологий нейронных сетей и в деятельности по защите информации.

Ранее в целях решения другой, как нам кажется, не менее важной задачи формирования единой федеральной политики в области правового регулирования искусственного интеллекта были приняты следующие важные документы.

В соответствии с Указом Президента РФ от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» сформирована национальная программа «Цифровая экономика Российской Федерации», одной из задач которой является «создание системы правового регулирования цифровой экономики, основанной на гибком подходе в каждой сфере»[60].

В соответствии с Указом Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации" (с изменениями и дополнениями) утверждена стратегия развития искусственного интеллекта до 2030 г.

---

[59] ГОСТ Р 71686-2024 Искусственный интеллект. Модели машинного обучения для проведения косвенных измерений свойств материалов. Общие положения. URL: https://mobileonline.garant.ru/#/document/411143783/paragraph/28/doclist/2160

[60] Кодификация основ правового регулирования цифровой среды и права человека: нужен ли цифровой кодекс? [Электронный ресурс] // Фонд Росконгресс. URL: https://roscongress.org/materials/kodifikatsiya-osnov-pravovogo-regulirovaniya-tsifrovoy-sredy-i-prava-cheloveka-nuzhen-li-tsifrovoy-k/ (дата обращения: 06.03.2025).

В соответствии с федеральным проектом «Нормативное регулирование цифровой среды» принят федеральный закон, регулирующий механизмы формирования и использования «облачной» электронной подписи, установление унифицированных требований к универсальной (единой) усиленной квалифицированной электронной подписи, визуализацию электронной подписи в электронном документе; принят федеральный закон, предусматривающий урегулирование статуса совершаемых в письменной (электронной) форме сделок, а также автоматизированных ("самоисполняемых") договоров и т.д.

Важно обратить внимание на то, что согласно Гражданскому Кодексу РФ программы для ЭВМ относятся к объектам авторских прав и охраняются как литературные произведения. Следовательно, авторские права разработчика на созданный им искусственный интеллект законодательно закреплены и защищены. Сегодня остается неурегулированным вопрос авторских прав на объекты, созданные самим искусственным интеллектом: нет ни единой позиции у правоприменителей, и на сегодняшний день нет нормативного правового акта, регулирующего этот вопрос. Представляется возможным наделить искусственный интеллект правосубъектностью, создать закон, закрепляющий и регулирующий данные процессы, поскольку сегодня не урегулированы вопросы ответственности: за решения предлагаемые самим искусственным интеллектом, людей (пользователей, должностных лиц, компаний) за действия искусственного интеллекта, вызванные самой рекомендаций, указанием искусственного интеллекта, что является неотъемлемой частью введения таких технологий в деятельность по защите информации.

В рамках национальной безопасности Российской Федерации для своевременного обнаружения и предотвращения кибератак на массивы данных предлагаем создание программного обеспечения, основанного на технологиях искусственного интеллекта. Продукт, который сможет обнаруживать вредоносные программы, уведомлять человека, а при должном регулировании и отлаженной работе самостоятельно реагировать на угрозу, например Endpoint Detectionand Response. Также стоит рассмотреть технологии нейронных

сетей как механизм анализа поведения пользователей. Воспользовавшись отраслью искусственного интеллекта, основанной на том, что «нейронные сети могут обучаться – Machine-learning»,[61] мы можем отслеживать поведение пользователей и своевременно выявлять отклонения от «нормы». После испытания такого программного обеспечения можно попробовать доверить технологии реагировать на попытки нарушения, например блокировать доступ к системе или изолировать зараженные устройства, что позволит минимизировать ущерб. Также возможности нейронных сетей позволяют прогнозировать кибератаки.

Таким образом, создание специального программного обеспечения, основанного на технологиях искусственного интеллекта, возможно при адаптации под реалии двадцать первого века и при должном законодательном регулировании.

Библиографический список

1. Кодификация основ правового регулирования цифровой среды и права человека: нужен ли цифровой кодекс? [Электронный ресурс] // Фонд Росконгресс : Пространство доверия. – URL: https://roscongress.org/materials/kodifikatsiya-osnov-pravovogo-regulirovaniya-tsifrovoy-sredy-i-prava-cheloveka-nuzhen-li-tsifrovoy-k/ (дата обращения: 06.03.2025).

2. Черкасов Д.Ю., Иванов В.В. Машинное обучение // Наука, техника и образование. – 2018. – № 5 (46). – URL: https://cyberleninka.ru/article/n/mashinnoe-obuchenie (дата обращения: 08.03.2025).

[61] Черкасов Д.Ю., Иванов В.В. Машинное обучение : [Электронный ресурс] // Наука, техника и образование. 2018. № 5 (46). URL: https://cyberleninka.ru/article/n/mashinnoe-obuchenie (дата обращения: 08.03.2025).

Некрасова Елена Владимировна,

к.э.н., доцент кафедры информационной безопасности в управлении ИПСУБ ФГБОУ ВО «Удмуртский государственный университет», доцент кафедры менеджмента и права ФГБОУ ВО «Удмуртский государственный аграрный университет», г. Ижевск

АКТУАЛЬНЫЕ ВОПРОСЫ УПРАВЛЕНИЯ ПРОЦЕССАМИ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ В СОВРЕМЕННЫХ УСЛОВИЯХ

Обеспечение устойчивого социально-экономического развития хозяйствующего субъекта является приоритетной задачей руководителей разного уровня. В качестве основных принципов обеспечения эффективности систем управления являются инновационность, клиентоориентированность, гибкость и адаптивность к вызовам внешней среды. Этого во многом можно добиться, используя современные технологии цифровизации, которые позволят значительно повысить качество принятия и реализации управленческих решений. Однако неоспоримым является факт, что качество управленческих решений зависит от своевременности, полноты, структурированности и достоверности информации о состоянии и поведении объекта, степени влияния факторов внешней и внутренней среды.

Сегодня вопрос цифровой трансформации является одним из основных трендов современной экономики. Цифровая трансформация подразумевает процесс оптимизации бизнес-процессов производства и управления с целью повышения эффективности осуществляемой деятельности. В качестве инструментов цифровой трансформации сегодня используют: электронный документооборот, автоматизацию бизнес-процессов, привлечение виртуальных помощников и искусственного интеллекта для различных уровней управления.

Однако эти тенденции, находящиеся вне стратегической целенаправленности и системности функционирования и устойчивого развития организаций, могут дать лишь краткосрочный и фрагментарный эффект, что в условиях высококонкурентной и турбулентной среды недопустимо, особенно на национальном, региональном и отраслевом уровнях. Следовательно, процессы цифровой трансформации требуют фундаментальных изменений в системе стратегического управления. С нашей точки зрения, необходимо выделить ряд аспектов трансформации систем стратегического управления с учетом современных условий и тенденций изменения среды (табл. 1).

Таблица 1

Изменение стратегических методов управления экономическими субъектами

Аспекты систем управления	«Традиционное стратегическое планирование», основанное на стратегическом анализе и позиционировании	«Гибкое стратегическое проектирование» через выставление ключевых приоритетов и оценке стратегического потенциала
Цели	Последовательное (устойчивое) развитие социально-экономическими системами	Реализация стратегического потенциала обеспечения долгосрочных конкурентных преимуществ и обеспечения социально-экономической безопасности объекта
Задачи	Улучшение финансово-экономического положения. Изменение конкурентной позиции на целевом рынке	Моделирование будущего через развитие стратегического потенциала. Формирование механизмов гибкого стратегичекого планирования. Развитие систем принятия решений с использованием цифровых технологий и искусственного интеллекта
Направление принятия решений	Вертикально-ориентированное, централизованное	Целе- и проектоориентированное, интегрированное (сочетающее централизованные, децентрализованные процессы) при активном участии систем государственного управления в рамках национальных, отраслевых государственных целевых программ
Ресурсное обеспечение	Централизованное, бюджетно-ориентированное, использование субсидий и дотаций в социально-значимые области	Проектно-целевое, грантовое, инициативное бюджетирование активных групп населения

В принятой в 2024 году Стратегии научно-технологического развития Российской Федерации [1. С. 2–3] отмечается, что «научно-технологическое развитие является одним из стратегических национальных приоритетов Российской Федерации и определяется комплексом внешних и внутренних (по отношению к области науки и технологий) факторов, формирующих систему больших вызовов. Большие вызовы создают существенные риски для общества, экономики, системы государственного управления, но одновременно представляют собой важный фактор для появления новых возможностей и перспектив научно-технологического развития». Неоспоримым элементом реализации данной стратегии является цифровая трансформация систем государственного и отраслевого управления на разных уровнях. Это предполагает выделение следующих основных направлений преобразования систем стратегического управления социально-экономическими системами:

– формирование новой регуляторной среды взаимодействия (коммуникаций) граждан, бизнеса и государства, возникающих с развитием цифровой экономики;

– создание современной высокоскоростной инфраструктуры хранения, обработки и передачи данных, обеспечение устойчивости и безопасности ее функционирования;

– формирование системы подготовки и повышения квалификации специалистов для цифровой экономики;

– поддержка развития перспективных «сквозных» цифровых технологий и проектов по их внедрению в отраслях и регионах;

– повышение эффективности государственного управления и оказания государственных услуг посредством внедрения цифровых технологий и платформенных решений.

В рамках реализации Указов Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года», в том числе с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий

в экономике и социальной сфере, Правительством Российской Федерации была сформирована национальная программа «Цифровая экономика Российской Федерации», в состав которой входят ряд федеральных проектов: «Нормативное регулирование цифровой среды», «Кадры для цифровой экономики», «Информационная инфраструктура», «Информационная безопасность», «Цифровые технологии», «Цифровое государственное управление», «Искусственный интеллект», «Обеспечение доступа в Интернет за счет развития спутниковой связи», «Развитие кадрового потенциала ИТ-отрасли».

Однако следует отметить, что использование цифровых технологий должно быть гибким и адаптивным, применительно к конкретным отраслям социально-экономического развития национальной экономики. Так, цифровая трансформация в отрасли АПК предполагает не только комплексное внедрение ряда цифровых технологий в рамках взаимосвязанных концепций точного земледелия и умного сельского хозяйства, но и развитие интегрированных решений в области устойчивого ресурсосбережения, технологии Интернета вещей, автоматизированную и беспилотную технику, роботизированные производственные системы, платформенные технологии обработки больших данных и машинного обучения.

С нашей точки зрения, базовой задачей стратегического управления АПК на основе цифровой трансформации является создание платформ и программно-аппаратных средств поддержки принятия решений на основе анализа больших данных о внутренней и внешней среде и моделирования развития ситуации. Развитие и интеграция цифровых систем поддержки принятия решений на разных уровнях управления в сочетании с проектно-ориентированным подходом позволят значительно повысить эффективность социально-экономического отраслевого и национального развития.

Принятая в Удмуртской Республике Концепция цифрового развития экономики включает в себя комплекс целей и задач регионального значения, которые направлены на организацию преобразования приоритетных отраслей экономики и социальной сферы, включая здравоохранение, образование, промышленность, сельское

хозяйство, строительство, городское хозяйство, транспортную и энергетическую инфраструктуру, финансовые услуги, посредством внедрения цифровых технологий и платформенных решений. Концепция цифрового развития региона была разработана Высшей школой экономики (НИИ ВШЭ) по заказу Мининформсвязи Удмуртской Республики и утверждена в марте 2020 г. В ней предусмотрено три основных направления: цифровизация всех отраслей, формирование кадрового потенциала и создание условий для развития ИТ-отрасли [4]. Для каждой из отраслей утвержден план мероприятий по запуску смарт-сервисов. Для управления реализацией Концепции создан Координационный совет по развитию цифровой экономики.

Важным элементом стратегического управления развитием отраслевых и региональных систем управления является обеспечение кибербезопасности информационных систем и процессов. С учетом выявленного стратегического потенциала критической информационной инфраструктуры объектов формируются Политики информационной безопасности и планы перехода на преимущественное использование российского программного обеспечения, совершенствования программно-аппаратных комплексов, повышения квалификации специалистов с учетом поставленных задач.

В условиях роста сложности среды и развития технологий в системе управления кибербезопасности организаций разного уровня можно выявить следующие тенденции:

1) постоянный рост объема и сложности киберугроз, что влияет на скорость и качество принятия решений;

2) исходя из вышесказанного, расследования причин и последствий устранения угроз занимают все больше времени, возрастает уровень нагрузки на специалистов и руководителей, что влияет на мотивацию персонала;

3) для работы с киберугрозами часто используются множество технологий и инструментов, которые бывают неинтегрированы, что повышает использование ресурсов и стоимость работ по устранению и предотвращению опасностей;

4) усиливаются тенденции к ужесточению нормативно-правовых и технологических требований к системе информационной безопасности организаций, особенно в отношении обеспечения защиты критической инфраструктуры;

5) важным вопросом является приоритетное развитие использования отечественных программных продуктов в системе управления организациями и обеспечение адаптивной системы информационной безопасности;

6) совершенствование системы внутреннего информационного аудита безопасности систем управления организационных и производственных процессов.

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

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

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

– совершенствование адаптивной и многоуровневой системы информационной безопасности в организации;

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

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

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

Все решения должны быть сконцентрированы в рамках реализации Политики информационной безопасности организации на долгосрочный период в виде Стратегии развития информационной безопасности, соответствующих планов и программ.

Таким образом, комплексный подход к развитию стратегического потенциала на основе обеспечения информационной безопасности систем управления разного уровня позволит добиться необходимого уровня конкурентоспособности и социально-экономической стабильности организационного развития в долгосрочной перспективе с учетом динамики развития внешней и внутренней среды.

Библиографический список

1. О Стратегии научно-технологического развития Российской Федерации : Указ Президента Российской Федерации от 28 февраля 2024 г. № 145. – URL: https://www.garant.ru/products/ipo/prime/doc/408518353/

2. Об утверждении Стратегии цифровой трансформации в Удмуртской Республике на период до 2030 года : указ Главы Удмуртской Республики от 31 марта 2020 г. № 74. – URL: https://docs.cntd.ru/document/570733992

3. Министерство цифрового развития Удмуртской республики. URL: https://it.udmurt.ru/

4. Некрасова Е.В. Научно-методические аспекты совершенствования стратегического планирования на региональном уровне (на примере муниципальных образований Удмуртской Республики) // Развитие управления экономической безопасностью деятельности хозяйствующих субъектов и публичных образований : материалы Международной научно-практической конференции, посвященной 70-летию д.э.н., профессора Алборова Р.А. – 2023. С. 250–257.

5. Чазова И.Ю., Акмаров П.Б., Князева О.П. Развитие цифровизации аграрного производства и оценка использования ее потенциала в Удмуртии // Вестник УдГУ. – 2022. – Т. 32, № 6. – С. 1035–1041.

Денисович Вероника Владимировна,

канд. юрид. наук, доцент, старший научный сотрудник
Научно-исследовательского института цифровых технологий
и права Казанского инновационного университета
имени В.Г. Тимирясова,
г. Казань

СОДЕРЖАНИЕ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ МЕТАВСЕЛЕННЫХ: ПРОБЛЕМЫ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ

С точки зрения Н.А. Носова, «виртуальная реальность» – это особого свойства материя, которая не зависит от природы и физических свойств ее отдельных элементов, характеризующаяся следующими основными признаками: производная от психики человека, актуальность для данного пространства и времени, автономность, интерактивность[62].

Если рассматривать виртуальный мир с точки зрения технологического обоснования, то верным следует считать точку зрения А.Б. Смушкина[63], который в своих исследованиях подтверждает, что VR-пространства компьютерно-опосредованы. Это утверждение не дает возможности ложно смешивать рассматриваемый вид цифровых технологий с симулякрами психологического или мифотворческого характера.

В.С. Бабенко, М.Б. Игнатьев, Е.А. Шаповалов, Д.И. Шапиро, включая ряд зарубежных авторов[64], рассматривают виртуальную

[62] Носов Н.А. Словарь виртуальных терминов // Труды лаборатории виртуалистики. Вып. 7. Труды центра профориентации. М. : Путь, 2000. С. 16.

[63] Смушкин А.Б. Использование компьютерно-опосредованной реальности в правоохранительной деятельности // Вестник Томского государственного университета. 2020. № 454. С. 251-259.

[64] Носов Н.А. Виртуальные реальности // Труды лаборатории виртуалистики. Вып. 4. М. : Центр профориентации: Центр виртуалистики, 1998. 212 с.; Игнатьев М.Б. Архитектура виртуальных миров : монография. СПб. : Политехника, 2005. 150 с.; Шаповалов Е.А. Философские проблемы

реальность как кибернетическое пространство, созданное на базе вычислительной техники. Суть виртуального пространства в этом случае сводится к тому, что органы чувств человека реагируют несколько иначе. Пользователь реагирует на ту систему, которая создана в условиях виртуальной среды, это и является основным провоцирующим фактором в современных условиях реализации норм права, т.к. гарантии защиты людям никто по большому счету не предоставляет. Пользователю предъявляется особый мир, имеющий собственные, возможно, отличные от ординарных, повседневных, реальных, пространство, время и законы существования.

Виртуальное пространство представляет собой в целом разработанный термин[65]. Синонимичными можно считать – «киберпространство», «интернет-пространство»[66]. Суть всех вышеназванных категорий сводится к тому, что человек использует гарнитуры или технологические приспособления для того, чтобы попасть в VR-пространство, его изменить, использовать именно так, как он пожелает[67]. Сам по себе термин достаточно сложный и комплексный, его нельзя рассматривать только в одной плоскости[68].

виртуальной реальности // Виртуальная реальность как феномен науки, техники и культуры : материалы I Всероссийского симпозиума по философским проблемам виртуальной реальности. СПб. : СПбГАК, 1996. С. 6-12; Шапиро Д.И. Человек и виртуальный мир: Когнитивные, креативные и прикладные проблемы. М. : Эдиториал УРСС, 2000. 222 с.; Ребер Б. Виртуальное: апокалипсис или: повторное посещение платоновской пещеры // Концепция виртуальных миров и научное познание. СПб. : РХГИ, 2000. С. 213-225; Дрейфус Х.Л. Телеэпистемология: последний рубеж Декарта // Виртуалистика: экзистенциальные и эпистемологические аспекты. М. : Прогресс-Традиция, 2004. С. 98; Heim Michael. The Metaphysics of virtual reality / Virtual reality: theory, practice and promise Westport and London (1991); Krueger M. (1991). Artificial Reality II. Addison-Wesley.

[65] Залоило М.В. Метаморфозы юридического языка в виртуальном пространстве // Журнал российского права. 2024. № 12.

[66] History of Virtual Reality. URL: https://www.vrs.org.uk/virtual-reality/history.html.

[67] Virtual reality. An interview with Jaron Lanier // Whole Earth Review. Fall 1989. P. 110; Частиков А. Архитекторы компьютерного мира. Джарон Ланье – отец виртуальной реальности. URL: https://history.wiki-reading.ru/387591?ysclid=lbxg61tow68624146; Таратута Е.А. Социальный смысл виртуальной реальности : автореф. дис. ... канд. филос. наук. СПб.,

В зарубежной теории и практике VR-пространство и пространство дополненной реальности (гибридное пространство), киберпространство (такой перевод также имеет право на существование) – новое понимание реальности с новой формой юрисдикции государства. Для некоторых стран – это форма государственного суверенитета (Китай)[69]. Таким образом, можно констатировать возникновение новой отрасли права – киберправа. Широкую известность приобрело определение киберпространства, сформулированное в 1997 г. Верховным судом США: «совокупность инструментов, создающих уникальную среду, расположенную вне какого-либо определенного географического места, но доступную для всех в любой точке мира с имеющимся доступом в Интернет»[70].

Теперь необходимо проанализировать понятие «киберпространство» (или «виртуальный мир»). Современное определение киберпространства включает в себя набор социальных взаимодействий, которые возникают, когда пользователь подключается к Интернету или к локальным сетям. Эти взаимодействия связаны с данными, обработка которых происходит с помощью электронно-вычислительных машин[71].

2003. С. 6; Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 457-ст Национальный стандарт Российской Федерации «Защита информации при использовании технологий виртуализации общие положения» Information protection. Information security with virtualization technology. General ГОСТ Р 56938-2016.

[68] Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 457-ст Национальный стандарт Российской Федерации «Защита информации при использовании технологий виртуализации общие положения» Information protection. Information security with virtualization technology. General ГОСТ Р 56938-2016.

[69] Johnson D.R., Post D.G. Law and Borders – The Rise of Law in Cyberspace // Stanford Law Review. 1996. Vol. 48. P. 1367-1402.

[70] Цит. по: Мажорина М.В. Киберпространство и методология международного частного права // Право. Журнал Высшей школы экономики. 2020. № 2. С. 233.

[71] Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского университета. Серия 18. Социология и политология. 2018. № 1. URL: https://cyberleninka.ru/article/n/kiberprostranstvo-territoriya-sovremennoy-zhizni (дата обращения: 05.05.2024).

В наше время понятие «виртуальный мир» становится все более популярным среди специалистов различных областей. В контексте информационных технологий это выражение обычно описывает среду, созданную и поддерживаемую с помощью компьютерных технологий, которая предназначена для обеспечения взаимодействия пользователей через цифровые персонажи, известные как аватары. Этот термин, заимствованный из индуистской философии, изначально обозначал земное воплощение божества[72].

Термин «метавселенная» образован от английского «meta»[73] – «трансцендентность» и «verse» – «мир». Под метавселенной понимают современное многофункционное виртуальное пространство, объединяющее физическую, дополненную и виртуальную реальность (некоторые авторы включают еще одну цифровую технологию в эту категорию – гаптику). Это своего рода новейшая форма 3D-Интернет, направленная на создание общего самоподдерживающегося виртуального социального пространства, характеризующегося признаками иммерсивности, транспорентности и многомерности[74]. Метавселенная включает в себя искусственный интеллект, виртуальную и дополненную реальность, блокчейн, интернет-вещей и т.д.[75].

Выступая в 2021 г. на конференции «Технологии искусственного интеллекта для решения социальных задач», Президент России В.В. Путин подчеркнул необходимость использования возможностей метавселенных для общения, обучения, работы, охарактеризовав

---

[72] Четвергов Д.С. Правовой режим аватара: регулирование оборота цифрового образа личности в метавселенной // Юридическая наука. 2023. № 7. URL: https://cyberleninka.ru/article/n/pravovoy-rezhim-avatara-regulirovanie-oborota-tsifrovogo-obraza-lichnosti-v-metavselennoy (дата обращения: 05.05.2024).

[73] Деятельность Meta Platforms Inc. по реализации продуктов – социальных сетей Facebook и Instagram на территории РФ запрещена по основаниям осуществления экстремистской деятельности.

[74] Wang Y., Su Z., Zhang N. [et al.]. A Survey on Metaverse: Fundamentals, Security, and Privacy // arXiv:2203.02662v4.

[75] Zhao Ruoyu, Zhang Yushu, Zhu Youwen [et al.]. Metaverse: Security and Privacy Concerns // Journal of latex class files. 2021. Vol. 14. Iss. 8. P. 1–7; Лескина Э.И. Метавселенныя и задачи в области правового регулирования данных // Юрист. 2023. № 3.

их как «настоящий вызов для технологических компаний, креативных индустрий, для создателей устройств виртуальной и смешанной реальности. Даже для юристов, которым предстоит разработать нормы регулирования экономических, общественных отношений в принципиально новом мире... »[76].

Четкого определения метавселенных до сих пор не выработано[77], это касается и теории уголовного права. Т.Я. Хабриева отмечает: «Цифровые технологии способны менять образ права, влиять на его регулятивный потенциал и эффективность, открывать дорогу или блокировать его действие в новых измерениях социальной реальности»[78].

Определение метавселенной, выработанное М. Боллом, звучит следующим образом: «Это масштабируемая и совместимая сеть визуализируемых в реальном времени 3D-виртуальных миров и сред, которые могут синхронно и постоянно восприниматься практически неограниченным числом пользователей с индивидуальным ощущением присутствия и непрерывностью данных, таких как личность, история, права, объекты, коммуникации и платежи»[79].

К основным чертам нового объекта изучения и в том числе нового объекта уголовно-правовой охраны относится:

1) бесконечное существование;

2) непосредственная синхронизация с реальностью;

3) отсутствие ограничений по количеству одновременно подключившихся пользователей (аватаров или цифровых двойников человека);

---

[76] URL: http://www.kremlin.ru/events/president/news/67099#sel=42:1:HTU, 42:41:lhm (дата обращения: 15.12.2023).

[77] См., например: Лескина Э.И. Метавселенная и задачи в области правового регулирования данных // Юрист. 2023. № 3; Овчинников А.И., Ширинских П.И. Метавселенные и право: вызовы новых технологий в условиях дальнейшего развития Интернета // Вестник юридического факультета Южного федерального университета. 2023. Т. 10. № 2.

[78] Хабриева Т.Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9. С. 15.

[79] Ball M. What It Is, Where to Find it, and Who Will Build It. 13.01.2020. URL: https://www.matthewball.vc/all/themetaverse.

4) собственная полноценно функционирующая экономика;

5) интеграция цифрового и реального мира через публичные и частные платформы, частные и общедоступные сети;

6) трансплатформенность[80].

Тем самым мы можем достаточно уверенно утверждать: широкомасштабное использование метавселенной в жизни человека приводит к объединению внутри этого ресурса всех сервисов и цифровых пространств, отождествление виртуального и реального. Следовательно, быстрее происходит отождествление имеющихся отношений в реальном мире с правоотношениями внутри нового виртуального ресурса. Метавселенные, как новый этап развития технологий и цифровой экономики, требуют глубокого осмысления, так как необходимо добиться цифрового постоянства и идентичности и создать те же условия для взаимодействия людей, что и в физической реальности, в том числе и ее охраны. Технологии будущего и внедрение их в общественную систему – вопрос времени, поэтому запретительная политика не видится эффективной для развития Российской Федерации, отраслевого законодательства, в том числе и уголовно-правового[81].

Метавселенная требует адаптированных под новую реальность инструментов уголовно-правового регулирования рассматриваемых правоотношений. Не представляется возможным допустить полный запрет инновационных технологий, так как это означает технологическое отставание страны[82], что недопустимо в рамках государственной политики технологического суверенитета.

Несмотря на многочисленность споров относительно термина «метавселенная», нельзя отрицать то обстоятельство, что на современном этапе цифрового развития прототипы метавселенных

---

[80] URL: https://www.matthewball.vc/all/themetaverse (дата обращения: 21.03.2022); Boll M. The metaverse and how it will revolutionize everything, 2022 // Liveright. P. 48.

[81] Измайлова А.А. Метавселенная как новая экономическая система // Modern Economy Success. 2021. № 6. С. 175-179.

[82] Рожкова М.А. Виртуальная реальность и метавселенная: предмет правового исследования // Virtual reality and Metaverse: subject of legal research // Закон.ру. 2021. 12 января.

уже существуют в России и используются для упрощения гражданского оборота и общения граждан. Метавселенная – это прежде всего виртуальное пространство. Грань между метавселенной и виртуальной реальностью настолько тонкая, что обнаружить и обосновать ее крайне сложно[83], переход от реального в виртуальное может создать угрозу безопасности личности и государства, что не допустимо при нынешнем уровне развития правовой грамотности и юридической технике уголовного закона.

Стяжкина Светлана Александровна,

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

УГОЛОВНО-ПРАВОВАЯ ОХРАНА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность информационных систем, технологий и процессов становится ключевой задачей в сфере обеспечения общественной безопасности. Информация становится наиболее востребованным предметом преступных посягательств. Интенсивный рост преступлений в сфере информационных технологий требует и адекватной реакции со стороны законодателя в части обеспечения ее безопасности и стабильного функционирования информационных процессов.

Следует отметить, что уголовное законодательство не стоит на месте и активно развивается в части реагирования на динамично

[83] Ситников М.С. К вопросу о проблеме использования лицензионного договора в рамках метавселенных // Цивлист. 2023. № 2.

изменяющиеся механизмы и способы совершения преступлений, а также обеспечения защиты различных видов охраняемой информации.

В 2017 году был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» и, как следствие, Уголовный кодекс Российской Федерации был дополнен новой статьей 274.1, предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Понятие критической информационной инфраструктуры раскрывается в вышеуказанном законе. Исходя из анализа положений закона, можно сделать вывод о том, что КИИ – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Речь идет о наиболее важных сферах жизнеобеспечения общества и государства, воздействуя на которые, вред причиняется прежде всего общественной, экономической безопасности государства. Как указывается в литературе, «Нарушению стабильного функционирования объектов критической информационной инфраструктуры придается повышенное значение ввиду того, что это может стать причиной серьезных последствий. Об этом же свидетельствует и содержание пояснительной записки к законопроекту, в которой акцент сделан на том, что правильное планирование и реализация компьютерной атаки способно полностью остановить работу государственных организаций и привести к катастрофе в общественной, экономической или финансовой сфере»[84].

[84] Тамбиев С.А. Пути обеспечения безопасности критической информационной инфраструктуры Российской Федерации. URL: https://cyberleninka.ru/article/n/puti-obespecheniya-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (дата обращения: 01.05.2025).

Безусловно, следует согласиться с мнением ряда ученых, которые говорят о том, что «объекты критической информационной инфраструктуры действительно требуют особой уголовно-правовой охраны»[85]. Вопрос возникает в целесообразности выделения отдельного состава преступления, предметом которого будет выступать критическая информационная инфраструктура.

Обращаясь к анализу ст. 274.1 УК РФ, следует отметить, что по большей своей части она объединяет в себе признаки ст. 272, 273 и 274 УК РФ с той лишь разницей, что предметом ст. 274.1 выступает критическая информационная инфраструктура РФ. Многие исследователи обоснованно критикуют положения рассматриваемой статьи. В частности, особой критике подвергается ч. 1 ст. 274.1 УК РФ, где речь идет о создании, распространении и (или) использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Речь идет о программах, которые предназначаются именно для неправомерного воздействия на критическую информационную инфраструктуру. Но, по мнению Л.И. Федосеева, «практически невозможно определить предназначение программы для воздействия исключительно в отношении объектов КИИ РФ»[86]. Таким образом, «указание законодателя на заведомое предназначение таких программ порождает вопрос о квалификации использования уже существующей вредоносной программы, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации при воздействии на КИИ»[87].

---

[85] Дремлюга Р.И., Зотов С.С., Павлинская В.Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. № 2. С. 130-139.

[86] Федосеев Л.И. Анализ отдельных положений статьи 274.1 Уголовного кодекса Российской Федерации // Законность и правопорядок: история, современность, актуальные проблемы : материалы IV межвуз. студ. науч. конф. Москва, 2020. С. 190–194.

[87] Ефремова М.А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Россий-

В части второй рассматриваемой статьи речь идет о неправомерном доступе к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации. Это положение практически дублирует диспозиции ст. 272 УК РФ, за исключением признака последствий. Если в ст. 272 УК РФ в качестве последствий указывается на копирование, блокирование, модификацию и уничтожение информации, то в ст. 274.1 речь идет о вреде, причиняемом КИИ.

Не менее сложным является вопрос квалификации действий, предусмотренных ч. 3 ст. 274.1 УК РФ, где речь идет о нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации. Сложности возникают при оценке объективной стороны в части нарушения правил, которые разрабатываются в каждом конкретном учреждении, организации, носят локальный характер и могут существенно отличаться на каждом предприятии или организации.

ской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13, № 4 (50). С. 86–92.

А также одной из проблем является определение субъективной стороны рассматриваемого преступления, аналогично проблемам, возникающим при квалификации действий по ст. 274 УК РФ.

Общей проблемой, возникающей при квалификации по всем трем частям указанной статьи, является вопрос о субъективной стороне данного преступления. Особенностью состава преступления, предусмотренного ст. 274.1 УК РФ, является предмет преступного посягательства, а именно критическая информационная инфраструктура Российской Федерации, которая и определяет дифференциацию ответственности за посягательства на различные виды информационных ресурсов. Представляется, что виновное лицо должно знать о предмете преступления и его особенностях. Может ли лицо, осуществляющее посягательства на информационные ресурсы и технологии, достоверно знать, что они относятся к критической информационной инфраструктуре, принадлежность к которой определяется включенностью в реестр? Судя по всему, нет. Принадлежность к КИИ определяется Реестром значимых объектов критической информационной инфраструктуры РФ, порядок ведения которого утвержден Федеральной службой по техническому и экспортному контролю от 06.12.2017. В соответствии с вышеуказанным Порядком, сведения из Реестра относятся к информации ограниченного доступа. Таким образом, ни виновное лицо, ни сотрудники правоохранительных органов не могут знать о принадлежности данных информационных ресурсов и технологий к критической информационной инфраструктуре РФ. Об этом свидетельствуют и данные судебной практики, когда посягательства на один и тот же объект квалифицируются по-разному (в частности, речь идет о неправомерном доступе к данным абонентов мобильных систем, в одном случае квалифицировали по ст. 272 УК РФ, в другом по ч. 2 ст. 274.1 УК РФ).

Определяя предмет преступления в качестве кримообразующего фактора, законодатель указывает на его особую значимость и ценность, требующего особой уголовно-правовой охраны. Виновное лицо должно знать об особенностях предмета преступного посягательства, чтобы нести ответственность за причинение вреда

рассматриваемому предмету. Таким образом, субъективная сторона ст. 274.1 УК РФ предполагает наличие прямого умысла, включающее в себя знание о специфике предмета посягательства.

Являясь специальной нормой, ст. 274.1 УК РФ предусматривает только один признак, отграничивающий ее от смежных составов, таких как ст. 272, 273 и 274 УК РФ, это предмет преступления, а именно критическая информационная инфраструктура Российской Федерации.

В заключение хотелось бы отметить, что, на наш взгляд, выделение отдельной статьи, предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, предполагающей признаки, аналогичные тем, которые содержатся в ст. 272, 273 и 274 УК РФ, с разницей в предмете преступления, представляется необоснованным. Нагромождение действующего уголовного кодекса дополнительными специальными нормами, которые содержат лишь один из дифференцирующих признаков состава, ведет к казуистичности и вызывает дополнительные сложности в квалификации.

Следует согласиться с мнением М.А. Ефремовой о том, «что дифференцировать ответственность за посягательства в отношении объектов КИИ можно было бы и в рамках этих статей путем включения в них соответствующих квалифицирующих признаков»[88]. Такое законодательное решение было бы практичнее и грамотнее с точки зрения оснований дифференциации ответственности.

Библиографический список

1. Дремлюга Р.И., Зотов С.С., Павлинская В.Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. – 2019. – № 2. – С. 130–139.

[88] Ефремова М.А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13, № 4 (50). С. 86–92.

2. Ефремова М.А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. – 2022. – Т. 13, № 4 (50). – С. 86–92.

3. Тамбиев С.А. Пути обеспечения безопасности критической информационной инфраструктуры Российской Федерации. – URL: https://cyberleninka.ru/article/n/puti-obespecheniya-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (дата обращения: 01.05.2025).

4. Федосеев Л.И. Анализ отдельных положений статьи 274.1 Уголовного кодекса Российской Федерации // Законность и правопорядок: история, современность, актуальные проблемы : материалы IV межвуз. студ. науч. конф. – Москва, 2020. – С. 190–194.

Ровнейко Вера Владимировна,

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

СООТНОШЕНИЕ ПОНЯТИЙ «ПУБЛИЧНАЯ ДЕМОНСТРАЦИЯ» И «ПУБЛИЧНОЕ РАСПРОСТРАНЕНИЕ» ЗАПРЕЩЕННОЙ ИНФОРМАЦИИ ПО УГОЛОВНОМУ ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ

В условиях развития информатизации и информационных технологий уголовно-правовое воздействие, направленное на охрану от информации, приобретает все большее значение, поскольку и сама информация способна причинять вред законным интересам личности, общества и государства. Информация (ее целостность,

доступность или конфиденциальность) может являться не только предметом уголовно-правовой охраны, но и средством совершения преступлений. Исходя из содержания угроз информационной безопасности Российской Федерации, а также регулятивного законодательства, можно выделить два направления уголовно-правового воздействия:

– направленное на охрану информации;
– направленное на охрану **от** информации.

Существует достаточно обширный перечень запрещенной к распространению на территории Российской Федерации информации. Статьи 10 и 15^1 Федерального закона «Об информации, информационных технологиях и защите информации» устанавливают запрет «на распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность». Уголовно-правовые запреты, установленные для обеспечения соблюдения правил, установленных регулятивным законодательством, при использовании в конструкции составов преступлений одних и тех же понятий, должны исходить и из общего содержания этих понятий.

В Едином реестре запрещенной информации, который размещен на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)[89], содержится перечень (не исчерпывающий) видов такой информации (запрещенной к распространению на территории Российской Федерации):

– **порнография;**
– суицидальный контент;
– пронаркотический контент;
– незаконные азартные онлайн-игры;
– незаконная продажа лекарственных препаратов;

[89] Единый реестр запрещенной информации // Режим доступа: https://rkn.gov.ru/activity/electronic-communications/eais/

– незаконная продажа оружия, взрывчатых веществ, взрывных устройств и способы их изготовления;

– информация, вовлекающая несовершеннолетних в противоправную деятельность;

– незаконная продажа алкогольной продукции в сети «Интернет»;

– информация о пострадавших в результате противоправных действий несовершеннолетних;

– ЛГБТ, педофилия и смена пола;

– клевета и оскорбление;

– средства обхода блокировок[90].

В УК РФ с момента его принятия в 1996 году содержатся составы преступлений, в которых установлена ответственность за распространение «вредной» информации, например сведений, предметов и материалов, имеющих определенное негативное информационное содержание (например: клевета, распространение порнографических материалов и предметов).

Перечень таких запретов постоянно расширяется. Запрет на публичное распространение ложной информации (так называемых «фейков»), например, введен в УК РФ:

– в 2020 году – ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан», и ст. 207.2 УК РФ «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия»;

– в 2022 году – ст. 207.3 УК РФ «Публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий, оказании добровольческими формированиями, организациями или лицами содействия

[90] Пресечение распространения противоправной информации // Роскомнадзор. Режим доступа: https://rkn.gov.ru/activity/electronic-communications/p1568/

в выполнении задач, возложенных на Вооруженные Силы Российской Федерации или войска национальной гвардии Российской Федерации»[91].

К публичному распространению информации могут быть отнесены и другие составы преступлений, например ст. 205.2 УК РФ «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма», т.к. «под пропагандой терроризма понимается **деятельность по распространению** материалов и (или) информации, направленных на формирование у лица идеологии терроризма, убежденности в ее привлекательности либо представления о допустимости осуществления террористической деятельности»[92].

Уголовное законодательство, таким образом, разграничивает понятия «распространение» и «публичное распространение» какой-либо информации. Согласно разъяснениям Пленума Верховного Суда РФ, например, «под распространением сведений, порочащих честь и достоинство граждан или деловую репутацию граждан и юридических лиц, следует понимать опубликование таких сведений <…> или сообщение в той или иной, в том числе устной, форме хотя бы одному лицу»[93]. Т.е., распространение – не обязательно

---

[91] Методическое письмо «Об особенностях комплексных психолого-лингвистических судебных экспертиз информационных материалов, связанных с публичной дискредитацией использования Вооруженных Сил Российской Федерации» (утв. ФБУ РФЦСЭ при Минюсте России, протокол от 17.06.2022 № 2). URL: https://sudact.ru/law/metodicheskoe-pismo-ob-osobennostiakh-kompleksnykh-psikhologo-lingvisticheskikh-sudebnykh/; Методическое письмо "Об особенностях судебных лингвистических экспертиз информационных материалов, связанных с публичным распространением под видом достоверных сообщений заведомо ложной (недостоверной) информации". URL: https://ceur.ru/library/docs/departmental_regulations/metodicheskoe-pismo-ob-osobennostyax-sudebnyx-lingvisticheskix-ekspertiz-informaczionnyx-materialov-svyazannyx-s-publichnym-rasprostraneniem-pod-vidom-dostovernyx-soobshhenij-zavedomo-lozhnoj-nedostovernoj-informaczii/

[92] Примечание 1.1 к ст. 205.2 УК РФ (введен Федеральным законом от 29.12.2017 № 445-ФЗ).

[93] П. 7 постановления Пленума Верховного Суда РФ от 24.02.2005 № 3 "О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц".

должно быть публичным. Такое разъяснение противоречит регулятивному законодательству. Согласно положениям Федерального закона, «распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц»[94]. Исходя из нормативного определения понятия «распространение информации», оно не может быть не публичным, т.к. всегда направлено на получение информации неопределенным кругом лиц. Этим распространение информации отличается от предоставления, т.к. предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц[95].

Понятие «неопределенный круг лиц» в уголовном праве является оценочным, в уголовном законе его содержание не раскрывается: «Вопрос о публичности призывов к осуществлению террористической деятельности или оправдания терроризма (ст. 205.2 УК РФ) должен разрешаться судами с учетом места, способа, обстановки и других обстоятельств дела (например, обращения к группе людей в общественных местах, на собраниях, митингах, демонстрациях, распространение листовок, вывешивание плакатов, распространение обращений путем массовой рассылки сообщений абонентам мобильной связи и т.п.)»[96]. По мнению практикующих юристов, «согласно судебной практике, вся информация, размещенная в Интернете, имеет свойство публичности»[97].

---

[94] Ст. 2 Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.10.2024).

[95] Ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.10.2024).

[96] П. 19 постановления Пленума Верховного Суда РФ от 09.02.2012 № 1 (ред. от 03.11.2016) "О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности".

[97] Андрей Егупец. Как отличить фейк от дискредитации. URL: https://www.kommersant.ru/doc/5951659

Понятие «неопределенный круг лиц» является и межотраслевым. Оно связано с защитой интересов неопределенного круга лиц, которая имеет место не только в уголовном праве (например, ст. 242 УК РФ – преступление против общественной нравственности, т.к. посягает на интересы неопределенного круга лиц), но и в гражданском, и в административном. Для определения его содержания можно обратиться, например, к судебной практике по гражданским и административным делам. Так, в Обзоре судебной практики Верховного Суда Российской Федерации разъясняется, что «под неопределенным кругом лиц понимается такой круг лиц, который невозможно индивидуализировать (определить), привлечь в процесс в качестве истцов, указать в решении, а также решить вопрос о правах и обязанностях каждого из них при разрешении дела»[98]. Кроме того, понятие неопределенного круга лиц активно используется в правоприменительной и судебной практике в рамках Федерального закона от 13.03.2006 № 38-ФЗ «О рекламе» и Закона Российской Федерации от 07.02.1992 № 2300-1 «О защите прав потребителей». Анализ указанных источников показывает, что основным условием для применения понятия «неопределенный круг лиц» является невозможность индивидуализировать (определить) лиц, чьи права и интересы затронуты или могут быть затронуты рассматриваемыми действиями в определенный момент. При этом невозможность индивидуализации лиц характеризуется отсутствием общих для данных лиц критериев, позволяющих ограничить (определить) закрытость круга лиц и вероятностью изменения состава данных лиц во времени и пространстве.

В постановлении Пленума Верховного Суда РФ это противоречие между регулятивным законодательством и практикой применения уголовного закона было частично устранено и дано расширительное толкование понятиям «распространение» и «публичность»:

[98] Обзор судебной практики Верховного Суда Российской Федерации за первый квартал 2004 г. // Бюллетень Верховного Суда Российской Федерации. 2004. № 11. С. 27.

«Под распространением порнографических материалов понимается незаконное **предоставление конкретным лицам либо неопределенному кругу лиц** возможности их использования»[99]. Но теперь возникает вопрос об отграничении распространения информации от ее предоставления. Такое разъяснение опять не соответствует регулятивному законодательству.

В УК РФ в некоторых составах преступлений используется еще одно понятие – «публичная демонстрация (демонстрирование)» (например, в ст. 242 УК РФ – порнографических материалов, в ст. 282.4 УК РФ – нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами), которое не имеет нормативного определения в регулятивном законодательства, и определение его содержания вызывает некоторые проблемы, т.к. возникает вопрос о необходимости и критериях отграничения «публичной демонстрации» от «публичного распространения информации».

Изменения, которые были внесены в УК РФ Федеральным законом от 08.08.2024 № 218-ФЗ[100], расширили сферу применения уголовного закона для противодействия распространению в информационном пространстве деструктивного контента в виде трешстримов[101]. Суть изменений заключается в том, что в некоторые

---

[99] П. 23 постановления Пленума Верховного Суда РФ 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". URL: https://www.consultant.ru/document/cons_doc_LAW_434573/

[100] О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 08.08.2024 № 218-ФЗ.

[101] О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления ответственности за совершение преступлений с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)) : пояснительная записка к законопроекту № 506240-8. URL: https://sozd.duma.gov.ru/bill/506240-8

статьи Особенной части УК РФ, устанавливающие уголовную ответственность за преступления против личности (например: убийство, умышленное причинение вреда здоровью различной степени тяжести, побои, истязание) был введен дополнительный квалифицирующий признак «с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть "Интернет")»[102]. Таким образом, можно сказать, что демонстрация представляет собой разновидность распространения информации, но логично предположить, что форма информации – невербальная (изображения, видеозапись, предмет и т.п.).

В постановлении Пленума Верховного Суда РФ имеются разъяснения о содержании понятия «публичная демонстрация» в отношении порнографических материалов: «Публичная демонстрация с использованием электронных или информационно-телекоммуникационных сетей заключается в **открытом показе порнографических материалов либо в предоставлении неограниченному числу лиц возможности просмотра таких материалов.** Как публичная демонстрация подлежат квалификации действия, совершенные в прямом эфире (в частности на сайтах, позволяющих пользователям производить потоковое вещание, – стриминговых сервисах), а также состоящие в размещении запрещенной законом информации (материалов, сведений) на личных страницах и на страницах групп пользователей (в социальных сетях или на интернет-страницах)»[103]. Т.е. речь идет все о том же распространении информации, которое, в соответствии с нормативным определением,

[102] О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 08.08.2024 № 218-ФЗ.

[103] П. 23 постановления Пленума Верховного Суда РФ 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". URL: https://www.consultant.ru/document/cons_doc_LAW_434573/

содержащимся в регулятивном законодательстве, во-первых, не бывает не публичным, а во-вторых, всегда рассчитано на неопределенно широкий круг лиц. В редких случаях – можно использовать понятие «предоставление информации», рассчитанное на ее получение определенным кругом лиц.

Следует согласиться с авторами, которые считают, что «в целях повышения эффективности правового регулирования правоохранительных отношений и предупреждения преступности в информационной сфере представляется необходимым обеспечить законодательную унификацию рассматриваемого признака с учетом положений действующего регулятивного законодательства, в том числе Федерального закона «Об информации, информатизации и защите информации»[104].

Разнообразие терминологии для обозначения тождественных по содержанию понятий не вызывается целесообразностью и иногда противоречит принципу формальной определенности уголовно-правового запрета[105]. Уголовно-правовое воздействие, направленное на охрану от информации, распространение которой запрещено на территории Российской Федерации. Необходимость учета содержания регулятивного законодательства при установлении преступности

---

[104] Лобач Д.В. Развитие российского уголовного законодательства в сфере противодействия преступлениям, совершаемым в сети «Интернет» // Уголовное право: стратегия развития в XXI веке. 2023. № 3. Москва : Издательство «Проспект», 2023. С. 21–27 (С. 27).

[105] «Особую значимость требования определенности, ясности, недвусмысленности правовых норм и **их согласованности в системе общего правового регулирования** приобретают применительно к уголовному законодательству, являющемуся по своей правовой природе крайним (исключительным) средством, с помощью которого государство реагирует на факты противоправного поведения в целях охраны общественных отношений, если она не может быть обеспечена должным образом только с помощью правовых норм иной отраслевой принадлежности» – постановление Конституционного Суда РФ от 27.05.2008 № 8-П "По делу о проверке конституционности положения части первой статьи 188 Уголовного кодекса Российской Федерации в связи с жалобой гражданки М.А. Асламазян".

деяний – преступлений в сфере информационных технологий – обусловлена и необходимостью системного подхода, и межотраслевой согласованности для противодействия им.

Отсутствие учета системности в определении основных правовых понятий в сфере противодействия преступлениям в области информационных технологий (киберпреступлениям) возможно не так явно мешает эффективному противодействию этому виду преступлений, т.к. сложность противодействия этим преступлениям носит не только правовой, но и технический, и организационный характер. Например, проблемой, связанной с противодействием преступлениям в сфере компьютерной информации, является их анонимность. На этот аспект обращено внимание и в Стратегии национальной безопасности РФ[106]. Некоторые авторы в связи с этим предлагают ликвидировать возможность анонимного пользования публичным информационным пространством[107]. Но технические средства для реализации этого предложения ограничены. Правоприменители сталкиваются с проблемами идентификации личности преступника при совершении киберпреступлений, хотя способы идентификации устройств, с помощью которых совершаются такие преступления, установления приемов и методов их совершения и определения места совершения успешно применяются. В связи с этим «уголовно-правовой фетишизм» (т.е. переоценка права, преувеличение его реальных возможностей в регулировании общественных отношений), особенно в отношении киберпреступлений, неуместен. Обеспечение информационной безопасности предполагает системный характер, и правовые нормы (в том числе уголовно-правовые) имеют в этом случае большое значение.

---

[106] П. 54 Указа Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации".

[107] Габеев С.В. Проблемы реализации уголовной политики в отношении преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Уголовное право: стратегия развития в XXI веке. 2023. № 3. Москва : Издательство «Проспект», 2023. С. 28–38 (С. 37).

Библиографический список

1. Андрей Егупец. Как отличить фейк от дискредитации. – URL: https://www.kommersant.ru/doc/5951659

2. Габеев С.В. Проблемы реализации уголовной политики в отношении преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – Москва : Издательство «Проспект», 2023. – 272 с.

3. Лобач Д.В. Развитие российского уголовного законодательства в сфере противодействия преступлениям, совершаемым в сети «Интернет» // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – Москва : Издательство «Проспект», 2023. – 272 с.

Липинский Александр Павлович,

канд. юрид. наук, преподаватель кафедры публичного и частного права факультета (командного) Военной ордена Жукова академии войск национальной гвардии Российской Федерации,
г. Санкт-Петербург

ПРЕДУПРЕЖДЕНИЕ О НЕДОПУСТИМОСТИ РАЗГЛАШЕНИЯ ДАННЫХ ДОСУДЕБНОГО ПРОИЗВОДСТВА ПО УГОЛОВНЫМ ДЕЛАМ КАК СПОСОБ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Развитие информационных технологий все более приводит к их использованию в уголовном судопроизводстве, при этом возникают вопросы, связанные с обеспечением сохранения информации, которая вовлекается в судопроизводство с их применением. От сохранения информации зависит и качество расследования преступления,

а также безопасность личности[108], вовлекаемой в производство по уголовным делам, при этом однозначного подхода к обеспечению недопустимости разглашения данных в уголовном судопроизводстве не разработано.

В ходе досудебного производства использование информационных технологий при получении информации осуществляется следователем, дознавателем с привлечением не только специалистов к участию в следственном или ином процессуальном действии, но и сотрудниками различных организаций, компаний, связанных с получением, передачей информации, выполнением различного вида технических работ. Указанные сотрудники не являются представителями правоохранительных органов, их доступ к информации обусловлен выполнением ими непосредственных задач, решаемых по основному месту работы, однако в силу выполнения своих компетенций они становятся обладателями сведений, которые могут иметь доказательственное значение по уголовному делу, распространение которых может быть использовано в целях противостояния процессу расследования преступления, в связи с чем возникает необходимость обеспечения недопустимости разглашения полученной информации лицами, получающими ее в силу выполнения ими своей работы, или в процессе привлечения к участию в следственных или иных процессуальных действиях.

Законодатель в ст. 161 УПК РФ предусмотрел право следователя разъяснять лицам, вовлеченным в производство по уголовному делу, недопустимость разглашения данных предварительного расследования, предупреждая их об ответственности по ст. 310 УК РФ за разглашение указанной информации. При этом законодатель

[108] См.: Семенцов В.А. Публично-правовой механизм обеспечения безопасности личности в цифровом пространстве // Юридический вестник Кубанского государственного университета. 2022. № 1. С. 15–21; Гацолаева А.Х., Лолаева А.С. Понятие и сущность права личности на информационную безопасность // Право и государство: теория и практика. 2023. № 11 (227). С. 145–148; Андреева Т.Д. Публично-правовой механизм обеспечения безопасности личности // Алтайский юридический вестник. 2024. № 4 (44). С. 49–53 и др.

не определил перечень лиц, которые могут быть предупреждены о недопустимости разглашения указанных данных, отдав решение данного вопроса на усмотрение следователя, однако в ч. 3 ст. 161 УПК РФ отметил, что предупреждению подлежат участники уголовного судопроизводства[109]. Исходя из структуры УПК РФ, к ним относятся лица, указанные в гл. 5–8 УПК РФ, остальные лица, участие которых предусмотрено при производстве следственных и иных процессуальных действий, не рассматриваются в качестве участников, что вызывает определенные вопросы, так как при одновременном участии двух лиц в следственном действии один рассматривается как участник, другой – нет.

Законодатель в п. 58 ст. 5 УПК РФ указал, что «участники уголовного судопроизводства – лица, принимающие участие в уголовном процессе». Возникает вопрос о лицах, которые не перечислены в гл. 5–8 УПК РФ, но привлекаются к участию в производстве ряда следственных или иных процессуальных действий.

В частности, при допросе несовершеннолетнего свидетеля с участием переводчика и психолога, переводчик является участником и его можно предупреждать о недопустимости разглашения данных досудебного производства, а психолог не отнесен к числу участников, следовательно, его нельзя предупреждать о недопустимости разглашения данных досудебного производства. Приравнять психолога к специалисту как участнику процесса нельзя, поскольку цели их участия являются различными[110]. Аналогичная ситуация возникает при привлечении иных лиц в качестве статистов при опознании, следственном эксперименте и т.д.

---

[109] См.: Липинский А.П. Доступ участников уголовного судопроизводства к материалам уголовного дела в досудебном производстве в контексте обеспечения тайны частной жизни // Вестник Удмуртского университета. Серия «Экономика и право». 2021 Т. 31, вып. 1. С. 148–153; Он же. Участники, подлежащие предупреждению о недопустимости разглашения данных // Вестник Удмуртского университета. Серия «Экономика и право». 2022 Т. 32, вып. 5. С. 911–919.

[110] См.: Гришина Е.П. Концептуальные и правовые проблемы участия специалиста в состязательном уголовном судопроизводстве : монография. М. : «Юрлитинформ», 2015. С. 204 и др.

Лица, привлеченные к участию в уголовном процессе, но не наделенные статусом его участника, в отличие от последнего не обладают совокупностью процессуальных прав и обязанностей и не связаны с исследуемым событием. Их привлечение к участию в следственных действиях обусловлено их незаинтересованностью в исследуемом событии, необходимостью обеспечения прав и свобод лица, в отношении которого проводится следственное действие, поэтому приравнивать указанных лиц к участникам представляется нецелесообразным. Указанные лица принимают участие при производстве по уголовному делу, привлекаясь для решения отдельных задач, но участниками уголовного процесса не являются. Обладая информацией, полученной в результате участия в следственных и иных процессуальных действиях, они представляют интерес для лиц, которые желают оказать противодействие процессу расследования, в том числе путем привлечения лиц, принимавших участие в следственных действиях, для дачи показаний о их проведении в целях поставления под сомнение полученные результаты, что может изменить систему доказательств и привести к признанию ряда из них недопустимыми.

Представляется в целях обеспечения сохранения информации, полученной в ходе досудебного производства, целесообразным предусмотреть возможность предупреждения любого лица о недопустимости разглашения данных досудебного производства, который был привлечен к участию в следственном или процессуальном действии, соответственно, указанное положение должно быть установлено в ст. 161 УПК РФ.

При проведении следственных и иных процессуальных действий с использованием различных технических средств, лица, которые будут обеспечивать их применение либо которые передают полученную информацию на бумажных или электронных носителях в силу выполнения своих обязанностей, не могут в рамках уголовного дела быть все предупреждены о недопустимости разглашения данных досудебного производства, поскольку сложно определить состав лиц, которые будут выполнять определенные технические

работы. В связи с чем полагаю, что лица, имеющие допуск для выполнения работ, связанных с использованием информационных технологий при производстве по уголовным делам, должны быть изначально предупреждены по ст. 310 УК РФ об ответственности за разглашение данных досудебного производства и им должны быть разъяснены положения ст. 144 и 161 УПК РФ, только после этого они могут быть допущены до получения информации по уголовным делам. В случае распространения ими полученной информации должен решаться вопрос о привлечении к уголовной ответственности лица ее разгласившего. Поскольку допуск указанных лиц к выполнению своих профессиональных обязанностей будет возможен только после разъяснения им необходимости соблюдения правила о недопустимости разглашения полученной информации, они будут предупреждены о наступлении возможной ответственности за нарушение данного правила, то предупреждать дополнительно по каждому проводимому мероприятию представляется нецелесообразным.

Разглашение информации, полученной в досудебном производстве может негативно повлиять на процесс установления фактических обстоятельств совершения преступления посредством оказания воздействия на свидетелей, потерпевших, понятых, специалистов и др. в целях изменения ими данных ранее показаний. В связи с чем предупреждение о недопустимости разглашения данных является основным способом воздействия на участников и участвующих в деле лиц в целях сохранения ими первоначальной информации и недопустимости ее изменения.

Татьянин Дмитрий Владимирович,

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

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ ИСПОЛЬЗОВАНИИ ВИДЕО-КОНФЕРЕНЦ-СВЯЗИ

Одним из наиболее дискуссионных является вопрос о возможности использования видео-конференц-связи в процессе производства следственных действий при производстве предварительного расследования по уголовным делам. О целесообразности использования информационных технологий при производстве следственных действий указывают многие авторы[111], отмечая, что подобный подход обеспечит соблюдение разумного срока, позволит более качественно и эффективно осуществлять расследование, своевременно без лишних человеческих и ресурсных затрат проводить следственные действия. Соглашаясь с возможностью и целесообразностью

[111] См.: Семенцив В.А., Глимейда В.В. Особенности использования технических средств и технологий при производстве следственных действий : монография. М. : Юрлитинформ, 2025; Кочнев М.Е., Шестакова Л.А. Использование системы видео-конференц-связи при производстве следственных действий (ст. 189.1 УПК РФ): уголовно-процессуальный и криминалистический аспекты // Вестник Международного института рынка. 2023. № 2. С. 110–114; Гаас Н.Н. Использование видео-конференц-связи при производстве следственных действий в стадии предварительного расследования: изменения, в которых нуждается практика // Российский следователь. 2021. № 12. С. 11–15; Щерба С.П., Архипова Е.А. Правовые основы применения видеоконференцсвязи в уголовном судопроизводстве России и перспективы их совершенствования // Уголовное право. 2014. № 4. С. 109–117 и др.

использования информационных технологий при производстве следственных действий, следует отметить, что данный вопрос не является бесспорным, поскольку связан с проблемой не просто проведения следственного действия, но и сохранения получаемой в его процессе информации.

Одним из наиболее проблемных вопросов является проведение следственных действий с использованием видео-конференц-связи. Законодатель, введя Федеральным законом от 30.12.2021 № 501-ФЗ[112] статью 189.1 УПК РФ, регулирующую порядок производства следственных действий с использованием видео-конференц-связи (далее – ВКС), предусмотрел возможность производства в указанном формате только трех следственных действий: допроса, очной ставки и опознания, при этом он не указал о том, по чьей инициативе должен решаться вопрос о проведении указанных действий в указанном формате. Может ли лицо, которое пригласили к участию в следственном действии с использованием ВКС, отказаться от указанного формата, какие последствия может повлечь подобный отказ. Законодатель установил только два случая недопустимости применения ВКС, когда возникает возможность разглашения информации, связанной с государственной или иной охраняемой федеральным законом тайной, либо в отношении лица, к которому применены меры государственной защиты. В остальных случаях законодатель не усмотрел возможности отказа от применения ВКС. Отсутствуют в УПК РФ основания для применения ВКС при производстве следственных действий, что позволяет предполагать, что решение данного вопроса отдается на усмотрение следователя. Полагаю, что для применения ВКС при производстве следственных действий должно осуществляться при наличии веских оснований, практически исключающих возможность проведения следственных действий в иных условиях. В частности, производство допроса свидетеля, потерпевшего, специалиста или эксперта

[112] О внесении изменений в Уголовно-процессуальный кодекс России: Федеральный закон РФ от 30.12.2021 № 501-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_405493

с использованием ВКС может иметь смысл, когда указанные лица находятся в другом регионе, необходимость их приглашении для очного допроса неоднозначная, поскольку они могут дать полезную информацию, но могут не обладать ею, поручать допросить другому следователю в рамках выполнения отдельного поручения нецелесообразно, поскольку во время допроса может возникнуть необходимость уточнения определенных данных, о чем следователь, не владеющей информацией по уголовному делу, не может знать и необходимые сведения просто не будут получены, что может отразиться на процессе доказывания. Для исключения бессмысленного вызова на допрос для выяснения обладания/необладания лицом определенной информации представляется обоснованным использования в указанных ситуациях ВКС при допросе. В отношении обвиняемого и подозреваемого по уголовному делу использование ВКС представляется возможным только в двух случаях, во-первых, когда указанное лицо находится в тяжелом состоянии в больнице, что исключает возможность его транспортирования к месту допроса, например с травмой после дорожно-транспортного происшествия и т.п., либо в случае, когда указанное лицо находится за границей, отказывается прибыть в Россию, а в его выдаче отказано, при этом подозреваемый/обвиняемый идет на контакт со следствием и согласен давать показания, но в указанном случае следует урегулировать порядок допроса с учетом особенностей иностранного законодательства. В случае допроса подозреваемого/обвиняемого обязательно должен участвовать защитник, при этом защитник должен находиться вместе с подзащитным, если он не может присутствовать в месте нахождения подозреваемого/обвиняемого, то он должен принимать участие в месте нахождения следователя, а обвиняемому/подозреваемому должен быть представлен защитник по назначению, данный подход исключит возникновение различных инсинуаций в последующем.

Одним из наиболее дискуссионных является вопрос о проведении следственного действия с применением ВКС с участием несовершеннолетнего. Следует ли учитывать мнение самого несовершеннолетнего, его законного представителя, либо педагогического

работника, приглашенного к участию в следственном действии, если хотя бы один из них будет против, возможно ли использовать ВКС, особенно если против несовершеннолетнего, ведь для него в указанной ситуации участие будет против его воли в следственном действии, что предполагает воздействие на психику, если в последующем несовершеннолетний заявит о порабощении его воли при производстве следственного действия, то вряд ли его результат можно будет признать допустимым доказательством. Следует обратить внимание и на возраст несовершеннолетнего. Полагаю, что в отношении несовершеннолетних, не достигших возраста 14 лет, применение ВКС не должно применяться, так как несовершеннолетний в указанном возрасте не осознает полностью происходящего и не всегда правильно его оценивает. Использование ВКС при допросе несовершеннолетнего потерпевшего и свидетеля следует проводить при достижении им 14-летнего возраста и только с согласия несовершеннолетнего. Законный представитель и педагогический работник должны находиться вместе с несовершеннолетним, что позволит решить задачи, стоящие перед педагогическим работником. Аналогичные требования следует соблюдать и при проведении очной ставки с использованием ВКС.

В целях обеспечения сохранения информации, получаемой в процессе проведения следственного действия с участием ВКС до начала его производства следователь, ведущий допрос, должен разъяснить участникам следственного действия недопустимость разглашения данных досудебного производства и предупредить их об уголовной ответственности по ст. 310 УК РФ за разглашение данных предварительного расследования, о чем у всех участников следственного действия должна быть взята подписка. Мы разделяем позицию А.П. Липинского о необходимости предупреждения о недопустимости разглашения данных досудебного производства всех участников следственного действия[113], поскольку на момент произ-

[113] Липинский А.П. Обеспечение недопустимости разглашения данных досудебного производства : автореф. дис. … канд. юрид. наук. Ижевск, 2023. С. 12–13.

водства следственного действия однозначно невозможно быть уверенным в том, что все участники будут сохранять полученную информацию в тайне, если же информация будет разглашена, то это может привести к необратимым последствиям, связанным с утратой доказательств. Полагаем, что предложенный порядок производства следственных действий с применением ВКС обеспечит сохранение полученной информации.

Туров Сергей Юрьевич,

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

СОВРЕМЕННЫЙ АНАЛИЗ ПРИМЕНЕНИЯ КОММУНИКАТИВНЫХ ТЕХНОЛОГИЙ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Цифровизация, включая использование новых программ, дистанционных технологий, Интернета и искусственного интеллекта, оказывает огромное влияние на современное общество. Благодаря своей способности быстро собирать, обрабатывать и хранить информацию, а также снижать трудоёмкость и стоимость операций, цифровые инновации закономерно внедряются в систему государственного управления и особенно в судебно-правоохранительную сферу.

В целях повышения эффективности, качества и открытости уголовного судопроизводства для граждан представляется необходимым внедрение прогрессивных информационно-коммуникационных систем, обеспечивающих удобный и оперативный доступ к информации, организацию взаимодействия и обмена данными в цифровом формате, а также автоматизацию процедур принятия

процессуальных решений. В связи с этим необходимо проанализировать сущность информационно-коммуникационных технологий в уголовном судопроизводстве. Наиболее передовой технологией, допускаемой российским уголовно-процессуальным законодательством, является видео-конференц-связь (далее – ВКС). Применительно к судебному разбирательству ВКС определяется как предусмотренный процессуальными нормами способ проведения судебных действий с использованием технических средств для передачи аудио- и видеоинформации по каналам связи между удалёнными участниками процесса[114].

Популярность ВКС, обусловленная ее доступностью, простотой использования и удобством для всех категорий граждан, включая людей с нарушениями слуха и зрения, привела к расширению ее применения в уголовном процессе. Пандемия COVID-19, разразившаяся в 2020 году, стала решающим фактором, ускорившим процесс приведения Уголовно-процессуального кодекса РФ (далее – УПК РФ) в соответствие с новыми реалиями и потребностями общества.

Анализ законодательных изменений, касающихся ВКС в уголовном процессе, выявляет не только несогласованность, но и явные признаки непоследовательности, что наглядно демонстрируется даже различиями в орфографическом написании самого термина, обозначающего эту технологию[115].

Недостаточная проработка норм, регулирующих ВКС, объясняется, на наш взгляд, пренебрежением правилами юридической техники и принятием законов под влиянием текущей ситуации,

---

[114] См.: п. 1.5 Регламента организации применения видео-конференц-связи при подготовке и проведении судебных заседаний, утв. приказом Судебного департамента при Верховном Суде РФ от 28 декабря 2015 г. № 401 (ред. от 30 декабря 2020 г.). Здесь и далее, если не оговорено иное, ссылка сделана на источники (нормативные и научные, а также на судебные решения), опубликованные в СПС «КонсультантПлюс».

[115] Например, в ч. 2 ст. 401.13, чч. 2, 2.1 ст. 399, ч. 2 ст. 389.12, ч. 8 ст. 389.13 УК РФ, используется вариант написания – «видеоконференц-связь», а в ст. 278.1, ч. 3 ст. 258, ст. 241.1, ч. 4 ст. 240, ч. 4 ст. 108 УПК РФ – «видео-конференц-связь».

без учёта перспектив развития общества. Такая недальновидность, тормозящая необходимые изменения в законодательстве, не всегда может быть оправдана нехваткой средств. Примером удачного решения является недавнее введение законодателем в УПК РФ норм, предоставляющих право выбора использования ВКС «при наличии технической возможности»[116].

Несмотря на умеренный оптимизм, представляется маловероятным, что в обозримом будущем удастся полностью нивелировать риски, связанные с мутациями вирусов, существенно сократить расходы на конвоирование лиц, ограниченных в свободе в рамках уголовного судопроизводства, или исключить вероятность побега указанных лиц из-под стражи, а также полностью избежать глобальных чрезвычайных ситуаций и иных внешних угроз. Точно так же едва ли реально, что современная медицина сможет полностью излечить все физические и психические заболевания, препятствующие транспортировке лиц в судебное заседание, при отсутствии формальных противопоказаний к их участию в процессуальных действиях. Представляется невозможным международная изоляция российских правоохранительных органов и судебной системы, деятельность которых в сфере оказания взаимной правовой помощи по уголовным делам в современных условиях характеризуется укреплением и поступательным развитием.

Следует учитывать, что в юридической литературе высказываются сомнения относительно целесообразности применения ВКС и других новых технологий в уголовном процессе. Но эта критика, основанная на анализе сложности современного общества, помогает нам объективно оценить ситуацию и принять взвешенное решение.

Для совершенствования законодательства о ВКС в уголовном судопроизводстве необходимо проанализировать ранее принятые

---

[116] См.: ч. 1 ст. 189.1 УПК РФ «Особенности проведения допроса, очной ставки, опознания путем использования систем видео-конференц-связи», ч. 1 ст. 241.1 «Участие в судебном заседании путем использования систем видео-конференц-связи».

меры. В частности, в 2011 году были внесены изменения, направленные на сокращение сроков рассмотрения дел и устранение задержек, связанных с неявкой свидетелей. Эти изменения, внесённые Федеральным законом № 39-ФЗ[117], позволили проводить допросы свидетелей и потерпевших с использованием ВКС, что отразилось в статьях 277, 240 и 278.1 УПК РФ

Федеральным закон № 501-ФЗ от 30 декабря 2021 года[118], принятым через десять лет после предыдущих изменений, произведены значительные коррективы в порядок использования ВКС в уголовном процессе. Закон урегулировал применение ВКС в следственных действиях (ст. 189.1 УПК РФ), закрепил полномочия следователя (дознавателя) по организации участия в них необходимых лиц (ст. 38, 41 УПК РФ) и изменил порядок оформления протоколов (ст. 166 УПК РФ)

Однако обращает на себя внимание то, что статья 189.1 УПК РФ, регулирующая использование ВКС в следственных действиях, содержит ряд пробелов и нерешённых вопросов. В частности, в ней не определён порядок участия в следственных действиях по ВКС защитника, понятых, педагога, законного представителя, не согласован механизм установления личности. Не в полной мере регламентированы действия при применении мер безопасности, не решена проблема участия лиц с ограниченными возможностями и не урегулирована возможность проведения иных процессуальных действий по ВКС.

Не менее значимым недостатком закона от 30 декабря 2021 г. № 501-ФЗ следует признать отсутствие в нем корреспондирующих положений, регламентирующих возможность использования адвокатом ВКС при проведении опроса, предусмотренного ч. 3 ст. 86 УПК РФ. Указанная законодательная неполнота приводит к дисбалансу процессуальных возможностей сторон защиты и обвинения,

[117] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 20 марта 2011 г. № 39-ФЗ.

[118] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 30 декабря 2021 г. № 501-ФЗ.

ослабляя возможности защиты и усиливая позиции обвинения. Обозначенная позиция основывается на мнении Конституционного Суда РФ, согласно которому сведения, собранные стороной защиты в соответствии со ст. 86 УПК РФ, не могут признаваться недопустимыми, если при их получении не нарушались правовые нормы[119].

Внесённые в УПК РФ изменения Федеральным законом № 610-ФЗ от 29 декабря 2022 года[120] открыли новые возможности для применения ВКС в уголовном процессе. Теперь суд может избирать меру пресечения лицу по ВКС, если его присутствие невозможно; допускать участие подсудимого в судебном заседании по ВКС; обеспечивать безопасность участников процесса по тяжким преступлениям путём участия подсудимого в ВКС. Важно отметить высокую значимость изменений, внесенных этим законом в ч. 4 ст. 240 и ст. 278.1 УПК РФ, регламентирующих возможность проведения судом допросов и иных процессуальных действий с использованием ВКС. Существенным шагом в направлении совершенствования уголовного судопроизводства стало введение в действие статьи 474.1 УПК РФ, регламентирующей порядок использования электронных документов.

Позже, в 2024 году, Федеральным законом № 267-ФЗ[121] внесены дополнительные изменения в статьи 46, 47 и 49 УПК РФ, позволяющие подозреваемым и обвиняемым, находящимся под стражей, общаться со своими защитниками по ВКС.

В то время как нововведения, касающиеся применения ВКС, призваны улучшить судопроизводство, они противоречат порядку, установленному для апелляционной инстанции. Хотя апелляционное производство подчиняется общим правилам, в нем есть существенные

---

[119] Об отказе в принятии к рассмотрению жалобы гражданина Прохорова Ф.Г. на нарушение его конституционных прав пунктом 3 части второй статьи 75 УПК РФ : определение Конституционного Суда РФ от 27 февраля 2018 г. № 263-О.

[120] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 29 декабря 2022 г. № 610-ФЗ.

[121] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 8 августа 2024 г. № 267-ФЗ.

исключения: суд может исследовать любые доказательства с помощью ВКС и самостоятельно решать вопрос об участии осужденного в заседании по ВКС, не учитывая его волеизъявление, категорию преступления или ходатайства других участников процесса.

Отдельного внимания заслуживают недостатки, присущие производству в суде надзорной инстанции. Статья 412.10 УПК РФ не содержит положений, наделяющих осужденного или оправданного правом ходатайствовать об участии в судебном заседании суда надзорной инстанции по ВКС. Отсутствует регламентация вопроса об участии в заседании суда надзорной инстанции с использованием ВКС иных заинтересованных лиц, включая адвоката.

Обобщая вышесказанное, можно сделать вывод, что в суде первой инстанции принципы устности, непосредственности и права на защиту реализуются в большей степени, чем в апелляционном и надзорном суде, где их реализация ограничена особенностями процедуры и возможностями использования ВКС.

Описанные проблемы наглядно демонстрируют острую необходимость в четкой и согласованной регламентации использования ВКС в уголовном судопроизводстве. Разработка правил применения цифровых технологий должна основываться на неукоснительном соблюдении принципов: защиты конституционных прав и свобод граждан, обеспечения безопасности, прозрачности и открытости судопроизводства, равноправия и состязательности сторон.

Процесс глобализации приводит к имплементации норм международного права в российское законодательство, что требует активной работы по адаптации информационных технологий в уголовном процессе. В качестве иллюстрации можно привести пример из Колумбии, где в феврале 2023 года суд провёл судебное заседание в метавселенной[122], используя аватары для представления участников. Это свидетельствует о новых возможностях виртуальной коммуникации в судопроизводстве.

[122] Разработчик метавселенной компания Meta признана судом экстремистской организацией и ее деятельность запрещена в РФ – прим. автора.

Вместе с тем масштабная рационализация юридической деятельности, особенно в сфере уголовного судопроизводства, посредством внедрения автоматизированных информационных систем должна осуществляться с учетом потенциальных рисков и угроз. Поэтому крайне значимо внедрять механизмы мониторинга и нейтрализации потенциальных или реальных угроз информационной безопасности, направленных против объектов информатизации, которые могут повлечь за собой искажение, утрату или несанкционированное раскрытие информации.

Хомяков Эдуард Геннадьевич,

канд. юрид. наук, доцент, доцент кафедры уголовного процесса и криминалистики ИПСУБ ФГБОУ ВО «Удмуртский государственный университет»,

Русских Жанна Александровна,

преподаватель кафедры информационной безопасности в управлении ИПСУБ ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

О ТЕРМИНЕ «ФОРЕНЗИКА» И ЦИФРОВОЙ КРИМИНАЛИСТИКЕ

Современные методы расследования преступлений все чаще обращаются к технологическим инновациям, среди которых особое место занимают форензика и цифровая криминалистика. Хотя эти термины часто используются как взаимозаменяемые, между ними существуют значительные различия, которые важно понимать для правильного их применения в профессиональной деятельности.

Термин «форензика» происходит от английского слова «forensics», которое само восходит к латинскому корню «forensis», означающему «публичный», «присущий форуму» или «связанный с судебным разбирательством» («foren» в переводе с латинского буквально означает «речь перед форумом» или «выступление перед судом»).

В современных англоязычных странах термин «forensics» в основном используется для обозначения широкого спектра научных методов и технологий, применяемых для обнаружения и расследования преступлений, включая различные направления судебной экспертизы. Этот термин охватывает широкий спектр дисциплин, включая в том числе судебную медицину, криминалистику, отдельные направления судебной экспертизы[123]; при этом криминалистику не в российском, а собственном понимании.

Необходимо отметить, что термин «forensic» обычно используется как прилагательное, описывающее что-либо, связанное с судебными разбирательствами или криминалистикой. Например, «forensic evidence» (судебные доказательства) или «forensic science» (судебная наука). Это слово указывает на связь с судом или расследованием.

Термин «forensics», с другой стороны, чаще используется как существительное, обозначая саму науку или методы исследования, применяемые в правовой или криминалистической сфере. Например, «the application of forensics» (применение криминалистических методов).

В некоторых случаях «forensics» может быть сокращением от «forensic science» и использоваться для обозначения этой области знаний в целом.

Понятие «forensic science», что буквально означает «судебная наука», охватывает научные методы и техники, которые используются для обнаружения, исследования и предъявления доказательств в ходе судебных разбирательств. Это междисциплинарная область, которая объединяет знания из различных наук, таких как биология,

[123] Forensic science. URL: https://en.m.wikipedia.org/wiki/Forensic_science (дата обращения: 21.04.2025).

химия, физика, информатика и других, необходимых в расследовании преступлений и правовых спорах. Основная цель этой науки – сбор и анализ объективных данных, которые могут быть использованы в суде в качестве доказательств.

Первые упоминания о применении научных методов в судебных разбирательствах относятся еще к XVII веку, однако современное понимание форензики как комплексной научной дисциплины за рубежом сформировалось в середине XX века благодаря развитию новых технологий и методов исследования[124].

В нашей стране термин «форензика» в настоящее время воспринимается в ином значении.

Например, С.А. Еремеева в своей работе отмечает, что «У понятия forensic пока, к сожалению, нет «понимающего» русского эквивалента»[125]; со ссылкой на Вайцмана (Weizman E.) она констатирует, что «английский язык только в XVII веке усвоил этот латинский термин в смысле «судебной экспертизы», но первоначальный смысл – относящееся к форуму или суду – присутствовал до начала XIX в., и только в середине века, во время бурного развития науки, термин forensic стал использоваться для конкретного обозначения юридически-научного расследования (т.е. криминалистики)»[126].

Н.Н. Федотов указывает на то, что «Русское «форензика» означает не всякую криминалистику, а именно компьютерную», дополнительно поясняя, что «Форензика оказалась почти не связанной с другими разделами криминалистики»[127].

---

[124] History and Development of Forensic Science. URL: https://www.sifs.in/ (дата обращения: 21.04.2025); History of Forensics. URL: https://forensicshistory.wordpress.com/ (дата обращения: 21.04.2025).

[125] Еремеева С.А. Новая история слова/новое слово в истории: forensic // Диалог со временем. 2022. № 78. С. 312. URL: https://roii.ru/dialogue/roii-dialogue-78.pdf#page=311 (дата обращения: 21.04.2025).

[126] Там же. С. 313.

[127] Федотов Н.Н. Форензика – компьютерная криминалистика. М. : Юридический Мир, 2007. С. 11.

А.А. Шелупанов и А.Р. Смолина в своей работе определяют форензику как «компьютерную криминалистику, расследование киберпреступлений – совокупность знаний о методах поиска, исследования и закрепления цифровых доказательств по киберпреступлениям»[128].

Помимо термина «форензика» в русском языке закрепился термин «форензик», вошедший в профессиональный оборот в России через практику международных аудиторских фирм[129]; это произошло ближе к началу XXI века. Форензик можно рассматривать как комплекс услуг, которые направлены на выявление корпоративного мошенничества, неправомерных действий сотрудников и коррупции в компании[130]. Н.А. Шкляева и М.А. Городилов, анализируя определения понятия «форензик», данные разными авторами, указывают на то, что «Форензик – это услуга, сочетающая в себе знания из различных областей: бухгалтерского учета, экономического анализа, аудита, финансов, криминалистики, информатики, программирования, психологии, права и других», и предлагают свое определение, согласно которому «форензик представляет собой независимую деятельность по анализу, урегулированию спорных ситуаций со значительными экономическими рисками, разработке процедур, направленных на противодействие всем видам финансового мошенничества и на обнаружение не соответствующих нормативным актам действий сотрудников или организаций, инициированную собственниками компании или советом директоров»[131].

---

[128] Шелупанов А.А., Смолина А.Р. Форензика. Теория и практика расследования киберпреступлений. М. : Горячая линия. Телеком, 2020. С. 4.

[129] Иванов Д. Расследование для бизнеса // Журнал «Коммерсантъ Секрет Фирмы». 01.10.2012. URL: https://www.kommersant.ru/doc/2020000 (дата обращения: 21.04.2025).

[130] Что такое форензик. Объясняем простыми словами. 19 сентября 2021. URL: https://finance.rambler.ru/business/47232550-chto-takoe-forenzik-obyasnyaem-prostymi-slovami/ (дата обращения: 21.04.2025).

[131] Шкляева Н.А., Городилов М.А. Форензик: понятие, особенности, история возникновения и развития новой услуги // Аудит. 2019. № 6. С. 16-21.

Компьютерная форензика начала формироваться в России как отдельное направление с развитием компьютерных технологий. Первые шаги в этой области были сделаны в середине 70-х годов XX века, когда появились первые ЭВМ (электронно-вычислительные машины), которые использовались для экономических расчетов и решения оборонных задач. Однако именно массовое распространение компьютеров и сетей в 90-х годах XX века, а также появление специализированных лабораторий и подразделений (государственных и частных), занимающихся изучением вопросов информационной безопасности и ее обеспечением, создало предпосылки для развития компьютерной форензики как самостоятельной дисциплины.

Еще несколько лет назад в классических учебниках (учебных пособиях) по криминалистике форензика как часть криминалистики или ее структурный элемент не рассматривалась, однако некоторые авторы, упоминая форензику в своих научных работах, называли ее компьютерной (иногда цифровой) криминалистикой и обозначали ее либо разделом (подразделом) криминалистики, либо разделом (отраслью) криминалистической техники. В отдельных научных работах форензику относили к области специальных знаний, связанных с компьютерной техникой и направленных на выявление инцидентов в области информационной безопасности (кибербезопасности).

При этом многие образовательные организации, предлагая подготовку специалистов в области информационной безопасности, специалистов по расследованию угроз информационной безопасности, специалистов по форензике (форензик-специалистов, форензик-аналитиков), включают в учебные программы (программы курсов) вопросы из области форензики (основ форензики)[132].

---

[132] Профессия Форензик (специалист по форензике): в чем ее суть, обязанности, обучение. URL: https://kedu.ru/press-center/profgid/professiya-forenzik-spetsialist-po-forenzike-v-chem-eye-sut-obyazannosti-obuchenie/ (дата обращения: 21.04.2025); Расследование хакерских инцидентов. Основы форензики. URL: https://www.specialist.ru/course/ceh3 (дата обращения: 21.04.2025); Специализации в информационной безопасности: как выбрать свое направление. URL: https://netology.ru/blog/napravleniya-informatsionnoy-bezopasnosti (дата обращения: 21.04.2025).

Также в России и за рубежом ежегодно проводятся научные (научно-практические) конференции и форумы, киберчемпионаты, посвященные форензике либо близкой ей тематике, например: ежегодная международная конференция Moscow Forensics Day, International Conference on Law and Digital Forensics (ICLDF) и другие.

Следует отметить, что в 2021 году как следствие цифровизации криминалистической деятельности появился учебник «Цифровая криминалистика» (под редакцией В.Б. Вехова, С.В. Зуева), в котором цифровая криминалистика была обозначена как «частная криминалистическая теория, которая представляет собой систему научных положений и разрабатываемых на их основе технических средств, приемов, методик и рекомендаций по обнаружению, фиксации, предварительному исследованию, использованию компьютерной информации и средств ее обработки в целях раскрытия, расследования и предупреждения преступлений»[133] (в учебнике 2025 года издания в данном определении указано – « …в целях борьбы с правонарушениями»[134]). Слово «форензика» в тексте указанного учебника не встречается.

При анализе предмета, объекта, системы и задач цифровой криминалистики[135] напрашивается вывод, что в России существует заметное разделение между сферами применения форензики и цифровой криминалистики, что связано как с особенностями законодательства, так и с практическими потребностями различных субъектов.

Форензика в России активно применяется в корпоративном секторе для проведения внутренних расследований инцидентов информационной безопасности, финансовых махинаций и других

---

[133] Цифровая криминалистика : учебник для вузов / под редакцией В.Б. Вехова, С.В. Зуева. Москва : Издательство Юрайт, 2021. С. 25. URL: https://urait.ru/bcode/477984 (дата обращения: 21.04.2025).

[134] Цифровая криминалистика: учебник для вузов / под редакцией В.Б. Вехова, С.В. Зуева. 2-е изд., перераб. и доп. Москва : Издательство Юрайт, 2025. 490 с. URL: https://urait.ru/bcode/568013 (дата обращения: 21.04.2025).

[135] Там же. С. 11–25.

нарушений. Основные задачи подобных расследований заключаются в выявлении источников утечек данных, анализе действий сотрудников и предотвращении мошенничества. Субъектами таких расследований обычно являются внутренние службы безопасности компаний, независимые эксперты или аудиторы, которые работают в рамках договорных отношений. Эти исследования редко выходят за рамки гражданского права, если только дело не передается в правоохранительные органы.

Цифровая криминалистика решает свои задачи в рамках уголовного судопроизводства для расследования преступлений, связанных с использованием современных технологий, либо сопровождающихся образованием цифровых следов.

В уголовном процессе субъектами применения знаний из области цифровой криминалистики являются правоохранительные органы Российской Федерации (МВД, ФСБ, Следственный комитет).

Разница в сферах применения обуславливает и различия в методологии.

Форензика в большей степени ориентирована на оперативность и минимизацию ущерба для бизнеса. Здесь важна скорость выявления проблемы и принятия мер для ее устранения.

Цифровая криминалистика требует строгого соблюдения процессуальных норм, чтобы собранные в процессе расследования доказательства могли быть признаны в суде. Это делает ее более формализованной и зависимой от законодательства.

Существуют и терминологические отличия. Например, термин «инцидент» в рамках форензики (особенно в корпоративной среде) обычно обозначает событие, нарушающее нормальную работу информационных систем или представляющее угрозу безопасности данных. При этом внутренние расследования часто начинаются с анализа инцидентов, таких как подозрительная активность сотрудников, утечка данных или несанкционированный доступ. Инцидент рассматривается как отправная точка для сбора доказательств и анализа событий.

Под «артефактом» в форензике понимаются следы, оставленные в ходе совершения инцидента. Это могут быть файлы, логи, временные записи или другие данные, которые помогают восстановить картину произошедшего. Например, артефакты включают удаленные файлы, метаданные, записи реестра операционной системы или данные из оперативной памяти. Эти данные используются для анализа действий нарушителя и определения масштаба ущерба.

В цифровой криминалистике термины «инцидент» и «артефакт» практически не применяются, но если такое происходит, то их содержание может быть иным, адаптированным для уголовного процесса.

В цифровой криминалистике инцидент чаще связан с преступлениями, требующими расследования в рамках уголовного права. Инцидент рассматривается как событие, имеющее признаки преступления, что требует его фиксации (документирования), поиска и изъятия соответствующих следов (следов цифровых), их исследования (анализа) в рамках соответствующей судебной экспертизы (как правило, компьютерно-технической) для придания им статуса доказательств и последующего представления в суде.

В цифровой криминалистике аналогами артефактов можно считать цифровые следы, которые характеризуются как вещественные доказательства в уголовном процессе.

Во многих странах, например: в США, Канаде, Великобритании, отдельных странах Европы и Азии, границы между форензикой и цифровой криминалистикой (в российском понимании) менее выражены. Например, частные компании могут активно сотрудничать с правоохранительными органами, передавая данные, полученные в ходе внутренних расследований, для использования в уголовном процессе. В России такое взаимодействие пока менее развито.

В заключение следует отметить, что с появлением цифровой криминалистики и активной цифровизацией криминалистики и в теории, и на практике возникает необходимость отказаться от использования термина «форензика» в области криминалистической деятельности и уголовном судопроизводстве.

Рыскали Акжол Думанулы,

обучающийся 2 курса ОП «Вычислительная техника и информационные системы», Западно-Казахстанский инновационно-технологический университет;

Шынтемир Индира Бауржанкызы,

магистр техн. наук, старший преподаватель Западно-Казахстанского инновационно-технологического университета, Республика Казахстан, г. Уральск

БУДУЩЕЕ ОБРАЗОВАНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОТ ТЕОРИИ К ПРАКТИКЕ

Современная цифровая эпоха требует нового подхода к подготовке специалистов по информационной безопасности. Развитие технологий приводит к усложнению угроз, что делает традиционные методы обучения менее эффективными [1]. Высшие учебные заведения вынуждены пересматривать учебные программы, адаптируя их под современные реалии [2]. Однако одним из главных препятствий остается разрыв между теоретическим обучением и практическими навыками, необходимыми для работы в реальных условиях [3]. Многие выпускники испытывают трудности с применением знаний на практике, что снижает их конкурентоспособность на рынке труда [4].

Значительную роль в регулировании подготовки специалистов по информационной безопасности играют нормативные акты. Например, в России Федеральный закон «О безопасности критической информационной инфраструктуры» [5] устанавливает требования к защите данных, что напрямую влияет на образовательные стандарты. Международные стандарты, такие как ISO/IEC 27001 [6], задают направление для разработки учебных программ, ориентированных на актуальные угрозы и вызовы. Кроме того, в странах ЕС

приняты директивы, регулирующие подготовку специалистов в области кибербезопасности, что также способствует гармонизации образовательных стандартов [7].

Важную роль играет внедрение практико-ориентированных методик обучения, таких как киберучения, симуляции атак и работа с реальными инцидентами в области кибербезопасности [8]. Такие методы позволяют студентам лучше понимать принципы работы современных защитных систем и развивать навыки быстрого реагирования на угрозы. Кроме того, необходимо тесное взаимодействие учебных заведений с бизнесом и государственными структурами [9]. Совместные программы, стажировки и участие специалистов-практиков в образовательном процессе способствуют повышению уровня подготовки будущих специалистов. Важно также учитывать зарубежный опыт, например использование программы NICE в США, которая стандартизирует требования к специалистам по кибербезопасности [10].

Другим важным аспектом является внедрение передовых образовательных технологий. Онлайн-курсы, виртуальные лаборатории и адаптивные обучающие платформы позволяют студентам получать актуальные знания и совершенствовать практические навыки в удобном формате [11]. Гибкость образовательных программ становится ключевым фактором успешной подготовки кадров в условиях стремительных изменений в сфере информационной безопасности. В этом контексте перспективными направлениями становятся использование искусственного интеллекта для персонализации образовательного процесса и развитие виртуальных симуляторов для отработки навыков реагирования на кибератаки [12].

Таким образом, будущее образования в области информационной безопасности связано с интеграцией теоретической базы с практическим обучением, активным сотрудничеством с индустрией и внедрением инновационных образовательных технологий. Анализ нормативных документов и правоприменительной практики показывает, что государственное регулирование должно учитывать динамику развития угроз и потребности рынка. Только такой

комплексный подход позволит подготовить специалистов, способных эффективно противостоять современным киберугрозам и обеспечивать безопасность цифровой инфраструктуры [13].

Трансформация системы подготовки кадров в области информационной безопасности выходит за рамки сугубо образовательной проблемы – она становится частью глобального стратегического вызова, связанного с обеспечением устойчивого развития цифрового общества. Сегодня на первый план выходит необходимость формирования экосистемы киберобразования, в которой объединены усилия государства, бизнеса, научного сообщества и образовательных учреждений. Только в рамках такой кооперации возможно создать условия для появления по-настоящему компетентных специалистов, обладающих не только знаниями, но и широким спектром прикладных навыков.

Более того, в условиях стремительной цифровизации всех сфер жизни – от здравоохранения до промышленности – спрос на профессионалов в области информационной безопасности стремительно растёт. Этот спрос носит не локальный, а глобальный характер: квалифицированные кадры востребованы в любой точке мира. Это означает, что отечественная система образования должна не просто адаптироваться, но и конкурировать с международными практиками, предлагая студентам контент мирового уровня, доступ к международным сертификациям и участие в глобальных инициативах в сфере кибербезопасности.

Особую актуальность приобретает формирование непрерывной образовательной траектории, предполагающей обучение на протяжении всей профессиональной жизни. Технологии меняются быстрее, чем успевают обновляться стандарты, и только специалисты, готовые к постоянному развитию и самообучению, смогут оставаться на острие защиты цифрового пространства. Для этого необходимо внедрение механизмов микроквалификаций, онлайн-платформ с возможностью постоянного обновления знаний и программ наставничества, где опытные практики делятся реальными кейсами с молодыми специалистами.

Одним из ключевых направлений развития системы подготовки специалистов становится интеграция международного опыта и лучших практик, накопленных ведущими странами в сфере кибербезопасности. Так, в Сингапуре реализована государственная программа Cybersecurity Talent Development Scheme, направленная на выявление и развитие талантов ещё на школьном этапе. В Израиле действует система специализированных военных и гражданских учебных центров, где молодые специалисты получают уникальные навыки в условиях, максимально приближенных к реальным киберугрозам. Эти примеры демонстрируют важность ранней профориентации, инвестиции в человеческий капитал и системного подхода к подготовке профессионалов.

Не менее важную роль играет развитие научных исследований в области информационной безопасности. Университеты должны стать не только центрами обучения, но и центрами генерации новых знаний, технологий и методик защиты. На стыке научной и образовательной деятельности рождаются инновационные решения, позволяющие не просто реагировать на киберугрозы, но и предвосхищать их. Поддержка исследовательских проектов, вовлечение студентов в прикладные научные инициативы, проведение хакатонов и форумов – всё это должно стать неотъемлемой частью образовательного процесса.

Кроме того, нельзя игнорировать психологический и этический аспекты подготовки специалистов по информационной безопасности. В условиях, когда границы между частной жизнью и публичным пространством размываются, чрезвычайно важно формировать у будущих профессионалов высокий уровень ответственности, этического мышления и культуры кибергигиены. Осознание последствий своих действий, умение действовать в условиях неопределённости, уважение к правам пользователей и понимание этики кибервзаимодействия – вот ключевые элементы современного цифрового гражданства, которые должны прививаться с первых этапов обучения.

Особое внимание в этом контексте следует уделить формированию долгосрочной стратегии цифровой безопасности, в центре которой находится человек – подготовленный, осведомлённый и способный адаптироваться к новым вызовам специалист. Мы живём в эпоху, где границы между «физическим» и «цифровым» мирами стираются, а информационные технологии проникают во все сферы жизни: от умных городов до систем здравоохранения, от промышленности до личных гаджетов. Это означает, что информационная безопасность перестаёт быть прерогативой только ИТ-специалистов – она становится глобальной культурой, частью общественного сознания.

В этой связи необходим переход от узкопрофессиональной подготовки к междисциплинарному подходу, в котором технические знания сочетаются с юридическими, управленческими и гуманитарными компетенциями. Специалист по информационной безопасности будущего – это не просто «технарь», работающий с кодом, а стратег, аналитик и коммуникатор, способный понимать риски, оценивать последствия и принимать решения на основе комплексного анализа. Такой подход требует пересмотра не только содержания образовательных программ, но и самой философии образования – от передачи знаний к формированию мышления.

На этом фоне критически важным становится воспитание цифровой ответственности и лидерства. Молодые специалисты должны понимать, что защита данных – это не только про технологии, но и про доверие. Доверие граждан к государству, клиентов к бизнесу, общества к технологиям. И именно от уровня профессионализма, этики и зрелости тех, кто стоит на страже этой защиты, зависит устойчивость всего цифрового пространства. Поэтому сегодня как никогда важно вкладываться не только в навыки, но и в ценности, формировать новое поколение специалистов, способных не просто «решать задачи», но и задавать правильные вопросы.

Нельзя забывать и о том, что цифровое пространство уже давно стало ареной геополитического противостояния. Кибератаки на критическую инфраструктуру, утечки конфиденциальной информации,

вмешательства в выборные процессы – всё это поднимает вопросы не только технологического характера, но и вопросы национальной безопасности, суверенитета и международного права. В этих условиях подготовка специалистов по информационной безопасности приобретает не просто профессиональное, а стратегическое значение, сопоставимое с подготовкой офицеров обороны или дипломатов. Именно они, пусть и незаметно, стоят на переднем крае современного цифрового фронта.

Формируя такие кадры, важно не ограничиваться текущими задачами, а смотреть в будущее, опираясь на прогнозирование и анализ трендов. Уже сегодня мир стоит на пороге масштабного внедрения квантовых технологий, искусственного интеллекта и биометрических систем нового поколения. Всё это порождает совершенно новые риски, к которым традиционные образовательные подходы просто не готовы. Возникает потребность в специалистах, которые смогут мыслить нестандартно, находить решения в условиях неопределённости и гибко реагировать на появление угроз, которых ещё вчера не существовало.

Здесь критически важна роль цифровой этики – нового направления, находящегося на стыке философии, технологий и права. Каково допустимое поведение специалиста, обладающего доступом к системам национального уровня? Где границы допустимого в условиях цифровой войны? Как обеспечить баланс между безопасностью и правами человека? Эти вопросы должны становиться частью образовательной повестки, ведь без их осмысления невозможно сформировать поколение ответственных профессионалов. Образование должно не только обучать, но и воспитывать, формировать внутренний моральный компас, способный удержать человека от злоупотребления своими знаниями.

Кроме того, следует понимать, что в современном мире информационная безопасность – это ещё и инструмент цифровой дипломатии. Страны договариваются о правилах цифрового поведения, заключают соглашения о киберсотрудничестве, участвуют в международных форумах и рабочих группах. И в этих процессах всё большее

значение приобретает наличие подготовленных специалистов, способных говорить на одном языке с коллегами из других стран, понимать правовые и культурные контексты, предлагать решения, способствующие глобальной стабильности и взаимному доверию.

Всё это подчёркивает одно: в центре цифрового будущего стоит человек. Не машина, не алгоритм, не протокол, а человек – подготовленный, думающий, честный, ответственный. И именно от того, как мы сегодня будем вкладываться в его образование, зависит, каким будет наш завтрашний день. Безопасным или уязвимым. Цифрово-свободным или под постоянной угрозой. Стратегически сильным или зависимым от чужих решений.

Информационная безопасность – это не просто профессия. Это миссия. Это выбор в пользу служения обществу, ответственности за миллионы людей и бесконечного стремления к совершенству. И потому задача системы образования – не просто дать знания, а зажечь внутри студента огонь интереса, стремление к развитию, внутреннюю тягу к защите и справедливости. Только тогда на смену угрозам придёт устойчивость. На смену страху – уверенность. А на смену хаосу – порядок, выстроенный усилиями тех, кто осознанно выбрал путь цифрового защитника.

И если сегодня мы заложим эти основы – то завтра получим не просто специалистов, а лидеров новой цифровой эпохи, способных не только защищать мир от угроз, но и создавать его заново – безопасным, этичным и справедливым.

Библиографический список

1. Иванов И.И., Петров П.П. Цифровая трансформация и вызовы кибербезопасности. – Москва : Наука, 2021.

2. Смирнов А.А. Современные подходы к образовательным программам по ИБ. – Санкт-Петербург : Питер, 2020.

3. Сидоров В.В. Разрыв между теорией и практикой в обучении ИБ. – Екатеринбург : Уральский университет, 2019.

4. Захаров Д.Д. Конкурентоспособность выпускников в сфере информационной безопасности. – Казань : Таткнига, 2022.

5. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ.

6. ISO/IEC 27001:2022. Информационная безопасность, кибербезопасность и защита конфиденциальности – Системы управления информационной безопасностью – Требования.

7. European Union Agency for Cybersecurity (ENISA). Cybersecurity Skills Framework. – Brussels, 2021.

8. Новиков Е.Е. Практические методы обучения кибербезопасности. – Ростов-на-Дону : ДГТУ, 2023.

9. Лебедев О.О. Интеграция бизнеса и образования в подготовке кадров по ИБ. – Новосибирск : СибАкадемИздат, 2018.

10. National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. – USA, 2020.

11. Тихонов Р.Р. Виртуальные лаборатории и их роль в образовательном процессе. – Минск : Белкнига, 2021.

12. Brown J., Smith K. AI-driven cybersecurity education: The future of learning. – London : CyberTech Press, 2022.

13. Кузнецов М.М. Гибкость образовательных программ в сфере ИБ. – Москва : Экономика, 2022.

Шайхутдинова Надежда Павловна,

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

ПРАВОВЫЕ ПРОБЛЕМЫ РЕАЛИЗАЦИИ ТРУДОВЫХ ОТНОШЕНИЙ В УСЛОВИЯХ ЦИФРОВОЙ РЕАЛЬНОСТИ

Возникновение противоречий между отдельными элементами нормативно-правового регулирования обусловлено многоаспектностью и наличием определенных сложностей действующих правовых отношений, в том числе в сфере труда. Как самостоятельная отрасль права трудовое право также характеризуется наличием определенных правовых коллизий.

В трудовом праве коллизии представляют собой наличие противоречивой правовой ситуации в сфере применения наемного труда, требующей разрешения, но при этом имеет место расхождение отдельных трудоправовых норм. В случае когда предметом правового регулирования являются аналогичные трудовые отношения или отношения, тесно связанные с ними, наличие юридических коллизий вызывает немалые сложности в правоприменении, поскольку решение спорного вопроса не имеет единого подхода и в целом может оказывать негативное влияние на последующий результат рассмотрения вопроса.

Вопрос о видах коллизий трудового права не является новым. Так, принято выделять коллизии, возникающие в результате принятия нормативных правовых актов, содержащих нормы трудового права, на различном уровне (федеральном, региональном, местном, локальном). Правило о приоритете нормативно-правовых актов

более высокой юридической силы позволяет разрешить возникновение подобного рода противоречий.

Аналогично решается вопрос о преодолении коллизий, возникающих в результате расхождения норм трудового права, закрепленных в международных источниках регулирования отношений в сфере труда и имеющих место в нормах российского законодательства о труде. В соответствии со статьей 15 Конституции РФ[136] предусматривается приоритет международных норм и принципов, в том числе положений международных договоров, ратифицированных РФ.

Однако возникают немалые сложности в случае возникновения коллизий правовых норм, закрепленных в нормативно-правовых актах равной юридической силы, поскольку, в частности, как указал Конституционный Суд РФ: «ни один федеральный закон в силу статьи 76 Конституции РФ не обладает по отношению к другому федеральному закону большей юридической силой»[137].

Преодоление подобного рода коллизий может осуществляться путем принятия нового нормативно-правового акта, изменяющего или отменяющего действие предыдущего. Но такое правило устранения противоречий возможно в случае темпоральных коллизий, имеющих место в ситуации, когда несколько нормативно-правовых источников, регулирующих трудовые отношения, приняты в разное время и имеют различное правовое содержание применительно к одной и той же ситуации.

Возникновению темпоральных коллизий способствуют изменяющиеся общественные отношения, которые оказывают влияние на функционирование правовых связей в сфере наемного труда.

---

[136] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс» (дата обращения: 23.04 2025).

[137] По запросу Арбитражного суда города Москвы о проверке конституционности пунктов 1 и 4 части четвертой статьи 20 Федерального закона "О банках и банковской деятельности" : определение Конституционного Суда РФ от 05.11.1999 № 182-О // СПС «КонсультантПлюс» (дата обращения: 23.04 2025).

В рамках данной статьи рассмотрим появление правовых коллизий в условиях цифровизации прежде всего в трех основных направлениях регулирования отношений в сфере труда: электронные трудовые книжки, электронный кадровый документооборот и дистанционный труд.

Так, при внедрении цифровизации в Трудовом кодексе РФ[138] (далее – ТК РФ) появились новые нормы, касающиеся сведений о трудовой деятельности работника, которые регулируют отношения параллельно с ранее существующими применительно к одной и той же ситуации. Согласно статье 66 ТК РФ трудовые книжки ведутся работодателем по основному месту работы на каждого работника, проработавшего у него свыше пяти дней. В связи с цифровизацией и появлением «электронных трудовых книжек» у работодателя появилась обязанность формировать в электронном виде основную информацию о трудовой деятельности и трудовом стаже каждого работника в соответствии со статьей 66.1 ТК РФ. Данная информация подлежит учету в системах обязательного пенсионного страхования для хранения в информационных ресурсах Фонда пенсионного и социального страхования РФ. В связи с этим возникает вопрос о необходимости соблюдения пятидневного срока для ведения трудовых книжек, поскольку информацию о трудовой деятельности и трудовом стаже работника работодатель обязан передать в Социальный фонд России «не позднее рабочего дня, следующего за днем издания приказа (распоряжения), иного документа, принятия решения, которые подтверждают оформление, приостановление, возобновление или прекращение трудовых отношений»[139]. Возможно, условие о пятидневном сроке начала ведения трудовой

[138] Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 07.04.2025) // СПС «КонсультантПлюс» (дата обращения: 24.04.2025).

[139] Об индивидуальном (персонифицированном) учете в системах обязательного пенсионного страхования и обязательного социального страхования : Федеральный закон от 01.04.1996 № 27-ФЗ (ред. 25.12.2-23) (статья 11 пункт 5 подпункт 2) // СПС «КонсультантПлюс» (дата обращения: 24.04.2025).

книжки было актуально при исчислении непрерывного трудового стажа, а также для трудоправовой характеристики соискателя. Указанные причины в условиях цифровизации не имеют своего первоначального значения, поскольку при предъявлении документа «Сведения о трудовой деятельности» при заключении трудового договора информация о всех предыдущих работодателях и сроках работы у него будет представлена в электронном варианте.

Также не покидает внимание работодателей вопрос об определении категории трудового договора: по основному месту работы или о работе по совместительству. Исторически основное место работы работника определялось по наличию у работодателя его трудовой книжки. С переходом на «электронные трудовые книжки» данное определение основного места работы утратило свою актуальность. Безусловно, вопрос о наличии или отсутствии трудовых отношений с другим работодателем может быть решен при предъявлении соискателем сведений о трудовой деятельности по форме СТД-СФР через многофункциональный центр (далее – МФЦ), Социальный фонд России (далее – СФР) или на портале государственных услуг, о чем закрепляется в частях 4 и 5 статьи 66.1 ТК РФ. Трудовой кодекс РФ не содержит запрета о предоставлении работодателю при поступлении на работу сведений о трудовой деятельности, но и не обязывает предоставить данный документ. К такому выводу можно прийти из анализа части первой статьи 65 ТК РФ и статьи 283 ТК РФ. Вместе с тем в части третьей статьи 65 ТК РФ содержится запрет требовать от лица, поступающего на работу, документы помимо предусмотренных ТК РФ, иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ. Работодатель в целях определения у соискателя основной работы может только предложить предоставить сведения о трудовой деятельности. Но если работник не согласится их предоставить, это не может служить основанием для отказа ему в заключении трудового договора согласно части первой статьи 64 ТК РФ, поскольку такой отказ может быть квалифицирован как необоснованный.

Таким образом, имеет место коллизия темпоральных норм, где, с одной стороны, работодатель не вправе требовать документы, не предусмотренные законом, а, с другой стороны, отсутствие отдельных документов не позволяет решить объективно вопрос о том, какой трудовой договор может быть заключен: по основному месту работы или по совместительству.

Неоднократно в процессе регулирования трудовых отношений поднимается вопрос о возможном применении в качестве письменной формы документа его электронное оформление. Все вопросы снимаются, если у работодателя введен электронный документооборот при соблюдении всех необходимых для этого требований.

Определенные коллизии правовых норм в процессе регулирования отношений в сфере труда приходится наблюдать при применении работодателем цифровых средств контроля за исполнением работником своей трудовой функции: применение аудио, видеозаписей, sim-карт и т.п. С одной стороны, если это указано в локальном нормативном акте (например, в Правилах внутреннего трудового распорядка), с которым работник ознакомлен под роспись до подписания трудового договора, работодатель в своих интересах использует данные средства вполне легально, определяя трудовой распорядок в организации в соответствии со статьей 189 ТК РФ. С другой стороны, система цифрового контроля функционирует у работодателя не только в рабочее время конкретного работника, но и за его пределами. Цифровые средства контроля позволяют эффективно отслеживать соблюдение работниками трудовой дисциплины, но при этом они не должны нарушать требования норм о защите персональных данных в соответствии с требованиями Федерального закона «О персональных данных»[140] и неприкосновенности частной жизни, о чем говорится в статье 23 Конституции РФ.

[140] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) // СПС «КонсультантПлюс» (дата обращения: 24.04.2025).

Правовые коллизии в трудовом законодательстве в условиях цифровизации наблюдаются с введением норм о регулировании труда дистанционных работников. В условиях цифровизации основным инструментом взаимодействия сторон трудового договора дистанционных работников являются информационно-телекоммуникационные сети. В целях оформления дистанционной работы получил развитие электронный документооборот, учитывающий особенности работы удаленно. Обмен электронными документами для трудового права России также явился новой формой коммуникации сторон трудового отношения. При таком способе коммуникации необходимо соблюдать законодательно установленные специальные требования. В частности, сторонам необходимо направлять подтверждение о получении электронного документа в установленные сроки, использовать усиленную квалифицированную электронную подпись.

Так, часть четвертая статьи 91 ТК РФ предусматривает правило, согласно которому работодатель обязан вести учет фактически отработанного каждым работником времени. Но сложность возникает в том, что дистанционный работник преимущественно распределяет свое время самостоятельно, а это влечет за собой трудности в учете фактически отработанного времени.

Особенностью является также и отсутствие у работодателя обязанности оплачивать дистанционному работнику переработку (сверхурочную работу, привлечение к работе в выходные и праздничные дни), если содержание трудового договора не предусматривает установление строго определенного графика работы, продолжительность рабочей недели, режим работы и чередование рабочих и нерабочих дней. Такой вывод следует из анализа части второй статьи 312.4 ТК РФ, предоставляющей возможность дистанционному работнику устанавливать режим рабочего времени по своему усмотрению, если данное условие не предусмотрено соглашением сторон трудового договора, коллективным договором или локальным нормативным актом, принятым с учетом мнения выборного органа первичной профсоюзной организации.

В регулировании труда дистанционных работников существуют сложности также в обеспечении работодателем требований охраны труда, поскольку работа выполняется вне места нахождения работодателя. Несмотря на то, что в вопросах обеспечения безопасных условий и охраны труда работодатель законодательно ограничен рамками статьи 312.3 ТК РФ, в то же время он обязан обеспечить расследование и учет несчастных случаев в соответствии с общим порядком, установленным статьями 227–231 ТК РФ. При этом квалификация травмы как несчастный случай на производстве, имеющий место с дистанционным работником, производится, если комиссией установлено, что травма получена при выполнении задания работодателя, что довольно затруднительно в отсутствие свидетелей и других подтверждающих фактов.

В частности, некоторые работодатели полагают что, если в содержании трудового договора отсутствует условие о дистанционном характере работы, то в любое время работодатель вправе потребовать от работника выполнения работы на стационарном рабочем месте. Ошибочность данного суждения, предусматривающего приоритет юридического оформления отношений о дистанционном характере работы, подтверждается материалами судебной практики. Так, в Обзоре рассмотрения судами дел по спорам, связанным с прекращением трудового договора по инициативе работодателя, утвержденном Президиумом Верховного Суда Российской Федерации 09.12.2020[141], суд указал, что не может быть признано обоснованным дисциплинарное увольнение работника в случае, когда работник отсутствовал на стационарном рабочем месте по адресу нахождения работодателя и его отсутствие было обусловлено тем, что работник по согласованию с работодателем выполнял свои трудовые обязанности дистанционно, даже если условие о дистанционной работе не было включено в трудовой договор.

[141] Обзор практики рассмотрения судами дел по спорам, связанным с прекращением трудового договора по инициативе работодателя (утв. Президиумом Верховного Суда РФ 09.12.2020) // СПС «КонсультантПлюс» (дата обращения: 24.04.2025).

Аналогичный вывод в судебной практике сделан также при изменении условия трудового договора о характере работы. Так, судебная коллегия по гражданским делам Верховного Суда Российской Федерации по данному вопросу выразила правовую позицию о том, что следует считать заключенным и не оформленное в письменной форме соглашение сторон об изменении определенных сторонами условий трудового договора, если работник приступил к работе в таких измененных условиях с ведома или по поручению работодателя или его уполномоченного на это представителя, в том числе и о выполнении работником определенной трудовым договором трудовой функции дистанционно, то есть вне места нахождения работодателя и вне стационарного рабочего места. По мнению судебного органа неоформление работодателем в надлежащей форме изменений условий работы (перевод работника на удаленную работу вне места нахождения работодателя) прежде всего может свидетельствовать о допущенных нарушениях со стороны работодателя по надлежащему оформлению отношений с работником[142].

Проблематичным для работодателей является применение основания увольнения дистанционного работника за прогул, несмотря на то, что общие основания прекращения трудового договора, установленные статьей 81 ТК РФ, распространяются на данный вид трудовых отношений в полном объеме. Проблема заключается в том, что понятие «рабочее место», которое является ключевым в содержании подпункта «а» пункта 6 части первой статьи 81 ТК РФ и раскрывается в дефиниции части шестой статьи 209 ТК РФ, не может в полной мере применяться к дистанционному работнику, поскольку он выполняет свою трудовую функцию вне места нахождения работодателя, вне стационарного рабочего места, которое прямо или косвенно может находиться под его работодательским контролем. По данному поводу в судебной практике выработана правовая позиция, предусматривающая, что если в ходе судебного

[142] Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 16.09.2019 № 5-КГ19-106 // СПС «КонсультантПлюс» (дата обращения: 24.04.2025).

разбирательства факт осуществления работником трудовых обязанностей дистанционно подтвержден, а в трудовом договоре отсутствует условие о рабочем месте работника, на которое ему следует являться для осуществления трудовой функции и на котором он отсутствовал по утверждению работодателя, то это не может рассматриваться как нарушение трудовой дисциплины. Суд подчеркнул, что ненадлежащее оформление условий трудового договора не влечет невозможности установления фактических правоотношений сторон и не может повлечь за собой негативные последствия для работника[143]. При дистанционном исполнении по согласованию с работодателем трудовых обязанностей работником целесообразно четко определить в условиях трудового договора, где именно должно находиться рабочее место работника. В противном случае увольнение работника за прогул весьма затруднительно.

Таким образом, правовая природа и содержание трудового договора с дистанционным работником должно в полной мере соответствовать требованиям общей нормы статьи 57 ТК РФ, но в условиях цифровой реальности в нем необходимо предусмотреть особенности, продиктованные спецификой дистанционных отношений.

[143] Обзор практики рассмотрения судами дел по спорам, связанным с прекращением трудового договора по инициативе работодателя (утв. Президиумом Верховного Суда РФ 09.12.2020) // СПС «КонсультантПлюс» (дата обращения 24.04.2025).

Гончарова Наталья Николаевна,

канд. юрид. наук, доцент кафедры международного и европейского права ЧОУ ВО «Казанский инновационный университет им. В.Г. Тимирясова» (ИЭУП), г. Казань

ИНФОРМАЦИЯ, СОСТАВЛЯЮЩАЯ ГОСУДАРСТВЕННУЮ ТАЙНУ, В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Современный этап развития отличается повышенным вниманием государства к вопросам безопасности информации, составляющей высокую степень интересов акторов международных и внутригосударственных правоотношений.

Стремительный скачок в использовании технологий информационно-коммуникационного назначения объективно вызывает увеличение объема данных, являющихся предметом государственной охраны, разглашение которых способно оказать губительное влияние на ход политических или военных событий. Обращение информации может иметь государственное значение, а ее охрана влиять на реализацию принципов государственного суверенитета, невмешательства во внутренние дела государства и другие.

Национальная безопасность фактически зависит от тех правовых ограничений, которые предусмотрены законодательством России, начиная от ст. 29 Конституции Российской Федерации, где конституционные правомочия граждан в свободном поиске, получении, передаче и распространении сведений любым незащищенным способом не касаются тех, которые составляют государственную тайну. Серьезное внимание в обеспечении реализации идеи защиты государственной тайны отведено в уголовном законодательстве Российской Федерации, а Уголовный кодекс Российской Федерации[144] предусматривает ответственность за деяния в области обращения государственной тайны.

[144] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025) // Собрание законодательства РФ. 1996. № 25, ст. 2954; 2025. № 9, ст. 860.

Вопросы, взаимосвязанные с охраной государственной тайны, а также проблемы ее разглашения были и остаются весьма важными, особенно в условиях специальной военной операции. В качестве объектов, вызывающих немалый интерес разведывательных групп иностранных государств, выступают сведения о внешнеполитическом, научном, технологичном и военном потенциале Российской Федерации. Все это указывает на особое значение работы по применению мер охранительного характера и повышению стратегического уровня в таких вопросах, как развитие экстрадиционных связей[145].

Уголовным кодексом Российской Федерации гл. 29 предусматривается наступление уголовной ответственности за преступные деяния, в качестве предмета преступных посягательств которых выступает государственная тайна.

Составляющая государственную тайну информация строго засекречена, и доступ к ней предоставляется исключительно определенному кругу лиц. Государственная тайна отличается четкой взаимосвязью с интересами государства, и ее перехват или разглашение влечет причинение ущерба.

В настоящее время мы наблюдаем за установлением нового миропорядка в условиях развития принципов многополярности. Передел мироустройства заведомо связан с обеспечением силы государств, стремящихся к миру, где государства проложили путь к устойчивому развитию каждого.

В результате всеобщей цифровизации государственные системы и данные становятся мишенью для хакерских атак, шпионажа и кибертерроризма. Своевременно Генеральной Ассамблеей ООН в декабре 2024 года была принята Конвенция против киберпреступности[146], предложенная к ратификации государствам – членам ООН.

[145] Клемин А.В., Гончарова Н.Н., Денисович В.В. Экстрадиция сегодня: проблемы реализации // Проблемы экономики и юридической практики. 2022. Т. 18, № 6. С. 150–154.

[146] Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися

Киберпространство формирует новую информационную картину мира[147] и влияет на все сферы государственной безопасности.

В соответствии со ст. 29 Конституции РФ информация, которая составляет государственную тайну, определяется согласно федеральному законодательству. Статья 2 Закона «О государственной тайне»[148] закрепляет понятие государственной тайны, а именно находящиеся под защитой государства сведения, распространение которых способно причинить ущерб безопасности Российской Федерации.

Уголовный кодекс РФ в главе 29 предусмотрел ответственность за деяния, посягающие на сохранение государственной тайны в статьях 283, 283.1, 283.2 и 284. Данные нормы не предполагают сговор с зарубежными службами в целях нанесения ущерба России, однако квалифицируют деяния, способствующие утечке секретной информации за пределы Российской Федерации и применение ее против России, безопасности, государственной территории и др.

В качестве непосредственного объекта преступлений по указанным статьям УК РФ выступают общественные взаимоотношения, которые гарантируют соответствующую сохранность государственной тайны в интересах обеспечения безопасности Российской Федерации. В случае посягательств на данный объект может быть причинен ущерб военному, экономическому, научному потенциалу Российской Федерации. Дополнительным непосредственным объектом являются правила обращения с информацией, содержащей государственную тайну.

Для объективной стороны преступного состава ст. 283 УК РФ наиважнейшее значение имеет в первую очередь термин «разглашение». Уголовным законодательством РФ не дается определения данного понятия и способов, посредством которых совершается

к серьезным преступлениям 2024 года. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 10.03.2025).

[147] Радченко Т.В., Шевелева К.В. Правовые аспекты определения границ киберпространства // Вестник экономики, управления и права. 2024. Т. 17, № 3. С. 62.

[148] О государственной тайне : Закон Российской Федерации от 21.07.1993 № 5485-1 (ред. от 08.08.2024) // Российская газета. 1993. № 182.

это деяние. Таким образом, разглашение государственной тайны нужно рассматривать как деяние (действие или бездействие) лица, вследствие которого информация, содержащая государственную тайну, доверенная ему или ставшая известной вследствие осуществления им служебных обязанностей, стала известна хотя бы одному постороннему лицу.

Разглашение, производимое посредством активной деятельности, представляет собой любую форму передачи государственной тайны посторонним. Произведение разглашения посредством преступного бездействия заключается в непринятии соответствующих мер, направленных на сохранение сведений, содержащих государственную тайну, вследствие чего информация стала известна посторонним.

Объективную сторону преступления ч. 2 ст. 283.2 УК РФ представляют перемещение и пересылка, а преступление считается оконченным в момент пересечения границы носителем информации, являющейся государственной тайной. Объективную сторону в ст. 284 УК РФ – утрата документов, которые содержат государственную тайну, или материальных носителей, сведения, которые образуют государственную тайну, составляют деяния в форме действия или бездействия, связанные с нарушением правил обращения с государственной тайной и, возможно, приведшие к наступлению тяжких последствий.

Основными применяемыми судами разновидностями основных наказаний за преступления, предусматривающие посягательства на сохранность государственной тайны, являются лишение свободы, арест, ограничение свободы, штраф. Также возможно применение и дополнительных наказаний: лишение правомочий относительно занятия определенных должностей либо занятия определенными видами деятельности; лишение специальных, воинских или почетных званий, классного чина и государственных наград.

Уголовная ответственность не возникает при следующих обстоятельствах – по причине отсутствия события либо состава преступления; истечения срока давности. Сроки давности в отношении рассматриваемой группы преступлений, посягающих на сохранность

государственной тайны, выразившиеся в доведении до третьих лиц, не обладающих допуском до такого рода сведений, равны от 6–10 лет в зависимости от квалифицирующих составов.

Возможность уголовной ответственности как наиболее строгой разновидности наказаний должна быть установлена относительно деяний, обладающих высокой степенью и характером общественной опасности, поэтому необходимо установление дополнительных признаков в составе ст. 283.2 УК РФ, которые бы отражали уровень общественной опасности деяния. К таким могут относиться многократное перемещение через государственную границу или, возможно, сопряжено с любым разглашением информации, составляющей государственную тайну.

Важно отметить, что предложенная к ратификации Конвенция против киберпреступности в ст. 18 допускает оказание правовой помощи – допрос лица в качестве свидетеля, потерпевшего или эксперта по просьбе участника договора с помощью видеоконференц-связи, если личное присутствие лица, проводящего процессуальные действия, не является возможным или желательным. При этом при отсутствии технической возможности по взаимной договоренности техническое средство может быть предоставлено государством пребывания по взаимной договоренности. Такая возможность действительно дает возможность реализации задач следствия[149], может содействовать упрощенной процедуре получения известных сведений[150].

---

[149] Гончарова Н.Н., Дятлова Е.В. Развитие уголовного процессуального законодательства в сфере проведения следственных действий с использованием видео-конференц-связи с лицами, находящимися на территории иностранных государств // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции : в 6 т. (Казань, 22 сентября 2023 года). Казань : Издательство "Познание", 2023. С. 80.

[150] Гончарова Н.Н., Латыпова Э.Ю., Гончаров Н.А. Проблемы проведения уголовно-процессуальных действий с участием иностранных граждан, на российской территории, а также в зданиях посольств и консульств России // Пробелы в российском законодательстве. 2021. Т. 14, № 4. С. 371.

По нашему мнению, при ратификации Конвенции Российской Федерации следует сделать оговорку в части такой правовой помощи, «кроме допроса лиц по делу, включающему информацию составляющую государственную тайну». Это обусловлено, в частности, требованиями ст. 16 Закона «О государственной тайне», где четко закреплено, что органы государственной власти, <…> запрашивающие сведения, составляющие государственную тайну, обязаны соблюдать условия, обеспечивающие защиту таких сведений.

Выводы:

1. Степень общественной опасности преступлений, связанных с разглашением государственной тайны, была и остается очень высокой. В этой связи представляется нужным и обоснованным поднятие планки максимально предусматриваемых наказаний в отношении лиц, совершивших преступные деяния по ст. 283, 283.1, 283.2, 284 УК РФ. Максимальные наказания, предусматриваемые квалифицирующими частями статей, также соразмерно должны быть изменены.

2. Полагаем, что в процессе назначения наказания уровень тяжести возможного вреда при посягательствах на сохранность государственной тайны, при ее разглашении либо утраты, должен соотноситься с уровнем ее секретности.

3. При ратификации Конвенции против киберпреступности следует сделать оговорку об ограничениях в части использования видео-конференц-связи в делах, по которым предполагается передача информации, составляющей государственную тайну. Это необходимо в силу заведомо слабо защищенного способа передачи информации.

Библиографический список

1. Гончарова Н.Н. Развитие уголовного процессуального законодательства в сфере проведения следственных действий с использованием видео-конференц-связи с лицами, находящимися на территории иностранных государств / Н.Н. Гончарова, Е.В. Дятлова // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции : в 6 т. (Казань, 22 сентября 2023 года). – Казань : Издательство "Познание", 2023. – С. 77–80.

2. Гончарова Н.Н. Проблемы проведения уголовно-процессуальных действий с участием иностранных граждан, на российской территории, а также в зданиях посольств и консульств России / Н.Н. Гончарова, Э.Ю. Латыпова, Н.А. Гончаров // Пробелы в российском законодательстве. – 2021. – Т. 14, № 4. – С. 366–372.

3. Клёмин А.В. Экстрадиция сегодня: проблемы реализации / А.В. Клёмин, Н.Н. Гончарова, В.В. Денисович // Проблемы экономики и юридической практики. – 2022. – Т. 18, № 6. – С. 150–154.

4. Радченко Т.В. Правовые аспекты определения границ киберпространства / Т.В. Радченко, К.В. Шевелева // Вестник экономики, управления и права. – 2024. – Т. 17, № 3. – С. 62–68.

Дубень Андрей Кириллович,

канд. юрид. наук, ученый секретарь Института государства и права Российской академии наук, г. Москва

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ИНФОРМАЦИОННОГО ПРАВА

Правовое обеспечение информационной безопасности занимает особое место в системе информационного права. Актуальность данной темы обусловлено тем, что стремительный рост развития правового обеспечения информационной безопасности обусловлен геополитической трансформацией и турбулентностью. Стратегические задачи развития безопасности в информационной сфере определены в ряде нормативных актов. В частности, Стратегия национальной безопасности Российской Федерации определяет организационные, нормативные правовые и информационные основы обеспечения национальной безопасности Российской Федерации и содержит основные показатели ее состояния.

Как справедливо отмечает доктор юридических наук Г.Г. Камалова, стремительное развитие цифровых технологий и информационного пространства оказывает в настоящее время трансформирующее воздействие на все сферы жизни человека, детерминируя переход на следующий этап цивилизации, в этой связи цивилизационные процессы влияют на информационную безопасность, которая всегда испытывала значительное влияние информационно-технологического прогресса, используя его достижения в целях обеспечения национальной безопасности[151]. Кроме того, Т.А. Полякова справедливо отмечает, что сегодня задачи формирования системы информационной безопасности являются стратегическими для реализации национальной политики как во внешнем, так и во внутреннем контуре[152].

Одним из основных элементов правового регулирования информационной безопасности являются документы стратегического планирования, такие как Стратегия национальной безопасности, Стратегия комплексной безопасности детей в Российской Федерации, Основы государственной политики в области международной информационной безопасности, Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации, информационной безопасности детей, утвержденных указами Президента Российской Федерации и актами Правительства Российской Федерации.

---

[151] Обеспечение информационной безопасности: вопросы теории и практики : сборник статей Всероссийской научно-практической конференции (Ижевск, 29 мая 2023 года) / науч. редакторы Г.Г. Камалова, В.Г. Ившин, Г.А. Решетникова. Ижевск : Издательский дом «Удмуртский университет», 2023. С. 20.

[152] Полякова Т.А. Стратегические задачи формирования системы международной информационной безопасности и международное информационное право: проблемы и перспективы // Безопасность как стратегический национальный приоритет России в условиях современности : материалы Шестого международного транспортно-правового форума (Москва, 14–15 февраля 2024 года). Москва : Российский университет транспорта (МИИТ), 2024. С. 54.

Таким образом, из анализа нормативных актов стоит сделать вывод, что информационная безопасность – это часть национальной безопасности, имеющая определенные стратегические направления внутри государства, развитие которой определяется задачами противодействия внутренним и внешним информационным угрозам при использовании цифровых технологий; развивающимся геополитическим рискам деструктивного воздействия, связанным с разрушением информационного пространства Российской Федерации, нарушение прав и свобод граждан в информационной сфере, а также безопасности общества и государства и обеспечения социально-экономического развития страны и отечественных цифровых технологий в рамках достижения технологического суверенитета Российской Федерации.

В условиях высоких темпов развития информационных технологий и совершенствования цифрового общества актуализируется проблема по выявлению новых вызовов и угроз. Таким образом, развитие национальной системы правового обеспечения информационной безопасности определяется совокупностью факторов:

– динамичный рост использования цифровых технологий в государственном и частном секторе;

– обновление стратегических направлений государственной политики в информационной сфере;

– совершенствование механизмов правового обеспечения информационной безопасности;

– использование публично-правовых средств;

– стратегическая значимость обеспечения технологического суверенитета государства как одного из приоритетных направлений внутренней и внешней политики государства;

– правовые проблемы регулирования правоотношений при общественно опасном и противоправном деянии.

В связи с этим, проанализировав все факторы, важной задачей является активизация федеральных органов государственной власти по установлению общегосударственных стандартов, обеспечивающих информационную безопасность в Российской Федерации.

Считаем, что на сегодняшний день развитие российского законодательства в области информационной безопасности во многом определено общей модификацией норм национального законодательства, которая, безусловно, учитывает особенности правового, политического, социального и экономического характера развития государственности. В этой связи особенно важно остановиться на одной из проблем регулирования правоотношений при общественно опасном и противоправном деянии.

В этой связи существенное значение приобретает уголовно-правовая политика Российской Федерации, позволяющая обозначить ключевые аспекты уголовно-правовой охраны от посягательств на наиболее значимые интересы в области информационной безопасности граждан, общества и государства в целом[153].

Данный аспект важен тем, что в настоящее время проблема уголовно-правового обеспечения информационной безопасности требует незамедлительного принятия решений, которые обусловлены рядом факторов, одними из которых являются возникновение новых угроз, рисков и вызовов и стремительное развитие информационных технологий, использование которых влечет негативные последствия для общества и государства.

Согласно официальной статистике в первом квартале 2025 г. финансовый сектор столкнулся с беспрецедентным ростом кибератак – по сравнению с аналогичным периодом прошлого года их количество увеличилось в 2,2 раза[154]. Общее число зарегистрированных киберпреступлений в 2024 году возросло на 14,6 % по сравнению с показателями прошлого года, данный фактор обусловлен тем, что увеличилось число преступлений, связанных с неправомерным доступом к компьютерной информации, при этом на 11,5 %

[153] См.: Авдеев В.А., Авдеева О.А. Основные направления совершенствования правовой политики по обеспечению в условиях глобализации информационной безопасности // Российская юстиция. 2021. № 3. С. 2–4.

[154] В России выросло число кибератак на финансовый сектор // Официальный сайт «РИА Новости». URL: https://ria.ru/20250419/kiberataki-2012227202.html (дата обращения: 19.04.2025).

сократилось количество дистанционных краж[155]. Таким образом, наблюдается постоянная положительная динамика преступных деяний, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, и увеличение их доли в общей структуре преступности. Эксперты прогнозируют дальнейшее увеличение общественно опасных деяний в структуре киберпреступности ввиду быстроразвивающихся информационных технологий, которые являются оружием массового поражения, наносящим вред различным сферам деятельности личности, общества и государства[156].

Считаем, что в условиях геополитической нестабильности и трансформации мирового порядка современные кибератаки, имеющие нестандартные методы, способы и средства их совершения, требуют на законодательном уровне оперативности работы по предотвращению и недопущению деструктивного воздействия на отечественные информационные ресурсы и информационную инфраструктуру государственного и частного сектора.

Определяя научные подходы к определению основных направлений исполнения задач по реализации государственной политики национальной безопасности в сфере информационной безопасности, считаем, что в рамках уголовно-правовой защиты необходимо предпринять меры по отдельным направлениям:

– противодействие общественно опасным и противоправным деяниям, совершенным с использованием информационных, технических коммуникационных и иных технологий;

– минимизация преступлений против личности, государственной власти и общественной безопасности;

– создание эффективной организации современной антитеррористической борьбы, противодействие деструктивному информационному воздействию на человека.

---

[155] Краткая характеристика состояния преступности в Российской Федерации за январь – октябрь 2024 года // Официальный сайт МВД России. URL: https://мвд.рф/reports/item/57279296/ (дата обращения: 24.01.2025).

[156] См.: Голубых Н.В. Киберпреступность: современное состояние и прогноз // Вестник Уральского юридического института МВД России. 2021. № 4. С. 130.

Таким образом, эффективные меры по минимизации преступлений в данной сфере зависит от ряда факторов, в т.ч. от взаимодействия с отраслями права. Взаимосвязь информационной безопасности с уголовным правом проявляется в появлении новых видов преступлений в информационном пространстве, усиливающих роль информационной безопасности. Институционально правовое обеспечение информационной безопасности формируется и развивается «на стыке» отраслей информационной сферы и сферы обеспечения безопасности. О.С. Макаров по данному поводу справедливо отмечает, что «правовое обеспечение информационной безопасности концептуально надстраивается на уже существующие системы информационных правоотношений (базовые системы) и обеспечивает безопасность их поступательного развития»[157].

Таким образом, повышение качества правового обеспечения информационной безопасности зависит от принятия эффективных мер по формированию системы информационной безопасности на национальном и международном уровнях. Проанализировав основные факторы, влияющие на развитие информационной безопасности, важно определить направление государственной политики в данной сфере, одним из которых является минимизация преступлений с использованием информационных технологий. Считаем, что повышение эффективности мер по обеспечению информационной безопасности поспособствует установлению единообразного подхода к квалификации преступлений.

[157] Макаров О.С. Правовое обеспечение информационной безопасности на примере защиты государственных секретов государств – участников Содружества Независимых Государств : дис. ... д-ра юрид. наук. М., 2013. С. 73.

Невоструев Андрей Геннадьевич,

канд. юрид. наук, доцент, доцент кафедры гражданского права ИПСУБ ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

НЕКОТОРЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ИЗВЕЩЕНИЙ В ГРАЖДАНСКОМ СУДОПРОИЗВОДСТВЕ

Процесс внедрения информационных технологий и систем в гражданское судопроизводство имеет множество положительных моментов, например, судебный процесс становится более открытым и доступным для участников судопроизводства. Значительно растет скорость и качество судебного делопроизводства, сокращаются судебные издержки. Однако изменение судебной системы в сторону развития информационных технологий требует больших вложений, таких как преобразование процессуальных правил, доработка нормативных актов, закрепление в законодательстве новых положений, обеспечивающих права и свободы граждан в области применения информационных технологий в судебной системе. В результате внедрения новых технологий в судопроизводстве появляется новый круг прав и обязанностей сторон.

Информационные технологические изменения коснулись всей судебной системы, в том числе и области судебных извещений. Судебные извещения представляют собой информацию, содержащую данные по конкретному судебному делу, направляемую судом в адрес лиц, участвующих в процессе. Здесь же происходит подача документов в суд, получение извещений и иной информации от суда, о возбуждении дела, последующих процессуальных действиях и вынесенных судебных актах[158].

[158] Решетняк В.И., Смагина Е.С. Информационные технологии в гражданском судопроизводстве (российский и зарубежный опыт). М. : Городец, 2017. С. 14.

С момента внедрения новых технологий в судопроизводство были внесены изменения и дополнения в процессуальные кодексы, касающиеся применения таких технологий при извещении участников процесса.

Первопроходцем в области изменения способа извещения лиц, участвующих в деле, стал арбитражный процесс. Для разгрузки судов АПК РФ[159] предусмотрел правило, согласно которому бремя по отслеживанию судебной информации по конкретному делу было переложено на участников процесса. Связано это с тем, что участниками арбитражного судопроизводства могут быть только лица, осуществляющие предпринимательскую деятельность и другие виды экономической деятельности. Предполагается, что при осуществлении экономической деятельности субъект несет все риски, он имеет больше технических и финансовых возможностей по приобретению различных технических средств, с помощью которых возможно принять участие в судебных заседаниях. Экономических споров намного больше, поэтому для разгрузки судов с арбитражных судов была снята обязанность направлять извещения на бумажных носителях.

Для решения данной задачи была разработана система «Мой арбитр», которая представляет собой базу данных о судебных делах всех инстанций. Данная система не только хранит и обрабатывает большой объем данных, но и предоставляет участникам процесса возможность отслеживать и знакомиться с информацией по судебному делу.

Аналогичные изменения были внесены и в деятельность судов общей юрисдикции. Однако отличие от арбитражного процесса заключается в том, что в судах общей юрисдикции изменения по поводу судебного извещения коснулись только в отношении государственных органов различных уровней.

---

[159] Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ (ред. от 08.08.2024) // "Собрание законодательства РФ". 29.07.2002. № 30, ст. 3012.

В КАС РФ[160] получили нормативное закрепление новые способы извещения при помощи СМС. Законодательно была установлена допустимость их использования при наличии согласия лиц, участвующих в деле[161].

Нововведения, касающиеся внедрения новых технологий в процесс направления извещений об информировании о предстоящих судебных заседаниях, а также других процессуальных действиях путем использования электронных средств связи, стали вводиться в законодательство с 2020 года[162]. Данный процесс получил ускорение после короновирусной инфекции.

Для эффективной реализации применения электронных извещений необходимо не только обеспечить технологической базой, но повысить уровень открытости государственных органов в отношениях с гражданами, в том числе при осуществлении судопроизводства. Таким образом, правоприменителю следует сделать еще больший акцент на обеспечении и гарантировании прав участников процесса на получение всей информации, касающейся конкретного судебного дела. Одной из гарантий осуществления этого права может выступать закрепление обязанности суда в предоставлении всей необходимой информации в полном объеме и в определенные сроки.

При этом важно обеспечить гарантию равного доступа к этой информации всех участников процесса.

При изучении данного вопроса нам представляется, что можно говорить о внедрении самостоятельного принципа – принципа доступности информации.

---

[160] Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ (ред. от 08.08.2024) // Российская газета. 11.03.2015. № 49.

[161] О внесении изменений в некоторые Постановления Пленума ВС РФ : постановление Пленума ВС РФ от 9 февраля 2012 г. № 3 // Бюллетень Верховного Суда РФ. Апрель, 2012. № 4.

[162] О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 30.12.2021 № 440-ФЗ // Российская газета. 10.01.2022. № 1.

В области административного судопроизводства помимо основных принципов права и отраслевых принципов закреплен принцип открытости судебного разбирательства. Также закреплено правило о том, что лица, чьи интересы затронуты соответствующим решением, не могут быть ограничены в правах на получение соответствующей информации по делу, права на ознакомление с материалами дела.

Так, в результате закрепления данных прав в законодательстве можно говорить о реальной необходимости закрепления нового принципа гражданско-процессуального права, разработать теоретическую базу, провести анализ элементов, составляющих основу этого принципа, выработать положение о правах, обязанностях сторон правоотношений, а также ответственность в случае несоблюдения данного принципа.

Сущность принципа доступности информации в судопроизводстве можно раскрыть через особенности:

– лицо должно иметь право на получение информации о том, когда и где суд будет рассматривать дело, в случае его замены – узнать о причинах замены;

– у лица должна быть возможность иметь равный доступ к материалам дела как на бумажном носителе, так и в электронном виде.

– лицо должно иметь право на получение извещений о вынесенных решениях в электронном виде.

Значение данного принципа в первую очередь связано с тем, что гарантируется равный доступ к судебной информации. Внедрение этого принципа имеет своей целью совершенствование процессуальных норм и избежание риска ограничений права лица на получение информации. Таким образом, принцип доступности информации о судопроизводстве должен стать ориентиром на пути к разработке и внедрению информационных технологий и систем в гражданское судопроизводство.

По мнению И.Н. Спицына, «Представляется, что, рассматривая вопросы о доступе к информации о деле, необходимо анализировать в единстве нормы об извещениях о процессуальных

действиях и нормы о направлении судебных актов участникам судопроизводства»[163].

Институт судебного извещения имеет фундаментальное значение при осуществлении правосудия, так как закрепляет в себе нормы, гарантирующие право граждан на получение равных возможностей при защите своих интересов в судебном процессе, обеспечение личного участия в судебном заседании, возможность вовремя отреагировать на незаконно принятое решение с целью обеспечения справедливого правосудия. Однако при внедрении в данный институт новых информационных технологий возникает проблема, которая связана с необеспечением равного доступа населения к различным информационным ресурсам.

В современном мире, где в каждой сфере жизни общества применяются цифровые технологии, услуги, предоставляемые гражданам, также носят цифровой характер, и в связи с этим идет накопление большого объема информации, содержащей данные о гражданах, вплоть до определения геопозиции того или иного лица. Несмотря на такое масштабное использование информационных технологий, во взаимодействии суда и лиц, участвующих в процессе, в процессуальных нормах сохраняется правило о том, что при фактическом неполучении извещения вследствие неизвестности места пребывания лица или отсутствия лица по указанному адресу, оно признается извещенным надлежащим образом.

При этом стоит отметить, в законодательстве не закреплена обязанность суда предпринять все меры по поиску и выяснению надлежащего адреса лица. Данная проблема больше относится к взаимодействию суда с физическими лицами, так как информацию о месте нахождения или регистрации юридического лица возможно получить с помощью специальных сервисов, например таких, как Единая система государственной регистрации юридического лица, которая предоставляет свободный доступ ко всем интересующим данным. В отношении физических лиц намного сложнее

[163] Спицин И.Н. Проблемы транспарентности в гражданском и арбитражном процессе : автореф. дис. ... канд. юрид. наук. Екатеринбург, 2011. С. 12.

получить информацию, так как законодательство тщательно регулирует и защищает персональные данные таких лиц. В результате такого положения возникают некоторые проблемы при регулировании данных правоотношений.

Так, у гражданина появляется возможность злоупотребления своими правами путем указания неверного адреса своего местонахождения или регистрации. Это ведет к сомнениям в законности принятого судебного решения. Как устанавливает ГПК РФ[164], «Основаниями для отмены решения суда первой инстанции в любом случае являются: рассмотрение дела в отсутствие кого-либо из лиц, участвующих в деле и не извещенных надлежащим образом о времени и месте судебного заседания». К тому же, как отмечалось ранее, суд не обязан проверять достоверность указанных лицами адресов, но и не предоставляет возможность свободного поиска достоверных сведений. Также у суда отсутствует обязанность по повторному извещению лиц при неполучении ими извещений в первый раз.

Новые информационные системы, которые активно применяются в деятельности судов, позволяют разместить информацию о прошедших и предстоящих судебных заседаниях и принятых судебных актах. Также такие системы предусматривают функцию по автоматическому уведомлению участников процесса. Стоит отметить, что по сравнению с деятельностью суда по извещению лиц, участвующих в деле, данная система имеет более расширенный функционал по предоставлению информации. Данные системы предоставляют участникам процесса возможность ознакомиться не только с судебными актами, принятыми в ходе судебного разбирательства, но и увидеть каждый этап процессуальных действий, принятых судом. Несмотря на то, что прогресс в области доступности информации очевиден, следует указать некоторые недочеты данной системы.

---

[164] Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 06.04.2024, с изм. от 04.06.2024) // Российская газета. 08.12.1994. № 238–239.

Так, например, при выборе сторонами разных способов извещения, сроки получения необходимой информации будут отличаться, то есть сторона процесса, выбравшая традиционный способ извещения по почте или не имеющая доступа к различным информационным технологиям и системам в силу разных жизненных обстоятельств, будет получать извещения с задержкой. В гражданском судопроизводстве проблема так называемого «цифрового неравенства» также может быть связана с тем, что обязанность по отслеживанию движения дела закреплена только за различными государственными органами и организациями, и тем самым эти лица могут незамедлительно ознакомиться с интересующей их информацией, тогда как граждане, неограниченные в праве ознакомления с материалами дела самостоятельно, тем не менее не все имеют возможность использовать информационные технологии, а поэтому они находятся в ущемленном положении.

Информационные технологии и системы повышают качество, скорость и удобство по отправке судом и при получении участниками процесса электронных судебных извещений. Однако, несмотря на все эти плюсы, данные технологии не могут обеспечить стопроцентную гарантию вручения судебного извещения адресату. Причиной такого невручения может быть не только отказ или нежелание лица в получении извещения, но причина может не зависеть от воли лица. Например, к таким причинам могут относиться сбой в сети или некорректная работа оператора связи, сбой в работе техники или несанкционированный доступ иных лиц к телефонным данным гражданина[165].

Для решения данной проблемы необходимо применить комплексный подход. В мире еще не разработана такая система, которая могла бы обеспечить стопроцентное получение адресатом судебного извещения, к тому же остается нерешенной проблема

[165] Шаньгина С.В. Электронные извещения в гражданском судопроизводстве: проблемы и пути их решения // Молодой ученый. 2024. № 24 (523). С. 415–418. URL: https://moluch.ru/archive/523/115667/ (дата обращения: 23.09.2024).

в различии объема возможностей использования современных технологий и гаджетов гражданами. В законодательстве следует предусмотреть правила, минимизирующие различие и риски при получении судебных извещений. Например, считаем целесообразным внести положение о необходимости направления извещения судом по нескольким каналам связи. Обязать участников процесса указывать резервные адреса электронной почты, мобильного телефона для направления СМС-уведомления, сообщать о наличии личного кабинета на едином портале государственных и муниципальных услуг. Также для повышения вероятности получения извещения предлагается предусмотреть возможность указания лицом, участвующим в деле, доверенного лица, который в случае его длительного отсутствия будет управомочен получать информацию по делу.

Активное внедрение и использование новых технологий при использовании судебных извещений оказывает положительное влияние на работу судебных органов, однако наличие некоторых пробелов в законодательстве в области регулирования вопроса об извещениях создает противоречия. Очевидно, что идет рост технических возможностей по поиску, обработке достоверности информации, возрастает процент фактического извещения граждан, но несмотря на это, бремя и риски по получению соответствующей информации перекладываются на стороны.

Исходя из этого, как уже указывалось, находим нужным и целесообразным установить в гражданском, арбитражном и административном судопроизводстве принцип доступности информации в процессе, который гарантировал бы право быть извещенным о дате и времени судебного заседания, иметь доступ к информации о ходе движения дела, знать о вынесенных судебных актах, выбирать способ извещения: электронный или традиционный по почте; указать дополнительные адреса, на которые будет возможность направить соответствующее извещение.

Однако реализовать данный принцип только за счет осуществления прав будет невозможно. Необходимо также предусмотреть соответствующие обязанности, которые позволят осуществить

права, закрепляемые данным принципом в полном объеме. Одной из таких обязанностей может являться необходимость в незамедлительном информировании суда о смене места проживания или регистрации участника процесса. А в отношении электронного извещения – обязанность сообщить суду о смене номера телефона или адреса электронной почты.

Переход на цифровые рельсы и становление информационного общества само по себе не предполагает, что любой член общества обладает равными возможностями по использованию техники и доступом к новым технологиям. Для того, чтобы такое неравенство не повлияло на реализацию принципа доступности информации, необходимо закрепить обязанность суда учитывать такое различие при использовании технических средств связи.

Никишин Владимир Дмитриевич,

канд. юрид. наук, доцент кафедры информационного права и цифровых технологий, директор Института информационной и медиабезопасности Университета имени О.Е. Кутафина (МГЮА), г. Москва

ПРОТИВОДЕЙСТВИЕ ДЕСТРУКТИВНОМУ КОНТЕНТУ КАК НАПРАВЛЕНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Понятие «деструктивный контент» не закреплено в действующем законодательстве, хотя и прижилось в доктрине и в практической деятельности. Различные словосочетания, связанные с деструктивным контентом и деструктивным информационно-психологическим воздействием, уже содержатся в ряде документов стратегического планирования и иных документов:

– Стратегия национальной безопасности Российской Федерации[166];

[166] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 02.07.2021 № 400 // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

– Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей[167];

– Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года[168];

– Стратегия реализации молодежной политики в Российской Федерации на период до 2030 года[169];

– Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024 – 2028 годы[170];

– Распоряжение Правительства РФ «Об утверждении Перечня иностранных государств, реализующих политику, навязывающую деструктивные неолиберальные идеологические установки, противоречащие традиционным российским духовно-нравственным ценностям»[171];

– Модельный закон ОДКБ «Об обеспечении национальной безопасности»[172].

---

[167] Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей : Указ Президента РФ от 09.11.2022 № 809 // СЗ РФ. 2022. № 46, ст. 7977.

[168] О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года : Указ Президента РФ от 17.05.2023 № 358 // СЗ РФ. 2023. № 21, ст. 3696.

[169] Об утверждении Стратегии реализации молодежной политики в Российской Федерации на период до 2030 года : распоряжение Правительства РФ от 17.08.2024 № 2233-р // СЗ РФ. 2024. № 36, ст. 5484.

[170] Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024–2028 годы, утвержденный Президентом РФ 30.12.2023 № Пр-2610 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[171] Об утверждении Перечня иностранных государств, реализующих политику, навязывающую деструктивные неолиберальные идеологические установки, противоречащие традиционным российским духовно-нравственным ценностям : распоряжение Правительства РФ от 17.09.2024 № 2560-р // СЗ РФ. 2024. № 39, ст. 5838.

[172] Модельный закон ОДКБ «Об обеспечении национальной безопасности». Принят в г. Москве 30.10.2018 Постановлением 11-3.1 Парламентской Ассамблеи Организации Договора о коллективной безопасности // Сайт Парламентской Ассамблеи Организации Договора о коллективной безопасности. URL: https://paodkb.org/ (дата обращения: 22.09.2024).

Системный анализ документов стратегического планирования, а также Модельного закона ОДКБ показывает, что понятия «деструктивный контент», «деструктивное поведение», «деструктивная идеология», «деструктивное информационное воздействие» используются в контексте проблем противодействия распространению информации, причиняющей вред здоровью или развитию. Между тем в российском законодательстве отсутствует определение или даже упоминание понятия «деструктивный контент» («деструктивная информация»), на страницах юридической литературы до сих пор не сформировалось единых подходов к пониманию категории «деструктивный контент». Более того, наряду с понятием «деструктивный контент» исследователи используют понятия «вредная/вредоносная информация», «токсичный контент» и т.п.

В настоящее время российское законодательство использует только понятие «информации, ограниченной или запрещенной к распространению», что не охватывает всю сущность деструктивного характера контента в сети «Интернет» и исключает его из правовой квалификации (не все виды деструктивной информации подпадают под запрет в рамках действующего законодательства), что позволяет лицам, сознательно распространяющим вредоносную информацию в цифровой среде, уходить от юридической ответственности.

Кроме того, законодательство устанавливает запреты (ограничения) на распространение информации, не только деструктивно влияющей на мировоззрение граждан, склоняющей их к делинквентному поведению и т.п., но и на распространение информации, распространяемой с нарушением авторских и (или) смежных прав; информации, распространяемой с нарушением требований законодательства о выборах и референдумах и др. Соответственно, понятия «деструктивный контент» и «противоправный контент» являются именно пересекающимися по объему и содержанию понятиями.

На наш взгляд, необходимо закрепление в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[173] (далее – ФЗ об информации)

[173] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. 2006. № 31 (ч. I), ст. 3448.

понятия ***деструктивной информации (деструктивного контента)***, *под которой, на наш взгляд, необходимо понимать информацию, направленную на формирование представлений о допустимости и (или) необходимости девиантного поведения, пренебрежительного или отрицательного отношения к правам и свободам человека и гражданина, к традиционным российским духовно-нравственным ценностям.*

Институтом информационной и медиабезопасности МГЮА и представителями кафедры информационного права и цифровых технологий МГЮА (авторский коллектив: Никишин В.Д, Минбалеев А.В., Грищенко Г.А.) было проведено в 2024 году исследование проблем противодействия деструктивному контенту. Указанное исследование передано в Государственную Думу, и с учётом их результатов начата разработка пакета законопроектов в рамках Межфракционной рабочей группы по законодательной реализации государственной политики в сфере сохранения и укрепления традиционных российских духовно-нравственных ценностей.

Анализ действующей системы правового обеспечения противодействия деструктивному контенту и актуальных угроз медиабезопасности позволил заключить, что, во-первых, действующее законодательство охватывает не все актуальные контент-угрозы деструктивного информационного воздействия. Соответственно, принятие решений о запрете распространения конкретных информационных материалов происходит по формальным признакам, реагирование на угрозы распространения новых видов деструктивной информации требует значительного времени, в т.ч. из-за длительной процедуры законодательных инициатив, закрепляющих новые виды информации, запрещенной к распространению. Таким образом, целесообразно внесение в законодательство комплексного собирательного понятия для видов информации, оказывающей деструктивное информационно-психологическое воздействие.

Необходимо сломить практику принятия мер только на этапе, когда происходит прямое обоснование или оправдание радикальной деятельности, осуществляются призывы к ней и т.п., т.к. это уже запоздалые меры в отношении лиц или ресурсов, малая доля которых

выявляется в силу закрытого характера сообществ, а также перехода этих сообществ в сегмент Даркнета. За пределами досягаемости правовых мер сейчас находится широчайший пласт деструктивной информации, формально не подпадающей под действующие запреты, но направленной на нормализацию насилия, ненависти, романтизацию культа жестокости, распространение человеконенавистнических идей, антисемейных ценностей и т.д. Требуется не только введение в законодательство обобщающего понятия деструктивного контента, но и установление прозрачных принципов и критериев отнесения к нему, т.к. должен быть обеспечен баланс свободы слова и её ограничения для защиты прав иных лиц, их защиты от деструктивного информационно-психологического воздействия.

В экспертно-аналитическом исследовании проблем противодействия деструктивному контенту обоснована необходимость внесения системных изменений в законодательство в целях противодействия распространению деструктивного контента.

Во-первых, предлагается законодательно закрепить понятие деструктивной информации и порядок ограничения доступа к ней, а также предусмотреть порядок отнесения информации к деструктивной, для чего необходимо внесение изменений в Федеральные законы «Об информации, информационных технологиях и о защите информации», «О защите детей от информации, причиняющей вред их здоровью и развитию», а также в ряд подзаконных актов.

Во-вторых, предложены инициативы по совершенствованию противодействия распространению деструктивной информации отдельных, особо опасных, видов. Так, например, предложено предусмотреть возможность внесудебной блокировки информации, направленной на пропаганду самоубийства; информации, содержащей пропаганду наркотических средств и психотропных веществ, а также направленной на формирование представлений о привлекательности и (или) допустимости наркоторговли и др.

В-третьих, предлагается создать Экспертный центр по противодействию деструктивной информации, к компетенции которого отнести функцию по определению новых видов деструктивной

информации с целью признания ее запрещенной в установленном порядке. Данный Экспертный центр должен осуществлять в том числе функцию головного экспертного учреждения – методического центра, вырабатывающего унифицированные подходы к анализу и правовой оценке потенциально деструктивных информационных материалов уполномоченными Правительством РФ федеральными органами исполнительной власти.

В-четвертых, определяется комплекс мер по совершенствованию правовых и организационно-технических механизмов, направленных на защиту от деструктивного контента (пересмотр системы регистрации в социальных сетях и направления жалоб на обнаруженную вредоносную информацию в социальной сети, запрет на применение рекомендательных технологий в детских профилях (аккаунтах) и ряд других).

В рамках исследования проведен анализ зарубежных практик противодействия распространению противоправной информации, в т.ч. опыт Европейского союза, Франции, Германии, Великобритании, Китая, Японии, Южной Кореи, Сингапура, США, Турции. Как показало исследование, во-первых, ни в одной из стран не закреплено комплексное понятие деструктивного контента, а во-вторых, ни одна из этих практик не является совершенной или в связи с фрагментарным, несистемным подходом к закреплению видов противоправной информации и критериев ее определения, или в связи с фактическим отсутствием четких критериев к определению противоправности и широким усмотрением органов государственной власти, что приводит к фактической цензуре и нарушениям свободы слова.

В исследовании МГЮА изложена уникальная нормативная модель, призванная обеспечить противодействие деструктивному контенту при сохранении демократических принципов, баланса права на свободу слова и защиты иных прав.

Огальцева Ольга Юрьевна,

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

НАЛОГОВАЯ ТАЙНА КАК СРЕДСТВО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАЛОГОПЛАТЕЛЬЩИКОВ

Институт налоговой тайны как разновидности конфиденциальной информации регулируется законодательством весьма лаконично. Условия отнесения конфиденциальной информации к сведениям, составляющим налоговую тайну, установлены Налоговым кодексом Российской Федерации (далее по тексту – НК РФ). Согласно подп. 13 п. 1 ст. 21 во взаимосвязи с пп. 2 и 3 ст. 21, п. 2 ст. 24 НК РФ к таким сведениям относится информация, касающаяся не только налогоплательщиков, но и плательщиков сборов, страховых взносов и налоговых агентов (далее для удобства изложения все эти лица будут именоваться налогоплательщиками).

Налоговую тайну составляют любые сведения о налогоплательщике, которые получены налоговыми инспекциями и иными государственными органами. При этом список иных государственных органов, обладающих конфиденциальной информацией о налогоплательщике в названной статье ограничен. К ним относятся органы внутренних дел, следственные органы, органы государственного внебюджетного фонда и таможенные органы.

В 2004 г. режим налоговой тайны стал предметом рассмотрения Конституционного Суда РФ. Суд отметил, что специальный правовой статус сведений, составляющих налоговую тайну, закреплен ст. 102 НК РФ исходя из интересов налогоплательщиков и с учетом соблюдения принципа баланса публичных и частных интересов в указанной сфере, поскольку в процессе осуществления налоговыми органами Российской Федерации своих функций, установленных НК РФ и иными федеральными законами, в их распоряжении

оказывается значительный объем информации об имущественном состоянии каждого налогоплательщика, распространение которой может причинить ущерб как интересам отдельных граждан, частная жизнь которых является неприкосновенной и охраняется законом, так и юридических лиц, чьи коммерческие и иные интересы могут быть нарушены в случае произвольного распространения в конкурентной или криминальной среде значимой для бизнеса конфиденциальной информации.

Поэтому федеральное законодательство предусматривает ограниченный режим доступа к такой информации путем установления исчерпывающего перечня субъектов, обладающих в силу закона правом обращения к налоговым органам за предоставлением сведений, составляющих налоговую тайну, в указанных в законе целях[174].

Порядок доступа государственных органов и иных лиц к конфиденциальной информации налоговых органов, в том числе составляющих налоговую тайну, установлен Приказом Федеральной налоговой службы. Такая информация предоставляется только на основании запроса, оформленного по соответствующей форме[175].

Однако в некоторых случаях налоговый орган обязан передавать сведения, составляющие налоговую тайну. Например, по запросу полиции или судей[176]. Или запросить у налогового органа сведения о банковских счетах должника и другую информацию, указанную в части 9 статьи 69 Федерального закона об исполнительном производстве, может взыскатель, у которого есть исполнительный лист, срок предъявления которого не истек[177].

---

[174] Определение Конституционного Суда Российской Федерации от 30 сентября 2004 года № 317-О.

[175] Об утверждении Порядка доступа к конфиденциальной информации налоговых органов : приказ МНС РФ от 03.03.2003 № БГ-3-28/96.

[176] Подпункт 29 части 1 статьи 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции»; часть 6 статьи 1 Закона РФ от 26.06.1992 № 3132-1 «О статусе судей в Российской Федерации».

[177] Часть 8 статьи 69 Федерального закона от 02.10.2007 № 229-ФЗ «Об исполнительном производстве»; Письмо ФНС России от 10.04.2014 № СА-4-14/6708@).

Для определения принадлежности сведений к информации, составляющей налоговую тайну, используется их общее описание с перечислением общих признаков и установление закрытого перечня данных, которые к такой информации не относятся. В частности, к налоговой тайне не относятся сведения об идентификационном номере налогоплательщика, данные бухгалтерской (финансовой) отчетности, о среднесписочной численности работников, а также о нарушениях налогового законодательства и мерах ответственности за них[178].

Также к налоговой тайне относится коммерческая тайна, к которой налоговое законодательство отнесло исключительно секреты производства (ноу-хау), т.е. производственные, технические, экономические, организационные сведения, о результатах интеллектуальной деятельности в научно-технической сфере, о способах ведения профессиональной деятельности, в отношении которых их обладатель ввёл режим коммерческой тайны[179].

Вопросы правового регулирования налоговой тайны не раз становились предметом исследования ученых-юристов[180]. Однако в последние несколько лет в данном институте налогового права произошли серьезные изменения.

В частности, на сайте ФНС России запущен и действует электронный сервис «Прозрачный бизнес», который содержит сведения, еще недавно составлявшие налоговую тайну.

Данный сервис был разработан для бизнеса с целью самостоятельной проверки своих контрагентов. В последнее время инспекции все чаще предъявляют компаниям и предпринимателям претензии в связи с тем, что они ненадлежащим образом выполняют

---

[178] Пункт 1 статьи 102 НК РФ.

[179] Пункт 2 статьи 102 НК РФ; пункт 2 статьи 3 Федерального закона от 29 июля 2004 г. № 98 «О коммерческой тайне»; статья 1465 Гражданского кодекса РФ.

[180] Кирилина В.Е. Правовой режим налоговой тайны // Законы России: опыт, анализ практика. 2010. № 4. С. 79–84; Крохина Ю.А. Принципы определения налоговой тайны в законодательстве России и зарубежных стран // Финансовое право. 2015. № 8. С. 26–30.

требование о проявлении должной осмотрительности при выборе своих контрагентов. И в результате по итогам проверок доначисляют налоги к уплате в бюджет, штрафы и пени.

Понятие "должная осмотрительность" появилось в 2006 году из позиции, изложенной в постановлении Пленума Высшего Арбитражного Суда Российской Федерации[181]. На сегодня под данным понятием понимается комплекс действий налогоплательщика, который позволяет ему убедиться в том, что его контрагент ведет реальную деятельность, и есть основания полагать, что он способен выполнить условия договора без рисков как для налогоплательщика, так и для бюджета[182].

До запуска электронного сервиса "Прозрачный бизнес" уже существовали иные системы для проверки контрагентов – "СПАРК", "Прима-Информ", "Интегрум", "Контур", "Фокус", "СБИС" и др. Однако доступ ко всем перечисленным системам является платным в отличие от сервиса ФНС России.

В 2024 году более 652 млн запросов направлено в сервис "Прозрачный бизнес"[183].

Как сказано на сайте ФНС России, сервис "Прозрачный бизнес" позволяет получить полную информацию о налогоплательщике-организации, среди которых идентификационный номер налогоплательщика (ИНН), а также сведения об основном виде деятельности и уставном капитале организаций, об адресе организации и наличии информации о недостоверности указанного адреса, о включении организации в реестр субъектов малого и среднего

---

[181] Об оценке Арбитражными судами обоснованности получения налогоплательщиком налоговой выгоды : постановление Пленума ВАС РФ от 12.10.2006 № 53.

[182] Письма ФНС от 10.10.2022 № БВ-4-7/13450@, от 10.03.2021 № БВ-4-7/3060@, от 31.10.2017 № ЕД-4-9/22123@; Обзор практики, утв. Президиумом ВС 13.12.2023; п. 20 Обзора судебной практики ВС № 1, утв. Президиумом ВС 01.06.2022; п. 39 Обзора судебной практики ВС № 3, утв. Президиумом ВС 10.11.2021.

[183] Информация с официального сайта ФНС России. URL: https://www.nalog.gov.ru

предпринимательства, о наличии недостоверных сведений об органах управления организаций, о многократном участии органов управления организаций в других компаниях, о публикации сообщений в журнале "Вестник государственной регистрации".

Еще одни серьезные изменения в институте налоговой тайны связаны с возможностью раскрытия информации с согласия их обладателя.

Изначально в соответствии с пунктом 4 статьи 31 и подпунктом 1 пункта 1 статьи 102 Налогового кодекса Российской Федерации организации были вправе раскрыть дополнительную информацию о себе, т.е. признать все сведения или их часть общедоступными. Для этого необходимо заполнить специальную форму согласия[184], данная форма действовала до 13 декабря 2022 года. Представляется, что таким правом налогоплательщики могут воспользоваться, чтобы выглядеть более привлекательными в глазах своих партнеров по бизнесу.

Впоследствии с 1 августа 2022 года в статью 102 НК РФ введено положение, согласно которому с согласия налогоплательщика сведения о них могут быть не только признаны общедоступными, но и переданы налоговыми органами иному лицу[185].

С 13 декабря 2022 года действует новый Порядок предоставления такого согласия и формы их заполнения. При этом налогоплательщик может дать согласие на раскрытие не всех сведений о нем, а только части и только за определенный период[186]. Соответственно, получить иное лицо сможет только эти разрешенные сведения. К остальным доступ будет закрыт.

---

[184] Об утверждении формы, формата согласия налогоплательщика (плательщика страховых взносов) на признание сведений, составляющих налоговую тайну, общедоступными, порядка заполнения формы, а также порядка его представления в налоговые органы : приказ ФНС России от 15 ноября 2016 г. № ММВ-7-17/615@.

[185] Пункт 2.3 статьи 102 НК РФ.

[186] Приказ ФНС России от 14.11.2022 N ЕД-7-19/1085@ "Об утверждении документов, предусмотренных подпунктом 1 пункта 1 и пунктом 2.3 статьи 102 Налогового кодекса Российской Федерации"

Кроме того, проверить контрагентов и предоставить им информацию о себе налогоплательщик может в личном кабинете на сайте ФНС. В разделе "Как меня видит налоговая" собраны показатели финансово-хозяйственной деятельности налогоплательщика, которые можно предоставить партнерам. Для этого надо просто добавить контрагента в "друзья". Если налогоплательщик захочет увидеть и данные контрагента, то надо просто "постучаться" в его личный кабинет и получить подтверждение запроса[187] (Информация ФНС России).

Подводя итоги, следует отметить, что с каждым годом все меньше информации подлежит охране в качестве налоговой тайны. Причина видится в том, что государство определило для себя сделать бизнес абсолютно прозрачным.

С одной стороны, доступность большого объема сведений о налогоплательщике и его деятельности – это повышение гарантий соблюдения законодательства о налогах и сборах налогоплательщиками, снижение рисков применения ими различных схем уклонения от уплаты налогов и в конечном итоге – рост налоговых отчислений.

С другой стороны, публикование некоторых сведений, например, о доначисленных суммах по налоговым проверкам, создаёт негативное мнение у контрагентов, что может привести к потере партнера по бизнесу. Хотя наличие такой недоимки может оказаться неправомерной, поскольку решения о привлечении (об отказе привлечения) к ответственности за совершение налоговых правонарушений в дальнейшем могут быть обжалованы в вышестоящем налоговом органе и в судебных инстанциях, и решение может быть вынесено в пользу налогоплательщика.

И в заключение хочется отметить, что с 1 января 2019 года налоговые органы также получили возможность истребовать документы (информацию), служащие основаниями для исчисления и уплаты (удержания, перечисления) налога (сбора, страховых взносов) у аудиторских организаций и индивидуальных аудиторов[188]. Следовательно, и аудиторская тайна не удержала своих позиций.

---

[187] <Информация> ФНС России "В личных кабинетах ЮЛ и ИП теперь можно найти информацию о показателях финансово-хозяйственной деятельности контрагентов".

[188] Статья 93.2 НК РФ.

Пашнина Татьяна Викторовна,

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

О НЕКОТОРЫХ АСПЕКТАХ ПРОТИВОДЕЙСТВИЯ АКТУАЛЬНЫМ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В ЦИФРОВОЙ СРЕДЕ

Научно-технологические достижения начала XXI в. обусловили появление и активное внедрение во все сферы жизни т.н. «сквозных» цифровых технологий, перечень которых был закреплен распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы "Цифровая экономика Российской Федерации"»[189].

Указанный документ к их числу отнес технологии больших данных, нейротехнологии и искусственный интеллект, системы распределенного реестра, квантовые технологии и ряд других.

Названные технологии не только стали катализатором инновационного развития страны и ключевых отраслей жизнедеятельности, но и сделали жизнь рядового человека гораздо комфортнее за счет предоставления публичных услуг в режиме «одного окна» 24/7, развития маркетплейсов, разнообразных цифровых сервисов и продуктов.

Однако, как и любое иное достижение научной мысли, сквозные цифровые технологии принесли новые риски и угрозы, наибольшую опасность представляющие для самого уязвимого субъекта правоотношений – человека.

[189] Об утверждении программы «Цифровая экономика Российской Федерации» : распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 27.03.2025).

Проблема обеспечения информационной безопасности личности в цифровой среде сложна и многогранна, поэтому коснемся лишь некоторых ее аспектов. Среди актуальных киберугроз считаем необходимым выделить:

1. *Возрастание рисков стать жертвой киберпреступления.* Так, по данным МВД России, в 2024 году в стране зафиксированы 765,4 тыс. преступлений, совершенных с использованием ИТ-технологий, что составляет примерно 40 % от общего числа противоправных деяний.

В отчете ведомства говорится, что в 2024 г. общее количество киберпреступлений в России увеличилось на 13,1 % по сравнению с предыдущим годом. Так, в ИТ-сфере совершены 369,3 тыс. тяжких и особо тяжких противоправных деяний. При этом среди ИТ-преступлений самый большой удельный вес приходится на *кибермошенничество* (40 %)[190].

Стабильно высокий уровень среди противоправных деяний демонстрирует и *кибераграссия* в различных формах – от хулиганства до доведения до самоубийства. Исследования показывают, что с этим явлением сталкивались более половины пользователей российских социальных сетей[191].

Особую опасность кибербуллинг представляет для подростков, для которых «ситуация переживания травли в Интернет-пространстве связана с широким спектром проблем психического здоровья и поведения… – депрессией, тревогой, низкой самооценкой, <…> формированием суицидального поведения»[192].

---

[190] Число киберпреступлений в России // TADVISER. Государство. Бизнес. Технологии. 2025. 24 янв. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 27.03.2025).

[191] Акимова Е. 57 % россиян сталкивались с кибербуллингом. Почему это проблема. Как люди ведут себя и что может помочь // РБК life. 2023. 10 ноября. URL: https://www.rbc.ru/life/news/654dfdeb9a79472d91e62168 (дата обращения: 27.03.2025).

[192] Карауш И.С., Куприянова И.Е., Кузнецова А.А. Кибербуллинг и суицидальное поведение подростков // Суицидология. 2020. № 1 (38). С. 117.

Соответственно, кибербуллинг в условиях снижения рождаемости представляет серьезную угрозу человеческому капиталу страны.

2. *Увеличение количества случаев использования дипфейков как средства совершения преступных деяний.* Эксперты отмечают, что «изначально дипфейк определялся как использование искусственного интеллекта для модификации карты лиц для создания новых реалистичных изображений... Сегодня технология дипфейк позволяет создавать аудио- или видеоматериалы с использованием голоса и (или) изображения другого человека. Использование данной технологии доступно любому владельцу смартфона, который с помощью нескольких приложений <…> может создать дипфейк за короткий промежуток времени… Технологии глубокого синтеза уже сейчас применяются для совершения мошенничества, вымогательства, изготовления порнографии, распространения заведомо ложной общественно значимой информации и т.д.»[193].

Таким образом, технология дипфейков, изначально трудоемкая и достаточно редко используемая, в основном – против публичных личностей, сегодня значительно удешевилась и широкого используется против рядовых граждан.

3. *Манипулирование массовым сознанием и общественным мнением путем распространения недостоверных (фейковых) новостей.* Эксперты отмечают, что «сегодня фейковые новости сопровождают любую сенсационную информацию или значимое событие... Они способны и нацелены на провоцирование страха и паники среди населения, распространение слухов и дестабилизацию внутриполитической обстановки. Эпоха цифровизации позволяет использовать фейки в политической сфере как инструмент информационной войны»[194].

---

[193] Ефремова М.А., Русскевич Е.А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. № 2 (56). С. 98.

[194] Григорян Д.К. Фейковые новости в эпоху цифроизации: технологии противодействия распространению // Юристъ-Правоведъ. 2024. № 3 (110). С. 133.

Примерами вышесказанного могут служить: произошедшее в 2023 г. нападение на аэропорт Махачкалы[195], поджог банкоматов в декабре 2024 г.[196] и пр., на практике подтверждающие, что манипулирование массовым сознанием представляет угрозу основам конституционного строя и создает значительный риск вовлечения граждан в совершение тяжких и особо тяжких преступлений.

4. *Стабильно высокий уровень утечек персональных данных*.

Так, в I квартале 2025 года произошло, по разным оценкам, от 37 до 46 утечек данных россиян. По данным сервиса разведки уязвимостей и утечек данных DLBI их общий объем составил около 21,5 млн уникальных телефонных номеров и 17 млн адресов электронной почты. По количеству утечек лидирует сегмент логистических компаний… В начале прошлого года лидерами были финансовые организации, чьи крупные утечки затронули 145 млн телефонных номеров и 51 млн e-mail их клиентов[197].

Проблема недостаточного уровня защиты персональных данных также усугубляется низкой цифровой грамотностью граждан, следствием которой является несоблюдение цифровой гигиены, приводящей к возрастанию утечек информации, составляющей личную и семейную тайну.

5. *Психологическая неготовность принимать реалии, диктуемые сквозными цифровыми технологиями.* Данная проблема находит осмысление в работах председателя Конституционного Суда РФ, который отмечает: «Исследователи еще в самом начале эры

---

[195] В Дагестане вынесены приговоры 240 участникам погромов в аэропорту Махачкалы // Ведомости. 2023. 1 дек. URL: https://www.vedomosti.ru/society/news/2023/12/01/1008985-uchastnikam-pogromov (дата обращения: 27.03.2025).

[196] За десятками поджогов банкоматов по всей стране стоят украинские спецслужбы // RG.RU. 2024. 22 дек. URL: https://rg.ru/2024/12/22/reg-szfo/pozharnaia-komanda-ot-kogo.html (дата обращения: 27.03.2025).

[197] Штурма Я. Знания слили: с начала года произошло почти 50 крупных утечек данных. Владельцы ботов начали массово скупать базы с персональной информацией о россиянах // Известия. 2025. 25 апр. URL: https://iz.ru/1876355/iana-shturma/znaniya-slili-s-nachala-goda-proizoshlo-pochti-50-krupnyh-utechek-dannyh (дата обращения: 27.03.2025).

Интернета <…> говорили о фрустрации людей, не успевающих воспринять в своём сознании стремительно меняющийся мир… Первый риск для современной цивилизации права в условиях грядущего цифрового будущего – это растерянность человека и общества, обусловленная изменением способов коммуникации и связанной с этим постмодернистской атомизацией общества»[198].

Особо В.Д. Зорькин отмечает опасность технологии искусственного интеллекта, который уже сегодня «способен осуществлять действия, ведущие к множеству социально и юридически значимых результатов, может изменять эмоциональную динамику межчеловеческого взаимодействия, развивать зависимость от использования приложений, которые предлагают нереальный, но приносящий удовлетворение опыт»[199].

Главную опасность искусственного интеллекта председатель Конституционного Суда РФ видит в попытках его субъективации, в идее «наделения искусственного интеллекта личным статусом»[200].

Справедливость позиции председателя высшего судебного органа подтверждают исследования психологов о феномене возникновения у людей романтических квази-отношений с искусственным интеллектом.

Дружеские или романтические отношения с искусственным интеллектом – относительно новое явление, поэтому <…> мнения в среде психологов бытуют разные: что таким образом человек может решить проблемы одиночества и неуверенности в себе, или же что это приведет к усилению социальной изоляции, замыканию в своем внутреннем мире, – отмечает практический психолог, член ассоциации когнитивно-поведенческих психотерапевтов Т. Сушкова, мнение которой приводит зарубежное издание[201].

---

[198] Зорькин В.Д. Лекции о праве и государстве. СПб. : Конституционный Суд Российской Федерации, 2024. С. 249.

[199] Там же. С. 255.

[200] Там же. С. 264.

[201] Роман с виртуальным разумом // TRT на русском. 2024. 1 марта. URL: https://www.trtrussian.com/tehnologii/roman-s-virtualnym-razumom-17185157 (дата обращения: 27.03.2025).

Приведенное выше свидетельствует о том, что цифровые технологии способны представлять не только информационную, но и психологическую угрозу личности, не обладающей достаточными компетенциями и готовностью для взаимодействия с ними.

В свете вышесказанного считаем необходимым подвести некоторые итоги:

1. Отметить ключевую роль государства в обеспечении информационной безопасности личности, которая в последнее время усиливается. В данном контексте необходимо рассматривать появление ряда актов, направленных на защиту личности в киберсреде: принятие закона о защите от кибермошенничества[202], разработки законопроектов о профилактике кибербуллинга[203]; внесение изменения в статью 63 Уголовного кодекса РФ в части повышения ответственности за преступления, совершаемые с применением технологий искусственного интеллекта[204].

Тем не менее одних усилий законодателей в плане усиления мер противодействия информационным угрозам недостаточно.

2. Полагаем, что законодательный компонент противодействия киберугрозам должен дополниться индивидуальным правовым регулированием посредством выработки соответствующих позиций высшими судебными органами. В настоящее время указанные органы преимущественно занимаются анализом соответствующих эмпирических данных и теоретическим осмыслением влияния технологий на правоотношения.

---

[202] О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 01 апреля 2025 г. № 41-ФЗ // СЗ РФ. 2025. № 14, ст. 1574.

[203] В Госдуме рассказали, как будет работать закон о буллинге // Парламентская газета. 2025. 28 янв. URL: https://www.pnp.ru/social/v-gosdume-rasskazali-kak-budet-rabotat-zakon-o-bullinge.html (дата обращения: 27.03.2025).

[204] О внесении изменения в статью 63 Уголовного кодекса Российской Федерации : законопроект № 885494-8. URL: https://sozd.duma.gov.ru/bill/885494-8 (дата обращения: 27.03.2025).

Однако появляются первые правовые позиции по данному вопросу. Так, в определении № 46-КГ23-6-К6 Верховный Суд РФ признал кредитный договор, заключенный от имени клиента путем его обмана третьими лицами с использованием мобильного приложения банка, ничтожным[205].

3. На наш взгляд, правовые и организационно-технические меры, предлагаемые государством, должны дополняться шагами, направленными на формирование устойчивой психологической готовности граждан реализовать себя в условиях цифровой трансформации в профессиональной и бытовой деятельности и эффективно противостоять противоправным посягательствам в киберсреде.

В данном ключе считаем целесообразным актуализацию «Концепции формирования и развития информационной безопасности граждан Российской Федерации»[206] с учетом вызовов и угроз информационной безопасности личности в цифровой среде, появившихся благодаря широкому распространению сквозных цифровых технологий.

Библиографический список

1. Зорькин В.Д. Лекции о праве и государстве. – Санкт-Петербург : Конституционный Суд Российской Федерации, 2024. – 353 с.

2. Григорян Д.К. Фейковые новости в эпоху цифроизации: технологии противодействия распространению // Юристъ-Правоведъ. – 2024. – № 3 (110). – С. 132–136.

3. Ефремова М.А., Русскевич Е.А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. – 2024. – № 2 (56). – С. 97–105.

4. Карауш И.С., Куприянова И.Е., Кузнецова А.А. Кибербуллинг и суицидальное поведение подростков // Суицидология. – 2020. – № 1 (38). – С. 117–129.

[205] Определение СК по гражданским делам Верховного Суда РФ от 18 июля 2023 г. № 46-КГ23-6-К6. URL: https://www.garant.ru/products/ipo/prime/doc/407421033/ (дата обращения: 27.03.2025).

[206] О Концепции формирования и развития культуры информационной безопасности граждан РФ: Распоряжение Правительства РФ от 22 декабря 2022 г. № 4088-р // СЗ РФ. 2022. № 52, ст. 9726.

Смолин Дмитрий Владимирович,

аспирант 1 года обучения Казанского инновационного университета имени В.Г. Тимирясова (ИЭУП).
Научный руководитель: К.Л. Томашевский, д-р юрид. наук, профессор, профессор кафедры гражданского и предпринимательского права Казанского инновационного университета имени В.Г. Тимирясова (ИЭУП),
г. Казань

ПРАВОВЫЕ И ЭТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИИ В ЦИФРОВОЙ СРЕДЕ

Ввиду широкого развития цифровой среды изобретение механизма автоматической генерации на основе данных, выгруженных в сеть «Интернет», и машинного обучения привело к созданию такой цифровой технологии, как искусственный интеллект (далее – ИИ). ИИ представляет собой базу знаний, которая на основе самостоятельного обучения приобретает возможность генерации логических алгоритмов и структур, такая генерация раскрывается в создании обособленных текстов, объектов творчества, анализа данных и т.д, а также позволяет получить ответы на конкретные вопросы, не тратя времени на поиски информации. Сгенерированные ответы не всегда являются достоверными, но развитие данной сферы идет широкими шагами, тем самым открывает новые «двери» в развитии информационного общества.

В связи с чем встает вопрос о том, на что способен ИИ в сфере цифрового развития и регулирования прав на цифровой контент. ИИ предполагает собой автоматическое обучение без участия человека, тем самым внимание человека как никогда важно. Чтобы ИИ, ввиду неправильных алгоритмов, не стал распространять ложную или недостоверную информацию, проявлял признаки дискриминации, потому в России был создан Альянс в сфере ИИ.

Кодекс этики, установленный данным Альянсом в сфере ИИ, выносит главные положения[207]:

1) главный приоритет развития технологий ИИ в защите интересов прав людей и отдельного человека;

2) необходимо осознавать ответственность при создании и использовании ИИ;

3) ответственность за последствия применения ИИ всегда несет человек;

4) технологии ИИ нужно применять по назначению и внедрять там, где это принесет пользу людям;

5) интересы развития технологий ИИ выше интересов конкуренции;

6) важна максимальная прозрачность и правдивость в информировании об уровне развития технологий ИИ, их возможностях и рисках.

Данный кодекс был принят на первом Международном форуме «Этика искусственного интеллекта: начало доверия» в 2021 г.

Цифровой контент представляет собой информацию, созданную и распространённую в цифровой среде. Контент существует в виде текста, изображений, аудио-, аудиовизуального элементов. Процесс создания контента представляет собой сложную последовательность этапов, начиная от зарождения идеи и заканчивая её реализацией. Традиционный способ создания контента требует специализированные программы, сервисы и творческое участие автора. Однако с развитием технологий ИИ все больше забирает на себя ключевые этапы работы, автоматизируя генерацию контента и изменяя сам подход к его созданию.

Правовое регулирование создания контента с использованием ИИ базируется на положениях Гражданского кодекса Российской Федерации (далее – ГК РФ) об авторском праве, хотя непосредственно ИИ в нормах ГК РФ не упоминается.

---

[207] Официальный сайт Национальной стратегии развития искусственного интеллекта в Российской Федерации : [Электронный ресурс]. URL: https://ai.gov.ru/ai/regulatory/ (дата обращения: 10.03.2025).

Определение авторства дается в статье 1257 ГК РФ: автором произведения науки, литературы или искусства признается гражданин, творческим трудом которого оно создано. Статья 1270 ГК РФ «Исключительное право на произведение» гарантирует автору исключительное право на использование произведения любым законным способом[208]. Это означает, что исключительные права на произведения, созданные с применением ИИ, принадлежат человеку (автору), который непосредственно использовал ИИ для их создания. Например, если художник сгенерировал изображение с помощью ИИ, он получает все права на его использование и распространение. Из чего можно предположить, что создание цифрового контента не влияет на правовой статус произведений, созданных с помощью ИИ, в данном случае главную роль играет значение человеческого творчества и участие в процессе создания контента, исключая возможность признания ИИ как автора или правообладателя. Таким образом, ИИ рассматривается как инструмент, находящийся в использовании человека в процессе творческой деятельности.

Исходя из вышесказанного, за контент, выгружаемый в сети «Интернет», ответственен автор – человек, который его создал с использованием ИИ. Для отслеживания правонарушающего контента также можно использовать ИИ. Последний способен выполнять функции анализа, мониторинга и защиты цифрового контента. Современные системы машинного обучения и нейросети позволяют в автоматическом порядке выявлять нарушения, связанные с авторскими правами, отслеживать распространение контента и даже участвовать в разрешении споров.

Ключевым аспектом законодательства является четкое разграничение между результатами интеллектуальной деятельности, созданными ИИ, и теми, что созданы с его использованием. В первом случае ИИ фактически выступает в роли самостоятельного

[208] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 24.03.2022) // Собрание законодательства РФ. 2006. № 52 (1 ч.), ст. 5496.

субъекта, создающего интеллектуальный продукт без участия человека-автора. Именно отсутствие человеческого творческого вклада в процессе создания таких результатов служит основанием для введения специального правового регулирования, включая возможность полного или частичного исключения таких объектов из сферы авторско-правовой охраны.

В то же время это не означает, что разработчики и пользователи ИИ не нуждаются в правовой защите, поскольку создание подобных объектов требует значительных финансовых, организационных и иных затрат. Учитывая отсутствие творческого участия человека, правовая охрана таких результатов должна основываться на принципах, отличных от традиционного авторского права.

Развитие этики в сфере ИИ выходит за рамки абстрактных принципов и теоретических исследований, оказывая непосредственное влияние на совершенствование правовой системы, особенно в отношении актуальных и социально значимых аспектов регулирования ИИ[209].

Этические вопросы в сфере ИИ актуальны не только на уровне отдельных личностей, социальных или общественных групп, но и в масштабах национальных образований и государств. Это подчеркивает необходимость формирования четких этических концепций на национальном уровне.

Эксперты рассматривают этику в сфере ИИ прежде всего как фундаментальную основу и источник законодательных инициатив. Сложность правового регулирования ИИ способствует активному использованию инструментов «мягкого права», включающих в себя и этические нормы. Чаще всего этические принципы находят отражение в рекомендациях и руководствах по развитию технологии в целом.

---

[209] Проблема машинного творчества в системе права: регулирование создания и использования результатов интеллектуальной деятельности с применением искусственного интеллекта, зарубежный опыт и российские перспективы : доклад НИУ ВШЭ / рук. авт. колл. В.О. Калятин. Москва : Издательский дом Высшей школы экономики, 2021.

В западных странах понятие «этика в области ИИ» (AI Ethics) охватывает широкий спектр вопросов, что приводит к его постепенному размыванию и расширению границ обсуждаемых проблем[210]. Это связано с тем, что развитие технологий ИИ затрагивает множество аспектов – от приватности и безопасности данных до социальной справедливости, прозрачности алгоритмов и ответственности за принимаемые решения. В результате дискуссии вокруг этики ИИ часто выходят за рамки чисто технических или правовых вопросов, включая философские, социальные и экономические аспекты.

В то же время среди наиболее целенаправленных инструментов регулирования можно выделить специализированные кодексы в сфере ИИ как общего, так и отраслевого характера. Эти документы призваны установить базовые принципы и стандарты, которые должны соблюдаться при разработке и внедрении ИИ-систем. Например, общие кодексы, такие как «Принципы ИИ» ОЭСР или «Руководящие принципы по этике ИИ» Европейской комиссии, задают универсальные рамки для ответственного использования технологий. В то же время отраслевые кодексы, например, в здравоохранении, финансах или образовании, учитывают специфику конкретных областей и предлагают более детализированные рекомендации[211].

С развитием технологий ИИ и нейросетей открываются новые возможности для создания контента, однако это также усиливает необходимость ответственного подхода к его использованию. Вопросы авторского права, прозрачности и достоверности информации становятся ключевыми аспектами при работе с контентом, созданным с помощью ИИ.

---

[210] Игнатьев А.Г. Этика в области искусственного интеллекта в фокусе междисциплинарных исследований и развития национальных подходов. М., 2022.

[211] Этика в области искусственного интеллекта – от дискуссии к научному обоснованию и практическому применению: аналитический доклад / А.В. Абрамова, А.Г. Игнатьев, М.С. Панова. М. : Издательство «МГИМО-Университет», 2021.

Нейросети выступают исключительно как инструмент, а не как субъект авторского права. Автором контента признается пользователь, который осуществляет контроль над процессом и вносит творческий вклад в его создание. Тем не менее использование результатов, сгенерированных ИИ, особенно в коммерческих целях, требует тщательного анализа правовых и этических аспектов, а также согласования с разработчиками соответствующих технологий.

Особое внимание необходимо уделять проверке фактов, чтобы избежать распространения недостоверной информации и повысить доверие к создаваемому контенту. Это предполагает тщательную перепроверку данных, анализ источников и строгое соблюдение норм законодательства.

Бердышева Светлана Николаевна,

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

ПОДДЕЛКА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В ВУЗЕ ПРИ КОНТРОЛЬНО-НАДЗОРНЫХ МЕРОПРИЯТИЯХ

Одним из центральных федеральных проектов в Российской Федерации в настоящий момент, несомненно, является «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации», который реализуется в рамках государственной программы «Информационное общество». Названный федеральный проект направлен на достижение национальной цели «Цифровая трансформация», основные параметры которой определенны Указом Президента Российской Федерации от 21 июля 2021 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года». В системе образования активно

используются цифровые средства, в том числе электронный документооборот и цифровые проверки.

Контроль и надзор за организациями, осуществляющими образовательную деятельность, осуществляется в форме плановых и внеплановых проверок, а также аккредитационного мониторинга и мониторинга эффективности деятельности вуза.

Однако сегодня неоднократно вузы подают в отчетах заведомо ложную информацию. Минобрнауки было выявлено несколько вузов, которые сфальсифицировали данные в мониторинге эффективности деятельности вузов, при аккредитации были обнаружены подделанные зачетные книжки, информация о составе профессорско-преподавательского состава и т.д.

В декабре 2022 года Минобрнауки выявило «признаки недостоверных данных» в отчётах 73 вузов, получающих федеральное финансирование в рамках госпрограммы «Приоритет-2030». В их число вошли, в частности, МГТУ им. Баумана, РАНХиГС, МИФИ, МГИМО, Нижегородский госуниверситет имени Н.И. Лобачевского, РХТУ им. Менделеева, ДВФК, ВШЭ, МФТИ, МЭИ и Сеченовский университет.

При проверках, аккредитации и лицензировании надзорный орган придерживается строго формального подхода: оцениваются только документы, предоставленные вузом, а не реальное качество образования. Например, по итогам апробации аккредитационного мониторинга в 2022 году выяснилось, что по многим образовательным программам вузы по объективным причинам не смогли предоставить информацию в полном объёме. Также данные в информационных системах представлены в основном в разрезе направлений подготовки, а не образовательных программ, в отношении которых должен проводиться мониторинг. Эксперимент по независимой оценке знаний студентов проводился Рособрнадзором в 2015–2017 гг. и был только экспериментом без последствий для вузов[212].

[212] Абрасова Л.М. Особенности правового обеспечения деятельности контрольно-надзорных органов в сфере высшего образования Российской Федерации // Молодой ученый. 2023. № 3 (450). С. 301–304.

На основе данных о формальном выполнении пороговых значений показателей мониторинга практически невозможно сделать объективные выводы об эффективности работы вузов. Значительная часть содержащихся в мониторинге показателей дублируется другими формами отчетности. Это, в частности, следует из инструктивного письма Министерства образования и науки от 29.03.2018 № ИК-463/05, где прямо отмечается, что «в целях оптимизации управления отчетностью, предоставляемой образовательными организациями в Минобрнауки России, электронная версия формы № 1 – Мониторинг предусматривает автоматическую синхронизацию с данными формы федерального статистического наблюдения № ВПО-1... ».

Иногда это подталкивает вузы предоставлять недостоверную информацию, например, о заработной плате путем оптимизации работников или доли профессорско-преподавательского состава. Это трудно объяснить исключительно техническими ошибками. Ложные сведения касаются как образовательной, так и научно-исследовательской и финансово-экономической деятельности[213].

Проведение мониторинга без выезда обосновано, а вот проведение аккредитационного мониторинга без выезда приводит к формальному подходу, к фальсификации документов, злоупотреблению правом со стороны вузов путем подачи недостоверных данных.

Наличие различных видов мониторинга приводит к увеличению документооборота, усилению бюрократизации вузовской деятельности, что снижает не только экономическую эффективность, но и качество функционирования вузов.

На наш взгляд, следует проверять результаты мониторинга эффективности деятельности вузов с предоставлением ими подтверждающих документов, а также проводить внеплановые проверки по показателям мониторинга эффективности деятельности вузов.

---

[213] Марголин А.М. Мониторинг вузов: всевидящее око регуляторной гильотины // Образовательная политика. 2019. № 1-2 (77-78). URL: https://cyberleninka.ru/article/n/monitoring-vuzov-vsevidyaschee-oko-regulyatornoy-gilotiny (дата обращения: 17.02.2025).

При этом сократить виды конкретизирующих мониторингов вузов за счет внеплановых проверок по показателям мониторинга эффективности деятельности вузов.

За представление вузами в отчетах подложной информации может наступить административная или уголовная ответственность. Выявление даже незначительных изменений в электронном документе достаточно для того, чтобы сказать, что электронный документ подвергался подлогу.

Согласно статье 19.23 КоАП РФ за подделку документов наступает административная ответственность в виде штрафа. Согласно Уголовному кодексу РФ «незаконные приобретение или сбыт официальных документов наказываются штрафом либо исправительными работами, либо арестом. За подделку и изготовление документов предусмотрено более жесткое наказание – ограничение свободы, либо принудительные работы, либо арест. Однако, несмотря на «карательные» меры Уголовного кодекса РФ, часть документов, к сожалению, носит поддельный характер, из чего следует, что на самом деле не каждый вуз добросовестно осуществляет свою деятельность.

В настоящее время встречаются примеры использования фальсифицированных документов вузами при формировании ими отчетов или предоставлении данных для проверок. Подобные действия могут нанести серьезный ущерб отдельным лицам, организациям и обществу в целом. Этот вопрос необходимо прорабатывать и решать на государственном уровне, так он из социальной сферы переходит в сферу криминала и общественной безопасности. Органам государственной власти необходимо разрабатывать проекты по урегулированию данной проблемы и реализовывать их на практике.

Кызим Екатерина Руслановна,

ассистент кафедры правового обеспечения
государственного управления и экономики ФГАОУ ВО
«Российский университет транспорта» (МИИТ),
г. Москва

ПРАВОВЫЕ ОСНОВЫ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ВОЗДУШНОМ ТРАНСПОРТЕ

В авиационной отрасли в Российской Федерации активно идет процесс цифровой трансформации, охватывая всю отрасль. Авиаотрасль на сегодняшний день должна стать одним из отраслевых лидеров экономики по созданию, накоплению, а также объемам хранения цифровых данных с помощью различных бизнес процессов в отрасли. В данной сфере активно внедряются различные цифровые технологии[214]. Важно упомянуть, что естественным процессом в сфере робототехники является искусственный интеллект. Это касается не только воздушного транспорта, но и других отраслей экономики. Искусственный интеллект в ближайшем будущем станет одной из самых прорывных и востребованных технологий. Именно благодаря использованию искусственного интеллекта активно будет развиваться и транспортная отрасль, особенно воздушный транспорт. К сожалению, пока не выработан правовой статус самого искусственного интеллекта. Сейчас действует ГОСТ Р 71476-2024 в области искусственного интеллекта, в котором прописаны общие требования к применению искусственного интеллекта.

На сегодняшний день гражданская авиация занимает значительное место в российской экономике. Хотя стоит отметить,

[214] Быков А.И. К некоторым вопросам правового регулирования полетов беспилотных летательных аппаратов на территории Российской Федерации // Вестник Воронежского государственного университета. Серия «Право». 2018. № 4 (35). С. 197.

что проблем в этой сфере накопилось не мало. Важным фактором для развития любого вида отрасли играет нормативное регулирование. К сожалению, на сегодняшний день в этой отрасли наблюдается стагнация, поскольку Воздушный кодекс не отвечает тем требованиям, которые стоят перед экономикой[215].

Необходимо отметить, что Воздушный кодекс как основной источник в сфере воздушного транспорта играет важную и исключительную роль в системе воздушного законодательства. В данном нормативном акте содержатся основные положения, которые определяют характер и развитие всех остальных источников в системе воздушного законодательства. Данный документ устанавливает общий правовой режим для всех видов гражданской авиации. Нашей задачей является разобраться в соотношении понятий «воздушный транспорт», «авиация», «гражданская авиация». Глубокое и всестороннее рассмотрение различных аспектов теории и практики в сфере воздушного законодательства содержится в трудах В.Д. Бордунова, Б.П. Елисеева. Следует заметить, что судьба данного нормативного акта сложилась совсем не просто. Как только воздушный кодекс был принят в 1997 году, он был подвергнут очень жесткой критике, которая в дальнейшем трансформировалась в значительные изменения и дополнения в данный нормативный акт. Понятие «воздушный транспорт» намного шире, поскольку включает в себя всю инфраструктуру для эксплуатации воздушных судов: аэропорты и диспетчерские службы, а также технические службы. Термин «авиация» подразумевает только один из видов воздушного транспорта. Таким образом, можно сделать вывод о том, что термин «воздушный транспорт» должен быть внесен в акты, регулирующие отрасль воздушного права[216].

---

[215] Грищенко Г.А. Правовое регулирование беспилотных летательных аппаратов: российский подход и мировая практика // Вестник Университета О.Е. Кутафина (МГЮА). 2019. № 12. С. 136.

[216] Макухин А.А. Законодательное регулирование правового статуса беспилотных летательных аппаратов // Научный вестник Крыма. 2017. № 1. URL: https//cyberleninka.ru/ (дата обращения: 18.03.2025).

Необходимо отметить, что появление и закрепление на законодательном уровне «воздушного транспорта» как особого объекта государственного регулирования сможет по-новому расставить юридические акценты в действующем законодательстве в сфере воздушного транспорта. В данном случае «имидж» Воздушного кодекса зависит от того, какие нормы будут прописаны и каким образом данные нормы смогут повлиять на развитие в том числе и рыночных отношений в сфере воздушного транспорта[217].

Таким образом, можно сделать вывод о том, что при принятии нового юридического документа может измениться и сам процесс восприятия данного документа. Вопрос государственного регулирования деятельности «авиации», ее деление на виды, к сожалению, не дает должного результата для последующего регулирования. Возвращаясь к терминологии, термин «гражданская авиация» не дает нам тоже полного представления о какой именно авиации идет речь? Теоретический анализ литературы по воздушному праву дает нам понять, что исходным правовым материалом для отнесения ее к государственной является не только термин «авиация», а воздушные суда и область их назначения. Хотя стоит заметить, что в Чикагской конвенции гражданской авиации 1944 года указано, что военная, таможенная, правоохранительная служба рассматриваются как государственные воздушные суда. Смысл такого подхода вполне очевиден. Так, необходимо разграничивать гражданские и государственные воздушные суда и немаловажно определить цели использования воздушного судна в определенных целях. Необходимо также понимать, что одним из немаловажных факторов и будет являться и то, что сейчас происходит цифровая трансформация и затрагивает в том числе и авиационную отрасль, в частности весь воздушный транспорт, поэтому необходимо понимать, каким образом необходимо менять законодательство.

---

[217] Брусникин В.Ю., Гаранин С.А., Глухов Г.Е. Оптимизация процесса обмена информацией между авиапредприятиями в рамках единого информационного пространства // Научный вестник ГосНИИГА. 2017. № 17 (328). С. 27.

Внедрение цифровых технологий в авиацию не завершено. В рамках нового национального проекта «Экономика данных и цифровая трансформация государства» перед авиаотраслью поставлены задачи по обеспечению технологического суверенитета в Российской Федерации в данной стратегической сфере, в том числе и информационной безопасности.

Важно отметить, что сейчас идет активное внедрение цифровых платформ в сфере воздушного транспорта. Платформа для регистрации и учета правил для владельцев беспилотных летательных аппаратов разрабатывалась уже давно. Еще в начале 2019–2020 гг. все осложнялось тем, что все документы необходимо было заполнять только на бумажном носителе, и отправлены они могли быть только по почте. Сейчас система учета и регистрации перешла на электронный вариант подачи всех документов. В настоящее время отмечается большой прирост лиц, зарегистрированных на электронном портале.

Также хотелось бы отметить, что на сегодняшний день реализуется еще один проект – концепция «Цифровое небо России», разработанная совместно с платформой НТИ, формируется на основе долгосрочного видения развития новых рынков, основанных на единой информационной системе «ЭРА-ГЛОНАСС». Результаты проведенного нами анализа позволяют сделать некоторые частные выводы, представляющие интерес для нашего исследования. В первую очередь это касается терминологии воздушного законодательства. Государству необходимо всерьез задуматься о том, что важно внести изменения в действующие нормативные акты, в которых шла бы речь об употреблении термина «воздушный транспорт», а не авиации в целом. Для того, чтобы избежать путаницы при применении на практике. Наконец, необходимо принять новый кодифицированный акт, который бы отвечал требованиям сегодняшних реалий и соответствовал рыночной экономике. Помимо этого, одним из важных изменений является развитие цифровых платформ и цифрового регулирования со стороны государства, а именно предоставления государственных услуг через различные платформы.

Библиографический список

1. Брусникин В.Ю., Гаранин С.А., Глухов Г.Е. Оптимизация процесса обмена информацией между авиапредприятиями в рамках единого информационного пространства // Научный вестник ГосНИИГА. – 2017. – № 17 (328). – С. 27–33.
2. Быков А.И. К некоторым вопросам правового регулирования полетов беспилотных летательных аппаратов на территории Российской Федерации // Вестник Воронежского государственного университета. Серия. Право. – 2018. – № 4 (35). – С. 197–198.
3. Грищенко Г.А. Правовое регулирование беспилотных летательных аппаратов: российский подход и мировая практика // Вестник Университета О.Е. Кутафина (МГЮА). – 2019. – № 12. – С. 129–136.
4. Макухин А.А. Законодательное регулирование правового статуса беспилотных летательных аппаратов // Научный вестник Крыма. – 2017. – № 1. – URL: https://cyberleninka.ru/article/n/zakonodatelnoe-regulirovanie-pravovogo-statusa-bespilotnyh-letatelnyh-apparatov/viewer (дата обращения:18.03.2025).

Ахатова Алия Махмутовна,

преподаватель кафедры уголовного права и криминологии ИПСУБ ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

ОПРЕДЕЛЕНИЕ МЕСТА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ «ИНТЕРНЕТ» (ПО МАТЕРИАЛАМ СУДЕБНОЙ ПРАКТИКИ)

Особенностью всех преступлений в сфере компьютерной информации и совершаемыми с их использованием является транснациональность (трансграничность), ответственность за эти деяния предусмотрена законодательством различных государств. Именно

трансграничность преступных деяний значительно усложняет установление места совершения преступлений, затрудняет их раскрытие, расследование и профилактику совершения.

Преступления в сфере компьютерной информации могут начаться на территории одного государства, а продолжаться и закончиться на территории других государств. Кроме того, последствия, наступившие на территории одного государства, могут отражаться на территориях, находящихся под юрисдикцией других государств[218].

Информационное пространство не имеет государственных границ, и определение места совершения преступления порождает споры в уголовно-правовой науке и практике ее применения.

Место совершения преступления входит в число обстоятельств, подлежащих доказыванию по уголовному делу (ч. 1 ст. 73 УПК), указывается в обвинительном заключении (ст. 220, 225, 267 УПК РФ), а также в обвинительном приговоре (ст. 307 УПК РФ)[219].

В ***отечественной науке уголовного права*** вопрос определения места совершения преступления решается неоднозначно.

По общему правилу под местом совершения преступления понимается место, где **преступное деяние было пресечено либо окончено** (Кассационное определение Судебной коллегии по делам военнослужащих Верховного Суда РФ от 17.03.2022 № 229-УД22-1-К10). Если преступление было начато в одном месте, а окончено в другом месте, то уголовное дело расследуется **по месту окончания преступления** (ч. 2 ст. 152 УПК РФ). Соответственно, местом совершения преступления признается место его окончания, то есть место совершения последних действий, образующих объективную сторону состава преступления.

---

[218] Степанов-Егиянц В.Г. К вопросу о месте совершения компьютерных преступлений // Армия и общество. 2014. № 5 (42). URL: https://cyberleninka.ru/article/n/k-voprosu-o-meste-sovershеniya-kompyuternyh-prestupleniy

[219] Шарапов Р.Д. Место совершения киберпреступления // Сибирское юридическое обозрение. 2024. Т. 21, № 4. С. 621–635.

Согласно постановлению об отказе в удовлетворении надзорной жалобы Московского городского суда от 25 июня 2012 г. по делу № 4у-4809/2012 местом совершения преступления будет являться Российская Федерация, если **хотя бы один из системы волевых физических актов, образующих действие как признак объективной стороны преступления, совершен на территории России**[220]. Это означает, что если общественно опасное деяние (или хотя бы его часть) совершено за пределами Российской Федерации, однако общественно опасное последствие наступило на территории России, равно как и наоборот, то местом преступления будет считаться территория Российской Федерации[221].

Согласно п. 5 Обзора судебной практики Верховного Суда РФ от 04.07.2001 местом совершения преступления следует считать место, **где окончены все преступные действия, независимо от того, где наступили общественно опасные последствия**[222].

Рассматривая «информационное пространство» как место совершения преступления, необходимо обратиться к судебной практике, поскольку само понятие «места» не определено на законодательном уровне.

В каждом конкретном случае оно устанавливается с учетом конструкции состава преступления и способа причинения вреда охраняемым законом интересам

При определении места совершения преступлений с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», судам необходимо учитывать, что доступ к данной сети может осуществляться с помощью

---

[220] Постановление об отказе в удовлетворении надзорной жалобы Московского городского суда от 25 июня 2012 г. по делу № 4у-4809/2012. URL: https://mos-gorsud.ru/mgs/cases/docs/content/f0cd2035-b503-4074-aca9-b7c545974f07

[221] Есаков Г.А. Настольная книга судьи по уголовным делам / Г.А. Есаков ; Г.А. Есаков, А.И. Рарог, А.И. Чучаев ; ред. А.И. Рарог ; М-во образования и науки Российской Федерации, Московская гос. юридическая акад. Москва : Проспект, 2008. – 569 с.

[222] Обзор судебной практики Верховного Суда РФ от 04.07.2001 "Обзор судебной практики Верховного Суда Российской Федерации за первый квартал 2001 года".

различных компьютерных устройств, в том числе переносных (мобильных)". Согласно п. 19 постановления Пленума Верховного Суда РФ 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», **местом совершения преступления является место, где преступным лицом были выполнены действия, входящие в объективную сторону состава преступления**.

Вместе с тем анализ сложившейся судебной практики судов общей юрисдикции свидетельствует о том, что при определении места совершения преступлений в информационном пространстве, суды, как правило, придерживаются подхода, сводящегося к установлению территориальной привязки к конкретной территории государства, где физически располагается оборудование, компьютеры или иные технические средства, используемые при совершении преступления. Однако данная тенденция не всегда позволяет адекватно отразить специфику данных преступлений и может приводить к затруднениям в установлении юрисдикции, особенно в случаях, когда оборудование находится на территории иностранного государства, а преступление направлено против интересов Российской Федерации.

– Постановлением Калужского районного суда от 21.01.2019 по делу № 1-31/2019 местом преступления была признана **комната обвиняемого**, где фактически располагалось компьютерное оборудование, посредством которого последний реализовывал преступный умысел[223].

– Приговором Устиновского районного суда г. Ижевска Удмуртской Республики суда № 1-256/2017 местом совершения преступления была определена **компьютерной техника**, посредством которой было совершено преступление[224].

---

[223] Постановление Калужского районного суда № 1-31/2019 1-986/2018 от 21 января 2019 г. по делу № 1-31/2019. URL: https://sudact.ru/regular/doc/fxZzClQ44blJ/

[224] Приговором Устиновского районного суда г. Ижевска Удмуртской Республики суда № 1-256/2017.

Могут быть различные ситуации, когда преступления в информационном пространстве затрагивают территории разных государств. Примером может служить организация и проведение азартных игр посредством онлайн-трансляции с территории иностранного государства, где данная деятельность легальна, в то время как в Российской Федерации она запрещена. В таких случаях установление юрисдикции и привлечение к ответственности становится крайне затруднительным, а порой и невозможным.

Пленум Верховного Суда, принимая во внимание разнообразие ситуаций, связанных с определением места совершения преступления, использовал в постановлении формулировку "как правило". Это позволяет судам в каждом конкретном случае, при наличии спорных обстоятельств, самостоятельно определять место совершения преступления исходя из фактических обстоятельств дела и принципов справедливости.

Отсутствие унифицированного подхода к определению места совершения преступления влечет за собой нарушение принципа законности и единообразного применения уголовного законодательства, а также создает препятствия для реализации права обвиняемого на защиту и на рассмотрение его дела компетентным судом, установленным законом, что является существенным нарушением уголовно-процессуальных гарантий.

Представляется ошибочным отождествление места совершения преступления с сетью «Интернет» или виртуальным пространством, поскольку данные понятия лишены признаков географической территории или местности. Подобное расширительное толкование потребовало бы создания самостоятельной правовой системы и юрисдикции в рамках виртуального пространства, что в настоящее время не представляется возможным. Примечательно, что отдельные государства, как, например, Китайская Народная Республика, предпринимают шаги в данном направлении, создавая специализированные онлайн-суды для рассмотрения дел о преступлениях, совершенных исключительно в сети «Интернет». Однако данная практика не является общепринятой и требует дальнейшего изучения

и оценки с точки зрения соответствия общепризнанным принципам уголовного права и процесса.

Следует также учитывать, что в интернет-пространстве существуют международные домены, не имеющие четкой географической привязки к конкретному государству. Кроме того, в правоприменительной практике возможны ситуации, когда информация, размещенная на сайте домена, относящегося к национальному сегменту Российской Федерации (Рунету), физически хранится на сервере, расположенном на территории другого государства, что дополнительно затрудняет определение юрисдикции и места совершения преступления.

В целях обеспечения законности и обоснованности приговора, а также соблюдения права обвиняемого на защиту, необходимо чтобы место совершения преступления было четко установлено и документально зафиксировано в обвинительных документах. Данная фиксация должна включать указание географических координат, наименований географических объектов, населенных пунктов и принадлежности данной местности к конкретному муниципальному образованию субъекта Российской Федерации. Такой подход позволит суду однозначно идентифицировать место совершения преступления.

Таким образом, решение вопроса о юридическом определении места совершения преступления в информационном пространстве может рассматриваться в двух взаимосвязанных аспектах. Во-первых, применительно к конкретным видам общественных отношений, что предполагает анализ существующих и потенциальных общественно опасных деяний, их классификацию по объекту посягательства и выработку определения места совершения преступления для каждой категории. Во-вторых, в унифицированном аспекте, предполагающем разработку единого, универсального понятия места совершения преступления, применимого ко всем деяниям, совершенным в информационном пространстве, независимо от объекта посягательства. Придерживаясь первой точки зрения, необходимым является осуществить анализ всех возможных

общественно-опасных деяний в информационном пространстве, классифицировав их по общественным отношениям и предложить выработку понятия места совершения преступления.

Затруднительным является вопрос определения места совершения преступления в тех случаях, когда деяние, совершенное в интернет-пространстве, затрагивает интересы нескольких государств, создавая коллизию юрисдикций и требуя применения принципов международного права для определения компетентного органа, уполномоченного на расследование и рассмотрение дела. В подобных ситуациях необходимо учитывать не только местонахождение оборудования и серверов, но и место причинения вреда, место регистрации доменного имени и другие обстоятельства, имеющие существенное значение для установления наиболее тесной связи преступления с конкретным государством.

А.И. Бойцов высказал следующую идею по этому вопросу: «Совершенным в России признается как учиненное на ее территории деяние, последствия которого должны были наступить или наступили за границей, так и преступление, хотя бы и начатое за границей, но оконченное (результат наступил или должен был наступить) на ее территории. Такое же решение предлагается и относительно совершаемых в соучастии преступлений: для признания совместно совершенного преступления содеянным в России достаточно, чтобы исполнитель действовал на ее территории, если же он действовал за границей, а остальные участники – в России, то действия последних также признаются совершенными на ее территории».

Основываясь на принципе государственного суверенитета, следует исходить из того, что преступление должно признаваться совершенным на территории Российской Федерации, если хотя бы часть деяния, образующего состав преступления, была совершена на территории РФ. Данный подход находит свое выражение в принципе территориальности, закрепленном в уголовном законодательстве, и является важным инструментом защиты национальных интересов и обеспечения правопорядка в пределах государственной границы.

Однако применение данного принципа к преступлениям, совершенным с использованием ИТС, требует учета специфики этой среды и может потребовать более широкого толкования понятия «территория» для включения в него информационных ресурсов, серверов и иных объектов, находящихся под юрисдикцией Российской Федерации, вне зависимости от их физического местонахождения.

Семушин Александр Валентинович,

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

ПРОБЛЕМА ВОЗРАСТА ДЕЕСПОСОБНОСТИ НЕСОВЕРШЕННОЛЕТНЕГО ЛИЦА КАК СУБЪЕКТА ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

Прогрессирующая информационная вовлеченность и социализация при помощи Интернета несовершеннолетних лиц неизбежно ставит вопрос об их возрастной дееспособности в информационном пространстве, что обуславливает необходимость и актуальность исследования данной проблемы.

Согласно Окинавской Хартии Глобального информационного общества от 22 июля 2000 г. преимуществами глобального информационного общества, **общедоступным** информационным наполнением и открытыми для **всех пользователей** программными средствами должны пользоваться **все люди без исключения** (выделено здесь и по тексту авт.).

Конвенция о правах ребенка ООН № 44/25 от 20 ноября 1989 г. признает за ребенком право свободно выражать свое мнение, искать, получать и передавать информацию по его выбору. Замечания

общего порядка № 25 (2021) о правах детей в связи с цифровой средой от 21 марта 2021 г. к Конвенции о правах ребенка ООН расценивают не дискриминацию информационных прав ребенка как обеспечение государством полноценного, равного и реального доступа **всем детям** к электронной среде и **общедоступность** цифровых технологий для реализации ими своих прав.

Как видно, нормы международного права не только не ограничивают информационную дееспособность несовершеннолетнего, но и признают это дискриминацией и нарушением прав ребенка. Международные нормы приоритетны в системе российского права, которое в своих стержневых нормативных актах тоже достаточно широко и неопределенно относится к возрастному статусу участников информационного оборота.

Право на получение, передачу, производство и распространение информации признается за **каждым** ст. 29 Конституции РФ, а Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» – **за любыми лицами.** Возрастные грани реализации информационных прав не проведены. В других федеральных информационных законах прямых возрастных ограничений тоже не имеется. В соответствии с Федеральным законом № 59-ФЗ от 02 мая 2006 г. «О порядке рассмотрения обращений граждан Российской Федерации» и Федеральным законом № 8-ФЗ от 09 февраля 2009 г. «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» правом на обращение в органы власти наделен **любой гражданин**. Согласно Федеральному закону от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле» право на библиотечное обслуживание имеет **каждый гражданин** независимо от возраста. Для этого достаточно предъявить паспорт (выдается в 14 лет – прим. автора). Не установлен возраст доступа к архивным фондам Федеральным законом «Об архивном деле в Российской Федерации» от 22 октября 2004 г. № 125-ФЗ. Не определен возраста субъекта персональных данных и в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

В соответствии с Федеральным законом «О связи» от 07 июля 2003 г. № 126-ФЗ и правилами оказания услуг телефонной связи и передачи данных, данные услуги оказываются путем заключения возмездного гражданско-правового договора по предъявлению паспорта. Возраст лица, заключающего договор, не конкретизирован[225].

Отсутствие в приведенных актах возрастной правореализационной оговорки наряду с употребляемыми в них оборотами: **«каждый», «любые лица», «все люди без исключения», «полноценный доступ детям», «право ребенка на информацию», «всем детям», «каждый гражданин независимо от возраста», «всех пользователей», «общедоступный»** дают повод формально-юридически воспринимать их как наделяющих информационной дееспособностью физических лиц независимо от возраста, то есть с самого рождения. Подобное толкование принципиально противоречит отечественной правовой традиции, не признающей абсолютной, вне возрастной, дееспособности граждан, что является полностью обоснованным.

Нельзя утверждать о полном отсутствии возрастных ограничений дееспособности физических лиц в информационно-правовом поле. Требование о предъявлении паспорта опосредованно ограничивает самостоятельный доступ к услугам библиотек и телекоммуникаций возрастом его получения, то есть 14 годами, а гражданско-правовой характер услуг связи еще и нормами Гражданского кодекса РФ. По Закону РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» не может учреждать средство массовой информации лицо младше восемнадцатилетнего возраста. Запрещая распространять среди несовершеннолетних информацию, причиняющую вред их здоровью и развитию, одноименный федеральный

[225] О порядке оказания услуг телефонной связи : постановление Правительства РФ от 09 декабря 2014 г. № 1342 // СЗ РФ. 2014. № 51, ст. 7431; Об утверждении Правил оказания услуг телефонной связи : постановление Правительства РФ от 24 января 2024 г. № 59 // СЗ РФ. 2024. № 5, ст. 707; Об утверждении Правил оказания услуг связи по передаче данных : постановление Правительства РФ от 31 декабря 2021 г. № 2606 // СЗ РФ. 2022. № 3, ст. 578.

закон фактически ограничивает право ребенка на доступ к информации[226]. Ограничение прав ребенка на информацию установлено в виде запрета распространять среди несовершеннолетних рекламу определенного содержания Федеральным законом от 13 марта 2006 г. № 38-ФЗ «О рекламе».

Однако данные ограничения носят фрагментарный характер, касаются отдельных информационных отношений и комплексно в широком спектре проблему информационной дееспособности несовершеннолетних не решают. Отсутствует единая нормативно-определенная категория возраста дееспособности в виртуальном пространстве Интернета. Нет указания на возраст в правовом статусе таких субъектов, как пользователь, распространитель, обладатель информации, пользователь социальной сети и иных различных информационных ресурсов и сервисов Интернета. Вследствие этого владельцы и операторы информационных ресурсов Интернета самостоятельно определяют возраст доступа к ним в пользовательских соглашениях, процедурах авторизации и идентификации.

Отсутствие комплексного возрастного института информационной дееспособности, по аналогии с гражданским, трудовым, семейным правом, порождает правовую неопределенность в данной области и создает почву для нарушений информационных прав несовершеннолетних как в сфере получения и распространения ими информации, так и их защиты от противоправных посягательств в информационной экосистеме. На отсутствие комплексных решений, несформированность общего подхода к статусу личности в цифровом пространстве, в том числе недостаточную теоретическую проработку правового статуса участника социальных сетей, необходимость доктринального определения и нормативного закрепления правосубъектности физических лиц как участников правовых

[226] О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон от 29 декабря 2010 г. № 436-ФЗ (в ред. от 28 апреля 2023 г.) (принят Государственной Думой 21 декабря 2010 г., одобрен Советом Федерации 24 декабря 2010 года) // СЗ РФ. 2011. № 1, ст. 48.

отношений в цифровой сфере указывают в своих публикациях Е.А. Мамай[227], В.В. Богдан и Л. Лаксми[228].

Несмотря на очевидную значимость, вопрос дееспособности несовершеннолетних как общей правовой категории во всех информационных отношениях в академической среде должным образом не дискутируется. Научные работы в этом направлении в основном концентрируются на обсуждении ограничения доступа детям к информации, причиняющей психический и иной вред. В учебной литературе вопрос возраста дееспособности физических лиц как субъектов информационного права разрешается через гражданско-правовой статус. Так, в части реализации несовершеннолетними информационных прав И.Л. Бачило полностью приводит диспозицию п. 2 ст. 26 и 28 ГК РФ о праве малолетних совершать мелкие бытовые сделки[229]. Определяя пределы и объемы дееспособности в информационной сфере 6–14 и 14–18-летним возрастом, И.М. Рассолов тоже фактически воспроизводит положения ст. 21, 26, 28 ГК РФ[230]. Аналогично ссылается на ст. 26 ГК РФ и Н.Н. Ковалева[231]. Каких-либо правоприменительных проблем такого подхода авторами не обозначено.

---

[227] Мамай Е.А. Правосубъектность физического лица в системе цифровых отношений: исходная точка правового регулирования // Государство и граждане в электронной среде. Выпуск 5 (Труды XXIV Государство и граждане в электронной среде. Вып. 5. 2021. 45. Международной объединенной научной конференции «Интернет и современное общество», IMS-2021, Санкт-Петербург, 24–26 июня 2021 г. Сборник научных статей). СПб. : Университет ИТМО, 2021. С. 45–62.

[228] Богдан В.В., Лаксми Л. Субъекты права социальных сетей: к вопросу об определении правового статуса пользователей // Известия Юго-Западного государственного университета. Серия «История и право». 2022. Т. 12, № 5. С. 28–38. URL: https://doi.org/10.21869/2223-1501-2022-12-5-28-38.

[229] Информационное право : учебник для вузов / И.Л. Бачило. 5-е изд., перераб. и доп. Москва : Издательство Юрайт, 2023. С. 48–51.

[230] Информационное право : учебник и практикум для вузов / И.М. Рассолов. 6-е изд., перераб. и доп. М. : Юрайт, 2023. С. 119–120.

[231] Информационное право : учебник для вузов / Н.Н. Ковалева [и др.] ; под ред. Н.Н. Ковалевой. М. : Издательство Юрайт, 2024. С. 59.

На наш взгляд, безоговорочная отсылка к ст. 21, 26, 28 ГК РФ как к ключу, дающему все ответы по обозначенной теме и устраняющему ее проблематику, не верна. Действующая правовая конструкция ст. 26, 28 ГК РФ создает проблемы ее применения в информационных отношениях. Оставляя за скобками распоряжение денежными средствами, как вещное правомочие, в остальном указанные статьи признают за ребенком институт авторства и право заключения сделок мелко-бытового характера или направленных на безвозмездное получение выгоды. Ввиду отсутствия в законе понятия мелких бытовых сделок, на практике ими признаются сделки, удовлетворяющие личные бытовые потребности, соответствующие физическому, духовному или социальному развитию лица ее заключающему, и сравнительно невысокая стоимость предмета сделки.

В таком случае можно ли по данным критериям отнести к мелким бытовым сделкам пользовательские соглашения доступа к электронным библиотекам, аудиовизуальным сервисам, иным интернет-ресурсам; приобретение ауди-, видео- и иной информационной продукции; договоры на создание, администрирование, продвижение своих сайтов и персональной страницы в социальной сети, а также договоры на оказание услуг связи для подключения несовершеннолетними своих электронных устройств к телефонным и интернет-сетям, если эти сделки заключены в целях удовлетворения личных бытовых информационных потребностей ребенка, в частности для общения с родителями, друзьями, или это сделки, требующие письменного согласия законных представителей? Нормативного разъяснения данного вопроса нет.

Информационная деятельность сопряжена с совершением таких действий, как доступ к Интернету и цифровым сервисам разного рода, распространение через них информации, блогерство; согласие на предоставление своих персональных данных и их использование, согласие цифровым приложениям и программам на обработку cookie-файлов и доступа к личной информации пользователя на его устройстве: фото, видео, файлам, контактам и т.д.; направление

запроса на получение информации; требование к оператору, владельцу поисковой системы, социальной сети о прекращении распространения информации, нарушающей законодательство, и соответствующее обращение с жалобой в Роскомнадзор; создание персональной страницы в социальной сети и телеграмм-канала, аккаунта (учетной записи), регистрация доменного имени, администрирование, создание электронной подписи и т.д. Появились такие информационные объекты, как виртуальное пространство, цифровые сети, системы и приложения, сайты, телеграмм-каналы, контент, биометрия, доменные имена, аккаунты, и т.п. Дефиниции ст. 26, 28 ГК РФ не дают ясного и четкого ответа о возможности самостоятельного совершения несовершеннолетними и малолетними подобных действий и в отношении данных объектов. Невозможно оценить через гражданско-правовую призму правомочие несовершеннолетнего на создание аккаунта (учетной записи) в Интернете, передаче им прав на его администрирование третьему лицу, так как аккаунт к объектам гражданских прав не относится. В равной степени это касается и доменного имени, которое при использовании его только как средства адресации в сети «Интернет», не является объектом гражданских прав.

Проблема применения норм ГК РФ в качестве универсальной формулы дееспособности несовершеннолетнего в информационных отношениях заключается в их целевом предназначении для регулирования традиционных гражданско-правовых, в основном имущественных, отношений, тогда как информационный мир породил новые явления, неизвестные гражданскому праву.

Таким образом, в качестве результатов исследования можно сделать следующие выводы:

– на данный момент информационно-правовой статус несовершеннолетнего имеет неопределенный и противоречивый характер, позволяя говорить о существенном правовом пробеле в этом вопросе;

– априорное и универсальное применение гражданско-правового статуса несовершеннолетних ко всему комплексу информационных отношений проблему не разрешает;

– необходимо единое комплексное определение информационно-правового статуса несовершеннолетнего в основополагающих информационных нормативных актах по аналогии разрешения этого вопроса в гражданском, трудовом, семейном праве;

– при формировании информационно-правового статуса несовершеннолетнего исходить из разумного баланса между необходимостью ограничения дееспособности ребенка в целях обеспечения его информационной безопасности и в тоже время учитывать объективную потребность активного использования несовершеннолетними информационных технологий, самостоятельного и широкого доступа к ним.

Губайди Яна Алексеевна,

обучающаяся магистратуры Института права, социального управления и безопасности ФГБОУ ВО «Удмуртский государственный университет» г. Ижевск

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ДОВЕРИЯ К ИСКУССТВЕННОМУ ИНТЕЛЛЕКТУ

Ещё недавно искусственный интеллект для каждого из нас был неразгаданным и неизвестным объектом, а уже сегодня наша жизнь глубоко пронизана технологиями, функционирующими на основе искусственного интеллекта. Искусственный интеллект, исходя из Федерального закона от 24.04.2020 № 123-ФЗ, – это 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[232]. Однако в научных кругах искусственный интеллект (далее – ИИ) определяется с разных ракурсов. Например, Х.С. Алтемирова рассматривает ИИ как область компьютерных наук, посвященную созданию умственных машин, способных выполнять задачи, требующие человеческого интеллекта[233]. В работе П.М. Мохата ИИ указан в качестве полностью или частично автономной самоорганизующей (и самоорганизующейся) компьютерно-аппаратно-программной виртуальной (virtual) или киберфизической (cyberphysical), в том числе био-кибернетической (bio-cybernetic), системы (юнит), не живой в биологическом смысле этого понятия, с соответствующим математическим обеспечением, наделённой/обладающей программно-синтезированными (эмулированными) способностями и возможностями»[234]. Анализируя приведенные ранее понятия, следует отметить, что авторы рассматривают ИИ с той точки зрения, которая необходима им для дальнейшего исследования. В связи с тем, что отсутствует единообразное определение искусственного интеллекта, которое бы содержало в себе все характерные черты ИИ, возникает множественность понимания о том, что подразумевает под собой ИИ. Данную проблему выделяют многие ученые, например, В.Б. Наумов

[232] 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. URL: https://www.consultant.ru/document/cons_doc_LAW_351127/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 19.04.2025).

[233] Алтемирова Х.С. Искусственный интеллект и возможности его применения в разных сферах жизни // Молодой ученый. 2023. № 48 (495). С. 5–7. URL: https://moluch.ru/archive/495/108341/ (дата обращения: 19.04.2025).

[234] Мохат П.М. Правосубъектность юнита искусственного интеллекта: некоторые гражданско-правовые подходы // Вестник КГУ. 2018. № 3. С. 280-283. URL: https://cyberleninka.ru/article/n/pravosubektnost-yunita-iskusstvennogo-intellekta-nekotorye-grazhdansko-pravovye-podhody (дата обращения: 19.04.2025).

и Г.Г. Камалова в своем труде высказывают убеждение о том, что необходимо выработать правовое определение понятия «искусственный интеллект» и установить системные иерархические взаимосвязи с иными понятиями, используемыми в этой сфере[235].

Тенденция развития и внедрения ИИ является стремительной и господствующей во многих сферах деятельности общества (промышленность, бизнес, наука, искусство и др.). Однако стоит отметить, что при использовании искусственного интеллекта на современном этапе возникает множество различных проблем. А.И. Медведев в своём труде, говоря о возможностях использования ИИ, сделал акцент на проблемах, среди которых отметил этико-правовые и интеллектуально-правовые проблемы, проблемы ответственности за их действия, проблемы правосубъектности ИИ и др.[236].

В первую очередь общество озабочено проблемой доверия к новейшим технологиям при их использовании не только в повседневной жизни, но и в важнейших социально значимых сферах. Под доверием обычно понимается убежденность в чьей-либо честности, порядочности, добросовестности. В целях обеспечения доверительного отношения и защищенности при использовании искусственного интеллекта научными кругами была предложена концепция доверенного ИИ. В целом термин «доверенный» к вычислительным системам применяется достаточно давно. Доверительные системы подразумевают под собой совокупность стандартов, разрабатываемых на их основе технологий, аппаратного и программного обеспечения для создания высокой степени безопасности при работе

---

[235] Наумов В.Б., Камалова Г.Г. Вопросы построения юридических дефиниций в сфере искусственного интеллекта // Труды Института государства и права РАН. 2020. № 1. С. 81-93. URL: https://cyberleninka.ru/article/n/voprosy-postroeniya-yuridicheskih-definitsiy-v-sfere-iskusstvennogo-intellekta (дата обращения: 20.04.2025).

[236] Медведев А.И. Правовые аспекты искусственного интеллекта и смежных технологий // Журнал Суда по интеллектуальным правам. 2022. Вып. 4 (38). С. 48–63. URL: https://ipcmagazine.garant.ru/articles/1729271/ (дата обращения: 20.04.2025).

программ[237]. Таким образом, доверенный ИИ – это концепция разработки и эксплуатации систем искусственного интеллекта, гарантированно обладающих свойствами надежности, безопасности, эффективности, продуктивности, прозрачности, конфиденциальности, справедливости и этичности получаемых результатов[238]. Доверие к ИИ и его системам с физической точки зрения означает уверенность в корректной работе всех компонентов, а также в безопасности данных и контроле над системой. Кроме того, важно доверие к программному обеспечению, которое должно корректно работать и отвечать требованиям субъекта.

Роль данной концепции заключается в обеспечении золотой середины между применением быстроразвивающихся технологий и защитой этических и моральных аспектов жизнедеятельности человека. Сегодня в России отсутствует фундаментальная правовая база, регулирующая ИИ, его особенности и функции, требования к нему и ответственность за действия, совершенные им. Крайне важно сформировать не только нормативно-правовую систему, отвечающую запросам технологического прорыва, но и создать технологии, позволяющие противодействовать угрозам человеческим моральным ценностям[239].

На международном уровне множество организаций и комитетов озадачены вопросом разработки общих рекомендаций, стандартов и руководств по разработке нормативной базы в области внедрения

---

[237] Намиот Д.Е., Ильюшин Е.А., Пилипенко О.Г. Доверенные платформы искусственного интеллкте // International Journal of Open Information Technologies. 2022. № 7. С. 119-127. URL: https://cyberleninka.ru/article/n/doverennye-platformy-iskusstvennogo-intellekta (дата обращения: 20.04.2025).

[238] Прозоров А. Доверенный ИИ: от концепции до реализации // Открытые системы. СУБД. 2024. № 03. URL: https://www.osp.ru/os/2024/03/13058758?ysclid=m9oh85r4oi332496282 (дата обращения: 20.04.2025).

[239] Авдошин С.М., Песоцкая Е.Ю. Доверенный искусственный интеллект как способ цифровой защиты // Бизнес-информатика. 2022. № 2. С. 62-73. URL: https://cyberleninka.ru/article/n/doverennyy-iskusstvennyy-intellekt-kak-sposob-tsifrovoy-zaschity (дата обращения: 20.04.2025).

ИИ. Первым ключевым актом в сфере правового регулирования искусственного интеллекта является документ, принятый в 2019 г. Организацией экономического сотрудничества и развития «Рекомендации Совета по искусственному интеллекту» (далее – Рекомендации). В первом разделе данного акта закреплены принципы ответственного управления заслуживающим доверия ИИ, среди которых можно выделить:

1) инклюзивный рост, устойчивое развитие и благосостояние;

2) уважение к верховенству закона, правам человека и демократическим ценностям, включая справедливость и неприкосновенность частной жизни;

3) прозрачность и объяснимость;

4) надежность, защищенность и невредимость;

5) подотчетность[240].

Перечисленные руководствующие начала создали базис, на котором должны быть основаны последующие документы. Позже было принято несколько конвенций, посвященных области применения ИИ и закрепляющих принципы справедливости, непредвзятости, гибкости алгоритмов и др.

Деятельность как международных, так и национальных органов власти на данный момент должна быть акцентирована не только на адаптации правовой базы, но и на увеличении её объемов по мере развития современных правоотношений. Им необходимо обеспечить функционирование базовых принципов, указанных в Рекомендациях. Таким образом будет собрана система норм, осуществляющих сбалансированное правовое регулирование, разграничив области действия диспозитивных и императивных актов. Система правовых норм позволит государствам избежать потенциальные риски нарушения прав человека в связи с тем, что на государственном уровне будут закреплены основания доверять искусственному интеллекту.

[240] The Recommendation on Artificial Intelligence 22.05.2019 C(2019)34. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText (дата обращения: 21.04.2025).

Научное сообщество играет немаловажную роль при реализации концепции доверенного ИИ. Первостепенное значение имеет способность ученых и разработчиков защищать нейронные сети, в ином случае будет подорвано доверие к ИИ и развитие ИИ сведется к зависимости человека от третьих лиц. С.М. Авдошин, Е.Ю. Песоцкая отмечают, что наиболее важным является создание стандартов, гарантирующих постоянный анализ потенциальных рисков и внедрение новейших систем защиты[241].

Рассмотрим возникающие на сегодняшний день риски при использовании ИИ и возможности их управления в будущем:

1. Нарушение конфиденциальности – утечка личных данных, наиболее выгодная для третьих лиц информация, которая может быть изъята в любой момент использования нейросетей. Для повышения конфиденциальности информации предлагается технология OPAL (open algorithms progect) Security, которая предполагает предоставление алгоритмам доступа к данным удаленно и контролируемо. Новейшая платформа управления доступом нового поколения основывается на двух одинаково важных составляющих – конфиденциальности и безопасности данных. Данная позиция входит в комплексную стратегию защиты данных. OPAL использует строгие технические и административные меры безопасности, чтобы обеспечить соответствие услуг отраслевым стандартам.

2. Отравление данных заключается в том, чтобы включить в обучающую систему возможность предоставления ложной информации либо принятия неверных решений, выгодных кому-либо из третьих лиц. Очевидно, что таким образом технологии могут повлиять на общество, например, направив поведение людей в разрушительное русло – несанкционированные митинги, вандализм и др. А также возможно и нанесение урона репутации отдельной личности. При угрозе возникновения данных атак выступают важными

[241] Авдошин С.М., Песоцкая Е.Ю. Доверенный искусственный интеллект как способ цифровой защиты // Бизнес-информатика. 2022. № 2. С. 62-73. URL: https://cyberleninka.ru/article/n/doverennyy-iskusstvennyy-intellekt-kak-sposob-tsifrovoy-zaschity (дата обращения: 21.04.2025).

аспектами – человеческое управление и контроль над искусственным интеллектом.

3. Научное сообщество обеспокоено возможностью развития атак уклонения, которая возникает на этапе применения ИИ. Даже самые малейшие изменения во входных значениях могут повлиять на исходный ответ нейросети, что подразумевает возможные негативные последствия. Противодействием для таких атак является технология генеративно-состязательных тренировок – на этапе обучения ИИ разработчики вводят неверные данные, в дальнейшем нейронные сети не обращают внимание на потенциальные «угрозы».

4. Инверсия модели, которая представляет собой значительную утечку персональных данных любого пользователя. Борьба с такими угрозами возможна с помощью приватного агрегирования обучающих моделей, т.е. разделение группы данных на мини-области, по каждой из которых будет обучаться отдельная нейросеть, затем сети объединяют для конечного результата, не предоставляя доступ к первоначальным данным конечной модели.

Научному сообществу в сфере применения ИИ и управления рисками необходимо представлять современные технологии, с помощью которых будут активно реализовываться принципы, закрепленные в Рекомендациях ОЭСР.

В Российской Федерации Президент подписал Указ «О развитии искусственного интеллекта в Российской Федерации»[242], который включает в себя Национальную стратегию развития ИИ на период до 2030 года (далее – Стратегия). Согласно Стратегии доверенные технологии искусственного интеллекта – это технологии, отвечающие стандартам безопасности, разработанные с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку

[242] О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) : Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024). URL: https://sudact.ru/law/ukaz-prezidenta-rf-ot-10102019-n-490/ukaz/ (дата обращения: 22.04.2025).

и нарушения его основополагающих прав и свобод, нанесения ущерба интересам общества и государства[243].

Раздел № 51 (8) Стратегии содержит в себе направления внедрения доверенных технологий искусственного интеллекта в органах публичной власти и организациях:

1) включение в приоритетном порядке проектов по внедрению доверенных технологий искусственного интеллекта в программы цифровой трансформаци (в которых должны быть предусмотрены экономический эффект от их реализации и повышение эффективности деятельности органов публичной власти);

2) методическое и нормативно-правовое обеспечение внедрения доверенных технологий искусственного интеллекта в государственном управлении;

3) формирование реестра апробированных доверенных технологий искусственного интеллекта, проверенных на угрозы информационной безопасности;

4) внедрение в федеральных органах государственной власти только тех решений в области искусственного интеллекта, которые прошли сертификацию;

5) обеспечение внедрения и использования доверенных технологий искусственного интеллекта для выполнения органами публичной власти текущих задач;

6) обеспечение централизованной разработки и распространения типовых решений, созданных на основе доверенных технологий искусственного интеллекта;

7) формирование правил получения наборов данных от коммерческих и некоммерческих организаций в целях повышения эффективности государственного и муниципального управления и др.[244].

---

[243] Национальная стратегия развития искусственного интеллекта на период до 2030 года (в редакции Указа Президента Российской Федерации от 15.02.2024 № 124). URL: https://sudact.ru/law/ukaz-prezidenta-rf-ot-10102019-n-490/natsionalnaia-strategiia-razvitiia-iskusstvennogo-intellekta/ (дата обращения: 22.04.2025).

Основными целями в обеспечении эффективного правового обеспечения использования доверенного искусственного интеллекта являются формирование эффективной нормативно-правовой базы, соответствующей стандартам международного и национального уровня, её своевременное развитие и активное применение. Неотъемлемой частью достижения поставленных целей выступают устранение излишних правовых барьеров, распространение этических норм, а также использование инновационной мировой практики по регулированию доверенного ИИ. Среди принципов, на которых должны основываться акты регулирования ИИ в России, конечно, следует выделить безопасность, отсутствие дискриминации, уважение автономии человека, риск-ориентированный подход, ответственность.

Научно-технический прогресс, позволяющий использовать инновационные технологии ИИ, применяемые во многих сферах деятельности человечества, позволяет обществу принимать современные вызовы и угрозы, а также эффективно справляться с ними и добиваться нового уровня развития. Масштабное внедрение искусственного интеллекта видится возможным благодаря концепции доверенного ИИ, обеспечивающей надежность, корректность, а также безопасность данных.

В отечественном правовом поле достаточно скудно регулируется искусственный интеллект – его свойства, принципы применения, функции, однако отмечается, что в ближайшем будущем на основе закрепленных Стратегией принципов будет создана система нормативно-правовых актов, эффективно действующих в современных условиях и усматривающих механизмы для противодействия рискам применения ИИ.

---

[244] Национальная стратегия развития искусственного интеллекта на период до 2030 года (в редакции Указа Президента Российской Федерации от 15.02.2024 № 124). URL: https://sudact.ru/law/ukaz-prezidenta-rf-ot-10102019-n-490/natsionalnaia-strategiia-razvitiia-iskusstvennogo-intellekta/v/vnedrenie-doverennykh-tekhnologii-iskusstvennogo-intellekta/ (дата обращения: 22.04.2025).

Соловьев Николай Николаевич,

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

ИНФОРМИРОВАНИЕ ЗАЕМЩИКОВ КАК СПОСОБ ЗАЩИТЫ ОТ КИБЕРМОШЕННИЧЕСТВА

Современные технологии значительно упростили процесс получения финансовых услуг, однако вместе с удобством пришли новые риски. С развитием цифровых платформ кредитные продукты стали легко доступны онлайн, но это также создало благоприятные условия для мошенников. Согласно данным Центробанка РФ объем ущерба от мошенничеств с использованием банковских карт и счетов граждан в 2020 году составил около 10 млрд рублей [1]. Согласно данным Сбербанка аналогичный ущерб за 2024 г. составил как минимум 295 миллиардов рублей [2]. В условиях растущего количества преступлений в сфере кибермошенничества важно разработать эффективные меры по защите пользователей от несанкционированного использования их персональных данных и средств.

Одной из наиболее распространенных схем мошенничества становится получение кредита на имя жертвы путем подделки документов или взлома аккаунтов. Мошенник получает доступ к банковским аккаунтам клиента и оформляет займ, который впоследствии практически невозможно оспорить. Однако с изменением законодательства у граждан появилась возможность не платить такие займы, но заемщику необходимо доказывать, что кредит оформлен путем мошенничества. Это доставляет значительные моральные страдания и финансовые трудности для пострадавших, особенно учитывая тот факт, что многие узнают о существовании займа лишь спустя длительное время после его оформления.

Основная проблема заключается в недостаточной защищенности информационных систем большинства банков и микрофинансовых организаций. Несмотря на внедрение многоуровневых систем аутентификации и шифрования данных, злоумышленникам удается находить слабые места в защите. Часто преступники используют методы социальной инженерии – обманывают сотрудников банка или самих клиентов, чтобы получить необходимую информацию.

Например, фишинговые сайты все еще остаются одним из популярных способов хищения данных. Мошенники создают поддельные сайты, имитирующие страницы банков, и выманивают у пользователей пароли и коды подтверждения. После получения такой информации они имеют возможность оформить кредиты на чужое имя. Другим распространенным методом является использование вредоносного программного обеспечения (вирусов, троянов), которое крадет данные прямо с устройств пользователей.

Еще одной серьезной проблемой остается низкий уровень финансовой грамотности населения. Многие граждане недостаточно хорошо понимают принципы работы кредитных продуктов и не знают, какие права и обязанности у них есть в случае возникновения споров с банками. Особенно это касается молодых людей, которые впервые сталкиваются с кредитными продуктами. Данная проблема актуальна также и для старшего поколения нашей страны. Они часто становятся жертвами мошенников, поскольку доверяют непроверенной информации и не принимают должных мер предосторожности.

Кроме того, далеко не все пользователи регулярно проверяют свою кредитную историю. Даже если клиент замечает сомнительную активность, связанную с его аккаунтами и счетами, это происходит уже после того, как ущерб был нанесен. Поэтому своевременное уведомление о любом изменении в кредитной истории могло бы стать важным инструментом предотвращения мошенничества. В целях предотвращения кибермошенничества в Российской Федерации был принят закон, устанавливающий так называемый «Период охлаждения» при выдаче займов или кредитов. Если потребительский кредит (заем) или его лимит – от 50 тыс. до 200 тыс. руб. включи-

тельно, то банк либо МФО передаст деньги гражданину не ранее 4 ч после того, как последний подпишет индивидуальные условия. Если займ более 200 тыс. руб., то минимальный период "охлаждения" – 48 ч [3]. Данная мера должна обезопасить граждан нашей страны от неправомерного доступа к их банковским счетам. Однако можно дополнительно защитить заемщика от кибермошенничества.

Для повышения уровня безопасности заемщиков необходимо пересмотреть действующие нормы законодательства и предложить ряд новых инициатив. Одной из таких инициатив должно стать обязательное уведомление заемщика через SMS-сообщение о любой активности, связанной с его кредитной историей. Сюда следует отнести как запросы кредитной истории со стороны различных финансовых организаций, так и непосредственно факты выдачи кредита (займа).

Данный способ защиты от кибермошенничества имеет целый ряд преимуществ, таких как

– Оперативность. Получив сообщение сразу же после попытки оформления кредита или запроса кредитной истории, заемщик сможет быстро среагировать на возможное мошенничество. Если операция была совершена без его ведома, он имеет возможность немедленно связаться с банком и заблокировать дальнейшие действия.

– Простота реализации. Система SMS-уведомлений достаточно проста в техническом плане и может быть интегрирована в существующие банковские процессы без значительных затрат. Большинство банков уже отправляют своим клиентам SMS-оповещения о различных операциях, и добавление еще одного типа сообщений не потребует кардинальных изменений инфраструктуры.

– Повышение доверия к банку. Внедрение подобной системы повысит доверие клиентов к банковской системе, так как они будут уверены, что банк заботится о сохранности их финансов и вовремя предупреждает о любых изменениях.

– Снижение нагрузки на службы поддержки, правоохранительные и судебные органы. Чем быстрее будет выявлен случай мошенничества, тем меньше усилий потребуется для восстановле-

ния справедливости. Клиенты смогут самостоятельно предотвращать потенциальные проблемы до обращения в службу поддержки или правоохранительные и судебные органы.

Платная подписка Объединенного кредитного бюро как успешный пример защиты от кибермошенничества.

Примером успешного применения концепции регулярного мониторинга кредитных операций служит практика Объединенного Кредитного Бюро (ОКБ – структура, входящая в экосистему Сбера). ОКБ предлагает платную подписку, позволяющую гражданам получать регулярные отчеты о состоянии своей кредитной истории. Пользователи могут отслеживать любые изменения в своем кредитном рейтинге и своевременно реагировать на подозрительные события.

Подписчики получают уведомления обо всех попытках сторонних организаций проверить их кредитоспособность, будь то банк, микрофинансовая организация или даже работодатель. Это позволяет клиенту заранее узнать о возможных рисках и принять необходимые меры. Такой подход демонстрирует высокую эффективность в борьбе с мошенническими действиями, и аналогичные механизмы могут быть внедрены на уровне всей банковской системы.

Рост числа киберпреступлений требует немедленного реагирования со стороны государства и финансовых учреждений. Предлагаемые законодательные изменения, такие как обязательные SMS-уведомления о выдаче кредита и запросах кредитной истории, помогут существенно повысить безопасность заемщиков и сократить количество мошенничеств. Использование опыта ОКБ показывает, что регулярный мониторинг кредитных операций является эффективным средством защиты граждан от недобросовестных действий.

Необходимо продолжать работу над повышением уровня финансовой грамотности среди населения и развивать инфраструктуру информационной безопасности в банках. Только комплексный подход, включающий технические и образовательные меры, поможет минимизировать риски для потребителей финансовых услуг.

Библиографический список

1. Отчет Центрального Банка РФ о финансовых преступлениях за 2020 год. Москва, 2021.

2. Сбербанк подсчитал, сколько денег мошенники украли у россиян в 2024 году : [Электрон. ресурс]. – URL: https://www.sravni.ru/novost/2025/3/4/sberbank-podschital-skolko-deneg-moshenniki-ukrali-u-rossiyan-v-2024-godu/ (дата обращения: 31.03.2025).

3. О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 13.02.2025 № 9-ФЗ : [Электрон. ресурс]. – URL: https://www.garant.ru/hotlaw/federal/1795171/ (дата обращения: 02.04.2025).

4. Фролова Е.А., Михайлов А.В. Современные вызовы кибербезопасности в банковской сфере // Вестник Московского университета. Серия Экономика. – 2019. – № 6. – С. 23–35.

5. Сайт Объединенного Кредитного Бюро : [Электронный ресурс]. – URL: https://credistory.ru/ (дата обращения: 02.04.2025).

Ручкина Наталья Сергеевна,

обучающаяся магистратуры («Цифровое право»)
Института права, социального управления и безопасности
ФГБОУ ВО «Удмуртский государственный университет».
Научный руководитель: Г.Г. Камалова, д-р юрид. наук, доцент,
зав. кафедрой информационной безопасности в управлении
ИПСУБ ФГБОУ ВО «УдГУ», г. Ижевск

ЭВОЛЮЦИЯ АВТОРСКОГО ПРАВА В ЦИФРОВОМ МИРЕ

Для произведений искусства обязательным признаком является наличие творческого характера[245].

[245] Рагимов О.В. Объекты авторского права в цифровом пространстве. URL: http://www.iolr.org›wp-content/uploads/2023/01/ (дата обращения: 15.03.2025).

Впервые представления об авторском праве появились в Риме и Древней Греции. Тексты трагедий исполнялись на сцене и подлежали сохранению. Так можно было проследить за сохранностью авторского замысла в произведении. Плагиат рассматривался как проступок.

При изобретении печатных станков возникает необходимость защищать авторское право. Для широкого круга лиц произведения быстро распространялись с помощью тиражирования промышленным типографским способом авторских произведений.

Авторам для защиты их прав органами власти выдавался документ (охранная грамота), который назывался «привилегией». Антонио Сабеллико в 1486 году получает одним из первых исключительное право печатать свое произведение.

В 1709 году в Великобритании принимают первый закон об авторском праве. Статут Королевы Анны (закон) 10 апреля 1710 г. вступает в силу.

В 1830 году Государственный совет утверждает документ под названием «Положение о правах сочинителей, переводчиков и издателей».

В Швейцарии в 1886 году принимается Бернская конвенция об охране литературных и художественных произведений. С этого момента начинается Международная защита авторских прав.

Основные принципы защиты авторских прав, которые закрепила Конвенция, применяются и в настоящее время.

Потребность в адаптации авторского права с помощью цифровой эпохи кардинально изменила способы создания, распространения и потребления контента.

Ужесточился контроль за копированием и распространением контента.

Были предприняты первые попытки регулирования в цифровой среде.

С помощью более гибкого подхода при развитии Интернета будут учитываться интересы авторов, пользователей и бизнеса.

Стремление современного авторского права в цифровом мире стремится к балансу защиты прав интеллектуальной собственности и обеспеченности доступа к информации.

Разрабатываются новые информационные модели, ведется борьба с пиратством и регулируются цифровые платформы. Инновации и свобода выражения не имеют ограничения.

Я считаю, что будущее авторского права – в дальнейшем развитии технологий и поиске оптимального баланса между интересами заинтересованных сторон.

Важную роль играют уважение к интеллектуальной собственности, а также повышение осведомленности пользователей об авторских правах.

По моему мнению, для защиты авторских прав новые возможности открываются с развитием децентрализованных технологий, например блокчейна.

Культура потребления контента, основанная на законности и этике, способна сформироваться с помощью образовательных программ и просветительской работы. Авторы подтверждают подлинность и происхождение своих произведений с помощью NFT (невзаимозаменяемых токенов), а также контролируют их распространение и получение вознаграждения.

Значимостью авторского права в условиях стремительного развития цифровых технологий является обеспечение защиты прав авторов и создателей контента.

Существует ключевая проблема – это онлайн-пиратство.

Воспитание уважения к авторским правам воспитывается с правосознанием пользователей и ведется борьба с пиратством. Нужно усиливать законодательство, которое касается авторских прав, а также развивать международное сотрудничество для борьбы с пиратскими ресурсами[246].

Сложностью является соблюдение авторских прав на платформах социальных сетей. Вирусные посты и репосты часто ведут к несанкционированному использованию и переработке оригиналь-

[246] Абрамова В.Т. Проблемы пиратства и нарушения авторских прав в цифровой среде URL: http://www.conf.siblu.ru›problemy-piratstva-i-narusheniya-…(статья) (дата обращения: 15.03.2025).

ного контента. С помощью социальных сетей есть возможность разрабатывать алгоритмы и системы, позволяющие отслеживать и предотвращать такие нарушения.

На данный момент создаются современные и адаптивные нормативно-правовые акты. Они будут учитывать специфику цифрового контента и онлайн-потребителей, эффективного развития авторского права и его адаптации к цифровизации[247].

Системы цифровой подписи, смарт-контракты и алгоритмы машинного обучения для обнаружения нарушений важно развивать, как новые технологии и новые инструменты для защиты авторских прав.

Депонирование – фиксация копии произведения может способствовать подтверждению факта авторства лица в конкретный момент времени[248].

Цифровые объекты обладают легкостью копирования и возможностью распространения без согласия правообладателя. Это нарушает авторские права, причиняется ущерб авторам и правообладателям.

Авторы не могут отследить пользователя сети, им сложно контролировать распространение контента[249].

Потребность в создании справедливого баланса нужно исключить и это будет способствовать защите авторских прав и праву общества на доступ к информации.

Защита авторских прав – это применение юридических мер, направленных преимущественно на их признание или восстановление[250].

Современные цифровые технологии кардинально трансформируют мир вокруг нас, все глубже проникая в нашу повседневную

---

[247] Серебровский В.И. Вопросы советского авторского права. М. : Изд-во Академии наук СССР, 1956. – 283 с.

[248] Царев Е.О. Депонирование авторских прав. URL: http://www.tsarev.biz›offtop/yavlyaetsya-li-deponirovanie-…(дата обращения: 17.03.2025).

[249] Иноземцев М.И., Нектов А.В. Зарубежные диссертации по цифровому праву: статистический и библиографический обзор. URL: http://www.digitallawjournal.org›jour/article/view/132/94…(дата обращения: 12.03.2025).

[250] Защита авторских прав на программы на ЭВМ: судебная практика и тенденция регулирования. URL: http://www.sudact.ru› Глава 70. Авторское право›Статья 1261 ГК РФ. Программы для ЭВМ (дата обращения: 13.03.2025).

жизнь. Меняются способы общения, ведения бизнеса, самореализации в творчестве[251].

Перечень способов защиты законодательно закреплен. К ним относятся гражданско-правовые способы (возмещение убытков, выплата компенсации и т.д.), административно-правовые и уголовно-правовые. Применяются в том случае, когда права авторов либо оспариваются, либо нарушаются[252].

Выбор способов защиты нарушенных интеллектуальных прав достаточно широк. При грамотном подходе можно восстановить нарушенные права и добиться справедливости как в суде, так и в досудебном порядке[253].

Авторское право будет эволюционировать. Будут разрабатываться новые механизмы защиты прав авторов. Повышение осведомленности пользователей о последствиях нарушения авторских прав будет играть ключевую роль в формировании новой культуры уважения к творчеству.

Судебное толкование, расширение использования лицензионных соглашений и саморегулирование в Интернете – вот что нужно использовать, как более гибкие инструменты. Задача же права на современном этапе заключается в определении юридических и этических рамок для подобных инструментов.

---

[251] Бойков В.А. Авторское право в эпоху развития цифровых технологий (статья) URL: http://www.intjournal.ru›wp-content/uploads/2021/11/… (дата обращения: 15.03.2025).

[252] Нормативно-технические документы, касающиеся авторского права в цифровом мире. Часть 4 Гражданского кодекса РФ. URL: http://www.consultant.ru›document/cons_doc_LAW_64629/…/ («Права на результаты интеллектуальной деятельности и средства индивидуализации») (дата обращения: 15.03.2025); Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ от 27.07.2006. Бернская Конвенция об охране литературных и художественных произведений от 09.09.1886 (ред. от 28.09.1979). URL: http://www.consultant.ru› document/cons_doc_LAW_61798/

[253] Матвеев А.Г. Цифровое и аналоговое авторское право: различны ли принципы? URL: http://www: cyberleninka.ru›article/n/tsifrovoe-i-analogovoe-… (дата обращения: 12.03.2025).

Мои предпочтения отдаются эффективной защите авторских прав, при этом необходимо проводить профилактическую работу среди пользователей интернета, совершенствовать технологии и укреплять законодательство.

Непрерывным должен быть процесс эволюции авторского права в цифровом мире. Он требует гибкости и адаптации. Авторское право должно развиваться в соответствии с изменениями, чтобы эффективно защищать права авторов и обеспечивать доступ к культурным продуктам. Нужно учитывать технологический прогресс и новые вызовы, стоящие перед обществом. Текущие изменения имеют огромное значение для будущих поколений, и их правильное управление будет определять картину авторского права в ближайшие годы[254].

Кабанова Валерия Алексеевна,

обучающаяся магистратуры («Цифровое право»)
Института права, социального управления и безопасности
ФГБОУ ВО «Удмуртский государственный университет»,
г. Ижевск

ПРАВОВЫЕ ВОПРОСЫ И ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ АВТОРСТВА ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОЗДАНИИ ПРОИЗВЕДЕНИЙ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

В эпоху стремительного роста технологий и экономического прогресса мы не можем представить жизнь без цифровых технологий и искусственного интеллекта.

[254] Бойков В.А. Авторское право в эпоху развития цифровых технологий. URL: http://www.intjournal.ru›wp-content/uploads/2021/11/ (дата обращения: 15.03.2025).

Еще три десятилетия назад невозможно было осознать, что среднестатистический человек будет пользоваться сложной техникой в повседневной жизни не только в случае необходимости, но и для простого досуга. Уже сейчас искусственный интеллект стал нашим неотъемлемым инструментом, и данный процесс развития технологий необратим.

Удобство использования искусственного интеллекта приводит к внедрению его в массы. Уже никого не удивляет автомобиль на автопилотном управлении, способный анализировать дорожную обстановку с высокой точностью; пылесос без провода, способный «запоминать» особенности периметра дома; телефон с голосовым управлением. Кажется, тенденцией современного общества стало перекладывание своих обязанностей на технические инновации, а также использование технологий для ускорения, оптимизации труда.

Технологические прорывы в сфере искусственного интеллекта радикально ускоряются благодаря достижениям в алгоритмах машинного обучения. Каждый год стремительного развития в технологическом процессе приводит к созданию новых форм искусственного интеллекта, то есть «юнитов». Юнит искусственного интеллекта – это отдельная, обособленная технологическая единица, носитель, устройство[255].

Технологический прогресс последнего десятилетия в особенности привёл к возможности и способности юнитов искусственного интеллекта «выполнять виды деятельности, которые раньше были предоставлены исключительно человеку, а также развивать определенные автономные и когнитивные особенности – например, способность учиться на опыте и принимать независимые решения»[256].

---

[255] Gürkaynak G., Yılmaz I., Doygun T., İnce E. Questions of Intellectual Property in the Artificial Intelligence Realm [Вопросы интеллектуальной собственности в сфере искусственного интеллекта] // Robotics Law Journal. 2017, September-October. P. 9 11.

[256] Пшеунова В. Проблема авторства в контексте развития искусственного интеллекта // Правовая защита интеллектуальной собственности: проблемы теории и практики : сб. матер. VI Междунар. юридич. фо-

Ярким примером скачка развития использования юнитов искусственного интеллекта обычными людьми стало внедрение их в повседневную жизнь. Для современного ребенка уже не удивительно, что неживая музыкальная колонка может вести диалог и становится своего рода няней, помощником в получении знаний и даже способом коммуникации.

Однако чем обширнее происходит внедрение искусственного интеллекта в повседневную жизнь людей, тем больше возникает потребности законодательного урегулирования данной области взаимодействия человека и технологий. С определенностью можно сказать, данная область взаимодействия совершенно новая для человеческой эпохи и поэтому несет за собой ряд непонимания и трудностей в систематизировании правил регулирования отношений, законов как с точки зрения философских суждений, так и на уровне морально-нравственных и этических пониманий[257].

Одной из быстроразвивающихся и полезных сфер применения искусственного интеллекта является сфера интеллектуальной собственности.

Искусственный интеллект стал неотъемлемым помощником не только ученых, но и творческих деятелей. Уже сегодня искусственный интеллект применяют музыканты, чтобы создать новые комбинации звучания нот. Его хорошо освоили дизайнеры – искусственный интеллект помогает быстро и качественно менять образы или исправлять детали заданного формата. Писатели и литературные редакторы теперь используют искусственный интеллект для написания произведений и даже статей в средствах массовой информации[258].

рума (IP Форума). М. : Издат. центр Московского гос. юридич. универс. им. О.Е. Кутафина (МГЮА), 2018.

[257] Сенников Н.Л. Соотношение права интеллектуальной собственности и права искусственного интеллекта – проблема постановки вопроса // News of Science and Education. 2017.

[258] Интернет-портал «Российской газеты» зарегистрирован в Роскомнадзоре 21.06.2012. Номер свидетельства ЭЛ № ФС 77 – 50379. Учредитель ФГБУ «Редакция «Российской газеты». Гл. ред. В.А. Фронин.

На данном этапе развития юнитов искусственного интеллекта их алгоритмы в обучаемости ограничены человеком. Программа еще не научилась самостоятельно придумывать новые элементы искусства, она лишь смешивает уже знакомые ей образы. Поэтому очеловечивать способность искусственного интеллекта на данный момент нельзя – программа не способна придумать или создать новое, как человечек способен создавать благодаря образному мышлению и способности фантазировать[259].

Однако обратимся к самой известной фразе всех творческих деятелей современности: «Кради, как художник»[260]. Смысл высказывания Остина Клеона заключается в том, что все результаты творчества опираются на созданные ранее предметы искусства, нет ничего совершенно оригинального. Уникальные результаты интеллектуальной собственности скрывают в себе основу старых идей, где порой сильно размыты границы оригинального начала и малого плагиата. Поэтому нельзя утверждать, что и искусственный интеллект не создает ничего нового, используя алгоритмы кодов, основанные на анализе существующих в сети объектов, точно также поступают и люди.

Исходя из вышесказанного, возникает необходимость в правовом регулировании объектов авторского права, образы и модели которых созданы с помощью юнитов искусственного интеллекта.

Проблема определения прав и обязанностей юнитов искусственного интеллекта касаемо создания ими объектов авторского права остается актуальным и непростым вопросом правоведов всего мира. Юнит искусственного интеллекта хорошо имитирует творческие функции человека, опережает его в быстроте решений и помогает в работе, однако физической формы не имеет, поэтому наделить юнит авторскими правами и обязанностями, как человека,

[259] Gürkaynak G., Yılmaz I., Doygun T., İnce E. Questions of Intellectual Property in the Artificial Intelligence Realm [Вопросы интеллектуальной собственности в сфере искусственного интеллекта] // Robotics Law Journal. 2017, September-October. P. 9 11.

[260] Клеон О. Кради как художник. 2024.

мы не можем. Это оставляет без ответа вопрос о правах в отношении произведений, созданных автономными юнитами искусственного интеллекта или при их фактически и юридически существенном участии.

Как отмечает Яни Ихалайнен, «существует пустое пространство между авторским правом и развивающейся сферой искусственного интеллекта. Подобно периоду возникновения интернета, кажется, что закон играет в догонялки, что ведёт к потенциально негативным результатам, притом, что быстрое развитие и внедрение искусственного интеллекта происходит в настоящий момент»[261].

Отсутствие правового регулирования в данной сфере может сделать творческие результаты незащищенными от плагиата злоумышленниками, а также приводит к недооцениваю результатов, созданных искусственным интеллектом. Произведения, созданные юнитами искусственного интеллекта, являются незащищёнными и не попадают под действие законодательства об интеллектуальной собственности. Игнорирование развития данной сферы уже невозможно, человечество не откажется от комфорта и многозадачности, которые достигаются посредством применения искусственного интеллекта в различных сферах деятельности.

Ряд ученых предполагает возможным наделить правами, обязанностями и ответственностью программистов, которые создали непосредственный юнит искусственного интеллекта. Другие ученые предполагают, что ответственность нести должен пользователь программы.

Тимоти Батлер в 1982 году на вопрос, кому принадлежат права на произведения, созданные нейросетью, писал, что есть четыре возможных пути признания авторских прав:

– наделить авторскими правами программы на основе искусственного интеллекта, либо распределить эти права между системой и человеком;

[261] Ihalainen J. Computer creativity: artificial intelligence and copyright [Компьютерное творчество: искусственный интеллект и авторское право] // Journal of Intellectual Property Law & Practice. 06.03.2018. P. 5.

– распределить авторские права между правообладателем программного обеспечения и владельцем компьютера;

– полностью отказаться от наделения искусственного интеллекта авторскими правами;

– создать вымышленного автора – человека и передать его авторские права правообладателю базового программного обеспечения или владельцу компании[262].

Исследователи Дипак Сомайя и Лав Р. Варшней выделяют 3 возможных варианта развития правого регулирования:

1) приравнять системы искусственного интеллекта к инструменту, наподобие краски и кисти;

2) наделить системы искусственного интеллекта правовым статусом социального агента, не имеющего собственных прав;

3) система искусственного интеллекта может выступать как социальный агент, наделенный некоторыми правами[263].

Находится несколько альтернативных путей решения указанных вопросов, с учетом положений действующего гражданского законодательства:

Во-первых, можно программу на основе искусственного интеллекта признать автором. В этом случае программа наделяется правосубъектностью и за ней признаются права.

На данный момент в Российской Федерации такое невозможно ввиду особенностей субъектного состава правоотношений и статьи 1257 ГК РФ[264] – автором произведения науки, литературы или искусства признается гражданин, творческим трудом которого оно создано, также автором может быть только физическое лицо или несколько физических лиц.

---

[262] Артений Л.С. Искусственный интеллект в авторском праве. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-vavtorskom-prave

[263] Артений Л.С. Искусственный интеллект в авторском праве. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-vavtorskom-prave

[264] Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ (ред. от 31.01.2016) // СЗ РФ. 1994. № 32.

Во-вторых, признать автором создателя интернет-платформы. Программист искусственного интеллекта будет обладать авторскими правами на саму технологию.

Такой вариант имеет место быть, так как согласно статье 1261 ГК РФ, автором станет создатель исходного кода на все виды программ для электронно-вычислительных машин. Однако творческого участия в создании самих произведений разработчик не будет принимать, он лишь ответственен за алгоритмы, на основе которых программа обучается и творит сама.

3. Признать автором пользователя платформы. Искусственный интеллект работает по принципу – пользователь вводит команду с помощью комбинаций слов, и за некоторое время искусственный интеллект генерирует готовое произведение. Данный вариант не противоречит ГК РФ. К тому же он наиболее предпочтителен в современных реалиях.

4. Признать соавторство пользователя и технологии. То есть искусственный интеллект признается полноценным соавтором произведения и имеет авторское право наравне с человеком. С точки зрения действующего законодательства такой вариант невозможен, потому что соавтор должен быть физическим лицом.

В законодательстве большинства стран произведения создаются физическими лицами, поэтому искусственный интеллект не может быть автором либо соавтором. Такая же ситуация и в России, автором может быть только физическое лицо.

Для улучшения положения Российской Федерации в вопросе защиты авторских прав произведений, созданных искусственным интеллектом, стоит пересмотреть законодательство РФ об авторстве, следует добавить положения о том, что автор не обязательно должен быть физическим лицом. Наиболее удобный вариант – соавторство человека и искусственного интеллекта.

В заключение хочется отметить, авторское право на данном этапе развития современной эпохи не может игнорировать роль искусственного интеллекта, применяемого в качестве инструмента человеком. Нейросети, использующие искусственный интеллект,

с каждым разом становятся более удобными и качественными в использовании и оказывают вспомогательную роль для создания объектов авторского права. Правовое регулирование данной области уже становится не просто актуальной проблемой, но и необходимостью поиска новых решений для усовершенствования законодательства.

Библиографический список

1. Пшеунова В. Проблема авторства в контексте развития искусственного интеллекта // Правовая защита интеллектуальной собственности: проблемы теории и практики : сб. матер. VI Междунар. юридич. форума (IP Форума). – Москва : Издат. центр Московского гос. юридич. универс. им. О.Е. Кутафина (МГЮА), 2018.

2. Сенников Н.Л. Соотношение права интеллектуальной собственности и права искусственного интеллекта – проблема постановки вопроса // News of Science and Education. – 2017.

3. Артений Л.С. Искусственный интеллект в авторском праве. – URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-avtorskom-prave

4. Ihalainen J. Computer creativity: artificial intelligence and copyright [Компьютерное творчество: искусственный интеллект и авторское право] // Journal of Intellectual Property Law & Practice. – 06.03.2018. – P. 5.

5. Gürkaynak G., Yılmaz I., Doygun T., İnce E. Questions of Intellectual Property in the Artificial Intelligence Realm [Вопросы интеллектуальной собственности в сфере искусственного интеллекта] // Robotics Law Journal. – 2017, September-October. – P. 9 11.

6. Клеон О. Кради как художник. – 2024.

Привалов Александр Альбертович,

обучающийся магистратуры Института права,
социального управления и безопасности ФГБОУ ВО
«Удмуртский государственный университет»,
г. Ижевск

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ МЕДИЦИНСКИХ ОРГАНИЗАЦИЯХ

В последние десятилетия информационные технологии стали неотъемлемой частью всех сфер человеческой деятельности, включая здравоохранение. В условиях стремительного развития цифровых технологий и внедрения электронных медицинских записей, системы управления пациентами и других информационных систем, вопросы информационной безопасности (ИБ) в медицинских организациях приобретают особую актуальность. Государственные медицинские учреждения, как ключевые элементы системы здравоохранения, сталкиваются с множеством вызовов, связанных с защитой персональных данных пациентов, что делает тему данной работы особенно важной и своевременной.

Актуальность проблемы информационной безопасности в медицинских организациях обусловлена не только увеличением объемов обрабатываемой информации, но и ростом числа кибератак, направленных на получение доступа к конфиденциальным данным.

В интервью CNews.ru Александр Мартынов, генеральный директор «РТ МИС», компании разработчика медицинской информационной системы «ЕЦП МИС» сказал: «Наша задача, сделать медицинскую ИТ систему настоящим помощником врача. Наша компания разрабатывает программное обеспечение для цифровизации государственных медицинских организаций, и сегодня продуктами «РТ МИС» пользуются более двух тысяч медучреждений в 32 регионах страны. Эффективность наших программных продуктов

можно оценить по показателям федерального проекта «Создание единого цифрового контура в здравоохранении на основе ЕГИСЗ».

Внедрение Минздравом России в медицинскую деятельность медицинских учреждений электронного документооборота и программного продукта «ЕЦП МИС» значительно облегчило работу врача, но данная система концентрирует всю информацию, в том числе и персональные данные всех пациентов, на федеральном уровне, что создает определенную озабоченность у пациентов по несанкционированному доступу к информации, содержащей их персональные данные и врачебную тайну.

Утечка персональных данных может привести к серьезным последствиям, включая финансовые потери, утрату доверия со стороны пациентов и даже юридические последствия для медицинских учреждений. В связи с этим необходимо не только осознавать риски, но и активно работать над их минимизацией, что требует комплексного подхода к обеспечению информационной безопасности.

Обеспечение информационной безопасности в государственных медицинских организациях требует четкого понимания законодательных аспектов, охватывающих как защиту персональных данных, так и правовые нормы, регулирующие работу с ними. В России наиболее значимыми документами являются Закон о персональных данных, а также постановления и приказы, отвечающие на современные вызовы в области информационной безопасности, в частности Приказ ФСБ России от 10 июля 2014 года № 378, который устанавливает требования к защите информации в системах, обрабатывающих персональные данные[265].

Согласно иным исследованиям, вопросы прав пациентов на защиту конфиденциальности их данных нуждаются в особом внимании. Эти права подчеркивают важность обеспечения врачебной тайны и сохранения безопасности предоставляемой информации. Законодательство акцентирует внимание на правомерности

[265] Любаева Д.Ю. Правовые аспекты защиты персональных данных в медицинских учреждениях // Контентус. 2022. № 9 (122). URL: https://cyberleninka.ru/article/n/pravovye-aspekty-zaschity-personalnyh-dannyh-v-meditsinskih-uchrezhdeniyah (дата обращения: 11.12.2024).

обработки медицинских записей и требует соблюдения условий, необходимых для их защиты[266]. В условиях роста cyber-угроз критически важным становится понимание, как информационные риски могут повлиять на функционирование медицинских учреждений. Недостаток информации о потенциальных угрозах и слабых местах в системах защиты только усугубляет эту проблему.

Правовые аспекты защиты персональных данных также состоят в harmonизации российской нормативно-правовой базы с международными стандартами. Таким образом, медицинские организации должны обеспечить выполнение различных обязательств перед пациентами и государственными инстанциями, что дает возможность не только снизить риски, но и повысить доверие со стороны граждан[267]. Нормативные акты также должны учитывать современные технологии и методы их интеграции в существующие информационные системы.

Всё это требует постоянного обучения и повышения квалификации медицинских специалистов. Они должны не только осознавать важность защиты данных, но и быть готовы применять на практике принятые в законодательстве принципы[268]. Кадры, работающие с информацией, должны быть способны защищать данные от утечек и киберугроз, что предполагает наличие соответствующих навыков и знаний.

---

[266] Шутова А.А. Угрозы информационной безопасности учреждений системы здравоохранения: уголовно-правовой аспект // Вестник Уфимского юридического института МВД России. 2023. № 3 (101). URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-uchrezhdeniy-sistemy-zdravoohraneniya-ugolovno-pravovoy-aspekt (дата обращения: 26.12.2024).

[267] Фохт О.А., Цветков А.А. Защита персональных данных. Новое в законодательстве: тенденции, вопросы практического применения в медицинских информационных системах // Врач и информационные технологии. 2013. № 5. URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-novoe-v-zakonodatelstve-tendentsii-voprosy-prakticheskogo-primeneniya-v-meditsinskih-informatsionnyh (дата обращения: 21.12.2024).

[268] Лапо Л.Г., Орехова Е.А. Информационные права в здравоохранении // Вестник Клинической больницы № 51. 2010. № 11. URL: https://cyberleninka.ru/article/n/informatsionnye-prava-v-zdravoohranenii (09.03.2025).

Отметим, что в последние годы законодательство претерпело изменения, касающиеся права пациентов на доступ к своей медицинской информации. Это право включает не только возможность ознакомиться с записями, но и требование о том, чтобы такие записи были защищены от неправомерного доступа и манипуляций со стороны третьих лиц[269]. Права пациентов должны исполняться в полной мере, что способствовало бы созданию более безопасной и прозрачной системы предоставления медицинских услуг.

Важной задачей для государственных медицинских учреждений становится следование современным законодательным инициативам в области защиты данных. Это включает не только соблюдение юридических норм, но и инициативы, направленные на создание защищенных информационных систем и программных решений, что, в свою очередь, требует новых подходов к подготовке кадров.

Принимая во внимание все вышеизложенное, становится очевидно, что уровень подготовки медицинских работников и соблюдение законодательства в области информационной безопасности взаимосвязаны. Профессиональное образование, которое включает курсы по правовым аспектам, этике и безопасности данных, может стать основой для эффективного взаимодействия между медицинскими специалистами и пациентами, создает атмосферу доверия и способствует повышению качества медицинского обслуживания.

Утечка персональных данных в медицинских учреждениях представляет собой одну из наиболее актуальных и серьезных проблем современного здравоохранения. В условиях растущей цифровизации и внедрения телемедицинских технологий ответственность за защиту электронных медицинских данных (ЭМД) возлагается как на медицинские организации, так и на медицинский персонал. Нарушения, связанные с утечкой данных, могут привести не только

[269] Любаева Д.Ю. Правовые аспекты защиты персональных данных в медицинских учреждениях // Контентус. 2022. № 9 (122). URL: https://cyberleninka.ru/article/n/pravovye-aspekty-zaschity-personalnyh-dannyh-v-meditsinskih-uchrezhdeniyah (дата обращения: 11.12.2024).

к финансовым убыткам для учреждений, но и к серьезным последствиям для здоровья и безопасности пациентов[270].

Риски утечки персональных данных в медучреждениях.

Основные факторы риска, способствующие утечке информации, включают несанкционированный доступ, кибератаки, использование вредоносного программного обеспечения и недостаточную подготовку кадров. Нередко случаи утечки происходят в результате ошибок сотрудников, которые не имеют достаточно знаний в области информационной безопасности. Работники медицинских организаций могут случайно разглашать конфиденциальную информацию, если не проходят соответствующее обучение или не осознают важность соблюдения правил защиты данных[271].

Также немаловажным фактором является отсутствие четкой регуляции в области обработки и использования персональных данных в рамках телемедицины. Это приводит к правовым пробелам,

[270] Исрафилов А. Кибербезопасность в медицине: защита электронных медицинских данных // Холодная наука. 2024. № 6. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-meditsine-zaschita-elektronnyh-meditsinskih-dannyh (дата обращения: 09.12.2024).

[271] Фохт О.А., Цветков А.А. Защита персональных данных. Новое в законодательстве: тенденции, вопросы практического применения в медицинских информационных системах // Врач и информационные технологии. 2013. № 5. URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-novoe-v-zakonodatelstve-tendentsii-voprosy-prakticheskogo-primeneniya-v-meditsinskih-informatsionnyh (дата обращения: 21.12.2024).

которые могут использоваться злоумышленниками для получения запрещенного доступа к данным. В условиях недостаточной правовой базы медицинские учреждения нередко не имеют четких инструкций по безопасности[272]. Применение технологий блокчейн может стать одним из решений, позволяющим значительно повысить уровень защиты данных, обеспечивая прозрачность и доверие к процессам обработки информации[273].

Отдельное внимание стоит уделить специфике кадровой подготовки медицинских работников. Инвестиции в обучение сотрудников вопросу кибербезопасности становятся важной частью формирования защитного механизма в любой медицинской организации. Без надлежащей подготовки даже лучшие технические средства не смогут предотвратить утечку данных, если персонал не знает, как с ними безопасно обращаться. Необходимо внедрять регулярные тренинги и повышать осведомленность о возможных рисках, связанных с работой с ЭМД.

Проблемы утечки данных не ограничиваются только техническими мерами. Фактором риска также может быть низкий уровень осведомленности пациентов о своих правах на защиту персональной информации. Большинство людей не знают, как могут защищать свои данные и какие меры принимает медицина для их защиты. Создание механизма отзыва согласия на обработку данных может помочь увеличить уровень доверия пациентов к медицинским организациям и снизить вероятность утечки информации[274].

---

[272] Брумштейн Ю.М., Захаров Д.А., Акишкин В.Г. Риски информационной безопасности медучреждений, их специалистов и пациентов // Информационная безопасность регионов. 2013. № 1 (12). URL: https://cyberleninka.ru/article/n/riski-informatsionnoy-bezopasnosti-meduchrezhdeniy-ih-spetsialistov-i-patsientov (дата обращения: 26.12.2024).

[273] Марков Б.Б. Проблемы защиты персональных данных в телемедицине. Блокчейн, гражданско-правовая ответственность и другие способы их преодоления // Юридические исследования. 2023. № 4. URL: https://cyberleninka.ru/article/n/problemy-zaschity-personalnyh-dannyh-v-telemeditsine-blokcheyn-grazhdansko-pravovaya-otvetstvennost-i-drugie-sposoby-ih (11.12.2024).

[274] Исрафилов А. Кибербезопасность в медицине: защита электронных медицинских данных // Холодная наука. 2024. № 6. URL: https://cyber-

Кроме того, важной часть управления рисками является контроль и аудит существующих процедур безопасности. Регулярные проверки систем безопасности помогут выявить уязвимости и исправить их до того, как они будут использованы злоумышленниками. Использование автоматизированных систем для мониторинга может помочь в реальном времени обнаруживать возможные атаки и реагировать на них соответствующим образом. Такой комплексный подход позволит значительно уменьшить риск утечек.

В заключение можно сделать вывод, что необходимость комплексного подхода к защите персональных данных в медицинских учреждениях становится очевидной. Это включает не только использование современных технологий, но и разработку четких регламентов, повышение информированности сотрудников и пациентов, а также подготовку кадров, способных эффективно справляться с задачами кибербезопасности.

Привалов Александр Альбертович,

обучающийся магистратуры Института права, социального управления и безопасности ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск

РОЛЬ КАДРОВОЙ ПОДГОТОВКИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕДИЦИНСКИХ ОРГАНИЗАЦИЯХ

Современные вызовы и угрозы в области информационной безопасности (ИБ) требуют от медицинских учреждений не только соблюдения законодательных норм, но и постоянного совершенствования профессиональных навыков специалистов, работающих с персональными данными пациентов. Кадровая подготовка в этой

---

leninka.ru/article/n/kiberbezopasnost-v-meditsine-zaschita-elektronnyh-meditsinskih-dannyh (дата обращения: 09.12.2024).

области играет ключевую роль, так как именно от квалификации медицинского персонала зависит уровень защиты информации и предотвращение утечек данных.

С начала информационной революции в сфере здравоохранения возникли новые подходы и требования к подготовке кадров. Специалисты должны быть ознакомлены не только с профессиональными аспектами своей работы, но и с основами информационной безопасности и современными угрозами, которые могут повлиять на целостность и конфиденциальность данных пациентов[275]. Важность таких знаний возрастает на фоне новых технологий, активно внедряемых в практику. В частности, внедрение цифровых технологий требует от врачей и других медицинских работников умения безопасно обращаться с информацией, учитывать риски, связанные с утечками данных, а также владеть основами кибергигиены.

Одной из основных проблем является недостаток комплексных образовательных программ, которые охватывали бы все аспекты информационной безопасности в медицинской сфере. Указанный недостаток является следствием устаревших учебных планов и недостаточного внимания со стороны учебных заведений к внедрению новых технологий в учебный процесс. Учебные заведения должны разработать программы, включающие дисциплины, направленные на формирование информационной компетентности у будущих специалистов[276]. Эти программы должны учитывать как теоретические, так и практические знания в области ИБ, что позволит выпускникам уверенно действовать в условиях повышенной угрозы утечек данных.

---

[275] Исрафилов А. Кибербезопасность в медицине: защита электронных медицинских данных // Холодная наука. 2024. № 6. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-meditsine-zaschita-elektronnyh-meditsinskih-dannyh (дата обращения: 09.12.2024).

[276] Гавришев А.А. Исследование отдельных вопросов управления кадрами по информационной безопасности в медицинских учреждениях // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2024. № 1. URL: https://cyberleninka.ru/article/n/issledovanie-otdelnyh-voprosov-upravleniya-kadrami-po-informatsionnoy-bezopasnosti-v-meditsinskih-uchrezhdeniyah (дата обращения: 09.03.2025).

Кроме того, изменения в законодательстве в области защиты персональных данных оказывают влияние на содержание образовательных программ. Необходимость соблюдения норм и правил, предусмотренных законодательством, требует от медицинских работников знания актуальных требований и стандартов, касающихся обработки и хранения персональной информации[277]. Это также подчеркивает важность сертификации специалистов в области ИБ, что поможет обеспечить соответствие квалификации работников современным требованиям.

Результаты исследования проблемы подготовки медицинских кадров к работе с информацией в специализированных учебных заведениях показали, что более 60 % ответивших на анкеты специалистов отметили отсутствие должного уровня подготовки по вопросам ИБ[278]. Это свидетельствует о необходимости реформирования образовательного процесса и внедрения новых форм обучения, таких как тренинги, семинары и курсы повышения квалификации, которые делают акцент на актуальных вопросах информационной безопасности.

Участие в различных мероприятиях, касающихся цифровизации здравоохранения, также способствует повышению информационной грамотности специалистов. Обмен опытом между медицинскими учреждениями и образовательными учреждениями помогает выявить слабые места в подготовке кадров и разработать эффективные решения для устранения этих недостатков[279]. Кроме того,

---

[277] Зайцева Т.Н., Бараксанова К.М. Анализ рисков информационной безопасности в центрах медицинской реабилитации: проблемы и перспективы. Обзор // Вестник восстановительной медицины. 2025. № 1. URL: https://cyberleninka.ru/article/n/analiz-riskov-informatsionnoy-bezopasnosti-v-tsentrah-meditsinskoy-reabilitatsii-problemy-i-perspektivy-obzor (09.03.2025).

[278] Керейтова М.Р., Малыш В.Н. Информационная безопасность в медицинских информационных системах // Труды Международного симпозиума «Надежность и качество». 2012. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 22.12.2024).

[279] Гулиев Я.И., Цветков А.А. Обеспечение информационной безопасности в медицинских организациях // Врач и информационные техно-

программы сотрудничества между государственными органами и образовательными учреждениями могут значительно улучшить качество подготовки специалистов, работающих в условиях, когда вопросы безопасности данных становятся приоритетными.

В современном контексте важно акцентировать внимание на создании гибкой системы образовательных курсов, которая бы учитывала быстрые изменения в сфере технологий и возникающие новые угрозы. Такие курсы должны быть направлены на формирование у студентов практических навыков в области безопасности данных, чтобы они могли не только следовать установленным протоколам, но и самостоятельно определять меры по предотвращению инцидентов, связанных с утечками информации.

Вопросы информационной безопасности в медицинских учреждениях касаются не только защиты данных, но и обеспечения доверия пациентов, что, в свою очередь, отражается на качестве предоставляемых услуг. Правильная кадровая подготовка позволит не только повысить квалификацию работников, но и создать наиболее безопасную среду для обслуживания пациентов, что является основным приоритетом в здравоохранении.

Таким образом, кадровая подготовка медицинских работников является важным аспектом обеспечения информационной безопасности в государственных медицинских организациях. Разработка и внедрение современных образовательных программ, соответствующих требованиям времени, позволят повысить уровень управления рисками и защиты информационных систем, что, в свою очередь, положительно скажется на общем уровне здоровья населения.

Современное обучение в сфере информационной безопасности в медицинских организациях представляет собой важный аспект, учитывая рост числа инцидентов, связанных с утечками и несанкционированным доступом к персональным данным пациентов. В этих условиях актуальность образовательных программ, направленных

логии. 2016. № 6. URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-meditsinskih-organizatsiyah (11.12.2024).

на подготовку специалистов по информационной безопасности, не вызывает сомнений. Учебные программы, такие как те, что предлагает центр «Информзащита», акцентируют внимание на ключевых аспектах защиты электронных медицинских данных и формировании компетенций, необходимых для полноценного управления рисками информационной безопасности в медицинских учреждениях[280].

Кадровое обеспечение системы информационной безопасности является одним из популярных направлений в образовательных инициативах. Важно, чтобы учебные программы соответствовали современным требованиям и стандартам, установленным законодательством и другими нормативными актами. Настоящая необходимость в обучении сотрудников отражает растущие вызовы, связанные с кибератаками и утечками персональных данных, что, в свою очередь, требует системного подхода к организации учебного процесса.

Обучение становится двусторонним процессом, который не только передает знания, но и формирует культуру безопасности среди медицинских работников. Доступные программы включают в себя как теоретические аспекты, так и практические задания, что позволяет специалистам развивать навыки, необходимые для эффективного реагирования на угрозы безопасности[281].

К примеру, обучение должно охватывать темы, связанные с конфиденциальностью электронных медицинских данных (ЭМД), их защитой и процессами управления инцидентами. Эти аспекты вписываются в развитие общей стратегии кибербезопасности учреждения.

---

[280] Бурькова Е.В. Профессиональная подготовка специалистов в области информационной безопасности // Вестник Оренбургского государственного университета. 2016. № 2 (190). URL: https://cyberleninka.ru/article/n/professionalnaya-podgotovka-spetsialistov-v-oblasti-informatsionnoy-bezopasnosti (дата обращения: 10.12.2024).

[281] Исрафилов А. Кибербезопасность в медицине: защита электронных медицинских данных // Холодная наука. 2024. № 6. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-meditsine-zaschita-elektronnyh-meditsinskih-dannyh (дата обращения: 09.12.2024).

Не менее важным является понимание текущих угроз кибербезопасности, которые вызывают рост интереса к дальнейшему обучению и повышению квалификации. Специалисты должны уметь не только предотвращать инциденты, но и реагировать на них, уметь проводить анализ ситуации и делать выводы на основе полученных данных. Поэтому многие образовательные учреждения включают в свои программы изучение реальных кейсов, что помогает сформировать более глубокое понимание проблем безопасности в практической плоскости.

Практическая часть подготовки также становится важной составляющей. Исследования показывают, что практические занятия обеспечивают более высокую степень усвоения материала по сравнению с традиционными лекциями. Включение в обучение симуляторов ситуаций кибератак или утечек позволяет медицинским работникам получить реальный опыт и уверенность в своих действиях в критических ситуациях[282].

Кадровая политика в области информационной безопасности медицинских организаций требует внимания к множеству факторов, включая быстрое развитие цифровых технологий. Эти технологии уже сейчас внедряются в процессы управления, оптимизируя их и позволяя более эффективно использовать человеческие ресурсы. Внедрение систем управления, таких как ERP, CRM и HRM, открывает новые возможности для планирования и контроля за работой персонала, но также создает новые вызовы в аспекте информационной безопасности[283].

---

[282] Бурькова Е.В. Профессиональная подготовка специалистов в области информационной безопасности // Вестник Оренбургского государственного университета. 2016. № 2 (190). URL: https://cyberleninka.ru/article/n/professionalnaya-podgotovka-spetsialistov-v-oblasti-informatsionnoy-bezopasnosti (дата обращения: 10.12.2024).

[283] Задворная О.Л., Алексеев В.А., Борисов К.Т. Кадровые риски в обеспечении безопасности медицинской деятельности // МИР (Модернизация. Инновации. Развитие). 2017. № 1 (29). URL: https://cyberleninka.ru/article/n/kadrovye-riski-v-obespechenii-bezopasnosti-meditsinskoy-deyatelnosti (дата обращения: 21.01.2025).

Ключевая проблема заключается в недостаточной подготовке кадров. В современных условиях, когда информация становится важнейшим активом, даже незначительные ошибки в ее обработке могут привести к серьезным последствиям. Особенности кадрового менеджмента в медицинских учреждениях накладывают свои ограничения, так как медработники часто не обладают необходимыми навыками работы с информационными системами и данными. Это порождает серьезные риски, связанные с несанкционированным доступом к персональной информации пациентов и ее возможной утечкой.

Для решения этих проблем необходимо формирование системы непрерывного обучения и повышения квалификации медицинского персонала. Инновационные образовательные программы, ориентированные на информационную безопасность, помогут увеличить осведомлённость сотрудников об актуальных рисках и методах защиты данных. Важно, чтобы такие программы включали практическое применение знаний, а не ограничивались теоретическими знаниями. Здоровая кадровая политика должна основываться на системном подходе, который учитывает как получение новых знаний, так и внедрение technologies, которые облегчают выполнение задач[284].

Анализ текущей ситуации в сфере здравоохранения России показывает, что проблемы, связанные с кадровой подготовкой, в основном обусловлены недостатком квалифицированных специалистов и низкой оплатой труда. Это приводит к тому, что медицинские организации сталкиваются с дефицитом кадров, что, в свою очередь, ухудшает общее качество оказания медицинских услуг и увеличивает риски в области информационной безопасности.

Современные тенденции показывают, что цифровизация кадрового менеджмента становится неотъемлемой частью управления персоналом. Цифровые технологии не только сокращают временные затраты на рутинные задачи, но и позволяют собирать, обраба-

[284] Шуталев П.И., Молокова Е.Л. Цифровые технологии кадрового менеджмента в медицинских учреждениях // StudNet. 2022. № 1. URL: https://cyberleninka.ru/article/n/tsifrovye-tehnologii-kadrovogo-menedzhmenta-v-meditsinskih-uchrezhdeniyah (дата обращения: 19.12.2024).

тывать и анализировать данные о работе персонала. Использование этих технологий помогает выявлять слабые места в работе организаций и вносить соответствующие коррективы. Технологические решения, которые поддерживают автоматизацию управления кадрами и позволяют вести мониторинг задач, способствуют снижению риска человеческой ошибки и повышают уровень безопасности.

Разработка и внедрение специализированных подходов к обучению медработников в области информационной безопасности приведет к улучшению общей ситуации в здравоохранении. Систематический анализ и понимание рисков, связанных с работой медицинского персонала с информацией, позволит предотвратить множество инцидентов, связанных с утечкой данных. Важно, чтобы руководители медицинских организаций принимали активное участие в формировании стратегий кадровой подготовки, ориентированных на повышение уровня безопасности.

Таким образом, для уменьшения рисков в области информационной безопасности требуется комплексный подход, включающий как подготовку кадров, так и использование современных технологий управления. Это позволит значительно повысить уровень защиты персональных данных и увеличить доверие со стороны пациентов к системе здравоохранения. Каждая организация должна принять на себя ответственность за обучение своих сотрудников, что необходимо для обеспечения как их профессионального роста, так и безопасной и эффективной работы всей системы.

Важно, чтобы все заинтересованные стороны, включая государственные органы, образовательные учреждения и медицинские организации, работали совместно для достижения этой цели.

Рубинович Софья Дмитриевна,

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

РАЗРАБОТКА МОДУЛЯ ДЛЯ ITAM-СИСТЕМЫ НА БАЗЕ OPEN SOURCE РЕШЕНИЯ

С течением времени и развитием технологий, инфраструктура становится все более сложной и динамичной. Постоянное увеличение количества активов, внедрение технологий виртуализации и разнообразие конфигураций значительно усложняют управление информационными активами. При отсутствии полного перечня используемых активов организации сталкиваются с такими проблемами, как –

- высокие операционные риски;
- отсутствие контроля над активами;
- невозможность отслеживать изменения в конфигурациях;
- высокие риски инцидентов в результате эксплуатации уязвимостей.

В ответ на эти цифровые вызовы организации обращаются к системам управления ИТ-активами (ITAM), которые помогают обеспечить эффективное использование ресурсов, снижение затрат и минимизацию рисков, связанных с безопасностью.

При выборе платформы для реализации ITAM-системы были рассмотрены несколько популярных решений с открытым исходным кодом: Netbox, Wazuh и OpenSource Dashboard. Сравнительный анализ показал следующее[285]:

[285] Документация Netbox. URL: https://netbox.readthedocs.io

1. Управление активами

- Netbox полностью охватывает управление активами, включая физические устройства, виртуальные машины, сети и их взаимосвязи.
- Wazuh фокусируется на безопасности, но практически не предоставляет функций для управления активами.
- В OpenSource Dashboard отсутствует встроенный функционал для управления активами.

2. IPAM/DCIM

- Netbox обладает мощными возможностями для управления IP-адресами и центрами обработки данных.
- Wazuh, как и OpenSource Dashboard, не имеет встроенного функционала для IPAM или DCIM.

3. Интеграция с другими системами

- Netbox поддерживает интеграцию с широким спектром систем через API.
- Wazuh и OpenSource Dashboard имеют ограниченные возможности для работы с активами и сетевой инфраструктурой.

На основе проведенного анализа для решения проблем представленных выше был выбран продукт с открытым исходным кодом Netbox, который предоставляет широкий функционал для управления активами, включая IPAM (управление IP-адресами), DCIM (управление оборудованием дата-центров) и интеграцию с внешними системами через API.

Netbox, включающий в себя хороший функционал, разрешает подключить к себе любой модуль. Разработка модуля поможет автоматизировать анализ конфигураций виртуальных машин и выявлять уязвимости, тем самым повышая уровень безопасности инфраструктуры.

Модуль включает в себя определенные функции:

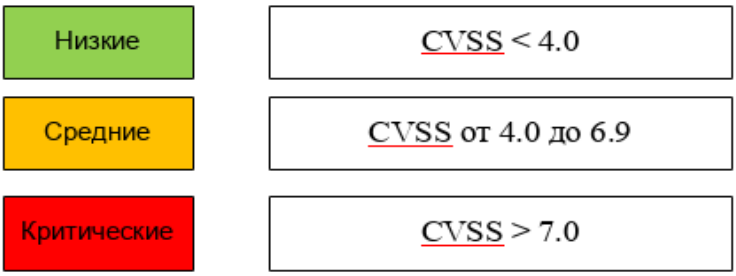
1. Сбор конфигураций с использованием шаблонов OpenSCAP[286] для анализа защищенности виртуальных машин.

[286] OpenSCAP Security Guide. URL: https://www.open-scap.org

2. Подтягивание уязвимостей, в том числе интеграция с базами данных уязвимостей (CVE, BDU).

3. CVSS-оценка[287]:

Классификация уязвимостей по уровню критичности:



4. Информирование, помогающее уведомить администраторов через email или Telegram.

Преимущества модуля:

- повышение безопасности инфраструктуры;
- централизация данных об уязвимостях и их критичности;
- упрощение процесса исправления проблем.

Работа модуля основана на многоступенчатом процессе, который начинается со сбора данных о конфигурациях через API гипервизоров (например: VMware vSphere, Proxmox, KVM). Собранные данные анализируются с использованием шаблонов OpenSCAP, которые проверяют защищенность системы по заранее определенным правилам, таким как наличие незащищенных портов или устаревших версий программного обеспечения. Дальше модуль отправляет запросы к базам данных уязвимостей (например CVE и BDU) для получения актуальной информации о потенциальных рисках и угрозах.

После обновления баз данных и получения необходимой информации происходит присвоение уровня критичности на основе CVSS-оценок. Модуль автоматически классифицирует уязвимости. В модуле присутствует информирование сотрудников о возникающих

[287] NIST National Vulnerability Database (NVD). URL: https://nvd.nist.gov

уязвимостях или проблемах в инфраструктуре. Уведомления отправляются администраторам через выбранный канал email или Telegram.

5. Результатами внедрения модуля являются:

- уменьшение времени реакции на новые уязвимости;
- структурированный подход к управлению активами;
- улучшение процессов мониторинга и исправления уязвимостей.

Разработанный модуль для Netbox позволяет автоматизировать процессы анализа конфигураций виртуальных машин и выявления уязвимостей, что значительно повышает уровень безопасности ИТ-инфраструктуры. Выбор Netbox в качестве основы для реализации обусловлен его гибкостью, активным сообществом и возможностью кастомизации. Предложенный подход может быть адаптирован под нужды организации, обеспечивая эффективное управление активами и минимизацию рисков.

Научное издание

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Сборник статей
Всероссийской научно-практической конференции
с международным участием

28 марта 2025 г.

Авторская редакция
Макет и компьютерная верстка:
И.А. Бусоргина

Подписано в печать 24.10.2025. Формат 60x84 1/16
Усл. печ. л. 13,07. Уч. изд. л. 8,94.
Тираж 27 экз. Заказ № 1620.

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, г. Ижевск, ул. Университетская, 1, корп. 2.
Тел. 68-57-18