Научная статья
УДК 342.951:351.82
DOI: 10.47475/2311-696X-2024-40-1-48-52

С. 48–52

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРАВОВОМ ПОЛЕ: СТРАТЕГИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ЗАЩИТЫ КИБЕРПРОСТРАНСТВА

Марина Николаевна Степанова
Российский государственный университет правосудия, Уральский филиал, Челябинск, Россия
mns017@mail.ru
https://orcid.org/0009-0006-3562-8705

Аннотация. В данной статье исследуется сложная и многоуровневая проблематика информационной безопасности национального масштаба, с акцентом на необходимость комплексного подхода для защиты национальных интересов Российской Федерации в этой сфере. Автор подчеркивает важность разработки и усовершенствования киберинфраструктуры, актуализации контроля за циркуляцией информационного контента в соответствии с законодательством РФ, а также совершенствования законодательных рамок, адаптированных к вызовам современных технологий. Статья освещает стратегические ориентиры развития информационного пространства РФ, заложенные в стратегических документах на период с 2017 по 2030 годы, уделяя внимание интеграции ИКТ в различные секторы экономики и государственного управления. Основной нормативный акт, регулирующий информационные технологии в России, Федеральный закон № 149-ФЗ, рассматривается как фундамент для установления принципов свободного обмена информацией. Кроме того, в статье отмечается особая роль России в формировании международной конвенции ООН по кибербезопасности и подчеркивают успехи российских инициатив на международном уровне, включая проекты, поддержанные комитетом Генеральной Ассамблеи ООН. Статья также касается вопросов унификации норм киберзащиты и защиты интеллектуальной собственности в контексте развития модели интернета, способствующей суверенитету и безопасности. Приводится пример зарубежного опыта, где правительственные руководящие документы по технологиям демонстрируют важность межсекторального взаимодействия для достижения технологической синергии.

Ключевые слова: информационная безопасность, киберсуверенитет, кибербезопасность, Федеральный закон РФ «Об информации...», международное сотрудничество, ООН, конвенция по кибербезопасности, интеллектуальная собственность, законодательство, технологическая самостоятельность

Для цитирования: Степанова М. Н. Информационная безопасность в правовом поле: стратегии правового регулирования и защиты киберпространства // Правопорядок: история, теория, практика. 2024. № 1 (40). С. 48–52. DOI: 10.47475/2311-696X-2024-40-1-48-52

Research article

INFORMATION SECURITY IN THE LEGAL FIELD: STRATEGIES FOR LEGAL REGULATION AND PROTECTION OF CYBERSPACE

Marina N. Stepanova
Russian State University of Justice, Ural Branch, Chelyabinsk, Russia
mns017@mail.ru
https://orcid.org/0009-0006-3562-8705

Abstract. This article explores the complex and multi-level issues of national-scale information security, with an emphasis on the need for a comprehensive approach to protect the national interests of the Russian Federation in this area. The author emphasizes the importance of developing and improving cyber infrastructure, updating control over the circulation of information content in accordance with Russian legislation, and improving legislative frameworks adapted to the challenges of modern technologies. The article highlights the strategic development objectives of the Russian information space, set out in the strategic document for the period from 2017 to 2030, with a focus on integrating ICT into various sectors of the economy and government. The main regulatory act governing information technologies in Russia, Federal Law No. 149-FZ, is considered as the

foundation for establishing principles of free exchange of information. In addition, the article notes Russia's special role in shaping the UN Convention on Cybersecurity and emphasizes the successes of Russian initiatives at the international level, including projects endorsed by the UN General Assembly Committee. The article also addresses the issues of unifying norms of cyber protection and intellectual property protection in the context of developing an internet model that promotes sovereignty and security. The example of the United Kingdom is given, where government guidance documents on technologies demonstrate the importance of cross-sectoral cooperation to achieve technological synergy.

Keywords: information security, cyber sovereignty, cyber security, Federal Law of the Russian Federation "On Information…", international cooperation, UN, cyber security convention, intellectual property, legislation, technological independence

For citation: Stepanova MN. Information security in the legal field: strategies for legal regulation and protection of cyberspace. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(1):48-52. DOI: 10.47475/2311-696X-2024-40-1-48-52 (In Russ.)

Введение

Недавние исследовательские работы указывают на то, что инновационная активность стала фундаментом, на котором строится прогресс международного сообщества, и представляет собой ключевой элемент, стимулирующий всеобщее экономическое развитие [1]. В контексте нынешней эры, стремление компаний к увеличению своей рыночной стоимости и достижению лидирующих позиций среди конкурентов приводит к внедрению передовых цифровых технологий в промышленности. Эти технологии совокупно обозначаются как «Индустрия 4.0», что представляет собой ключевую составляющую четвертой промышленной революции, также известной как «цифровая революция» [2].

В эпоху распространения цифровых инноваций, охватывающих социальные связи, бизнес-инициативы и механизмы управления на государственном уровне, правоприменительная сфера испытывает глубокие трансформации, вызванные проникновением современных цифровых технологий. Исследователи, анализирующие процессы цифрового преобразования в юридическом контексте, указывают на появление множества новаторских юридических явлений, которые затрагивают участников правоотношений и предметы правового урегулирования, а также взывают к переосмыслению концепции и основы цифровых прав и прочих аспектов.

Стратегический документ, определяющий направления развития информационного пространства Российской Федерации в течение 2017–2030 гг., подчеркивает, что информационно-коммуникационные технологии (далее — ИКТ) были интегрированы в управленческие структуры широкого спектра экономических секторов, включая сферы государственного регулирования, оборонные возможности страны, обеспечение общественного порядка и национальную безопасность.

Основным нормативным источником Российской Федерации в сфере информационных технологий является Федеральный закон № 149-ФЗ, принятый 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»[1]. Этот закон устанавливает принципы, согласно которым все участники могут свободно обмениваться и распространять информацию в отсутствие специальных федеральных ограничений, регулирующих этот доступ.

Описание исследования

Сегодня ученые уверенно заявляют о конвергенции цифрового и физического миров, о возникновении кибер-физического пространства и формировании уникального явления, называемого «Индустрия 4.0». Это явление характеризуется интеграцией и применением инновационных, революционных технологий в сфере цифровизации [2; 3].

Процесс цифровой трансформации оказывает весомое влияние на системы управления, включая структуры государственного аппарата. Используя новейшие технологии, граждане и интернет-пользователи приобретают упрощенный доступ к общественным услугам [4, с. 75]. Правительства индустриально развитых государств инициируют стратегические проекты для создания и совершенствования электронных интерфейсов, предназначенных для выполнения широкого спектра государственных задач. В Российской Федерации, такие действия определены в программе «Открытое правительство», реализация которой строится на фундаментальных принципах прозрачности, предусмотренных в документе об обеспечении доступа к информации, которой располагают федеральные органы исполнительной власти [5, с. 83].

Преобразование цифровых технологий радикально трансформировало традиционные методы взаимодействия между органами государственной власти, бизнес-сектором и гражданами, прежде всего в сферах, связанных с созданием, адаптацией и практическим применением новаторских

[1] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.11.2023) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 27.11.2023).

технологических решений. Одним из ярких примеров таких изменений является пакет руководящих документов, разработанный правительством Великобритании в 2013 году и пересмотренный в 2016 году, известный как Свод практических правил по технологиям[1]. Этот документ устанавливает ключевые принципы для эффективного партнерства и совместной работы между различными участниками общественных отношений.

Широкое внедрение цифровых технологических решений, в частности основанных на децентрализованных методах управления данными, каковым является блокчейн, спровоцировало создание и внедрение новых юридических механизмов и инструментов. Примерами таковых стали смарт-контракты, системы электронных цифровых подписей, а также установление базовых норм и стандартов в сфере высоких технологий. Проникновение и интеграция цифровых технологий в государственные информационные системы, в том числе регистры недвижимости и базы законодательных документов, стало обыденностью, а их использование охватило и другие направления, включая управление налоговыми процессами, оборот документации, организацию государственных услуг, контроль и управление комплексными процессами и системами в промышленности.

Мы убеждены, что интеграция цифровых новшеств может радикально изменить методы осуществления правовых процедур, обеспечивая защиту не только базовых прав человека, но и поддерживая его физическое благополучие и конфиденциальность персональных данных при взаимодействии и обмене информацией в цифровом мире.

Защита информационных данных стоит в центре внимания в области правовых нормативов. В докладе, опубликованном Европолом в 2017 году под названием «Анализ угроз от организованной киберпреступности»[2], были выделены основные области, в которых киберпреступность представляет наибольшую опасность. К основным угрозам в киберпространстве относятся атаки на критически важную инфраструктуру, такую как энергетические системы, транспорт и промышленные узлы, а также на устройства интернета вещей. Распространяются вирусы-вымогатели, банковские трояны, проводятся DDoS-атаки и создаются ботнеты. Проблемы вызывают действия, связанные с онлайн-мошенничеством через использование платежных карточек и электронных платежей, а также киберпреступления, основанные на социальной инженерии и злоупотреблении шифрованием. Распространение нелегального контента, включая материалы о сексуальном насилии над детьми, террористический контент в сети, торговле оружием, наркотиками и другими запрещенными товарами, торговле людьми, обороте поддельных товаров и незаконном использовании известных брендов также остаются серьезными проблемами. Преступления с криптовалютой, включая мошенничество и отмывание денег, усугубляются трансграничным характером киберпреступности.

С появлением передовых цифровых форм активов, включая криптовалюты и различные виды токенов, с повышением доступности финансовых онлайн-услуг возникают угрозы, касающиеся как отмывания средств, полученных противозаконным путем, так и финансирования деятельности, запрещенной законом. Деятельность «Группы разработки финансовых мер борьбы с отмыванием денег» (FATF) — международного органа, задействованного в создании стратегий противодействия отмыванию капитала, — подчеркивает важность объединения усилий стран для препятствия использованию электронных валют для финансирования противоправной и террористической активности[3].

Усиление акцента на защите информации происходит вслед за развитием новейших незаконных методов в сфере IT. В интернет-банкинге весьма частым является неправомерное изъятие средств из аккаунтов через эксплойты, которые используют уязвимости программного обеспечения для атак на компьютеры и иные информационно-телекоммуникационные устройства, взаимодействующие в сети Интернет. Киберсквоттинг заключается в регистрации доменных имен, сходных с имеющимися или заметно похожих на другие средства идентификации, такие как торговые марки, с целью их дальнейшей перепродажи.

Манипуляции на финансовых рынках, основанные на неправомерном использовании информации, считаются вредоносными экономическими стратегиями. В рамках российского права, в частности в соответствии со ст. 5 федерального закона № 224-ФЗ[4] и ст. 185.3 Уголовного кодекса Российской Федерации (далее — УК РФ), такие манипуляции признаются преступлением. Они характеризуются сознательным

[1] The Technology Code of Practice : Guidance // GOV.UK. URL: https://www.gov.uk/guidance/the-technology-code-of-practice (дата обращения: 27.11.2023).

[2] European Union Serious and Organised Crime Threat Assessment 2017. Crime in the age of technology // Europol. URL: https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 (дата обращения: 27.11.2023).

[3] FATF (2019), Anti-money laundering and counter-terrorist financing measures — Russian Federation, Fourth Round Mutual Evaluation Report. FATF, Paris. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Russian-Federation-2019.pdf (дата обращения: 27.11.2023).

[4] О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 27.07.2010 № 224-ФЗ (ред. от 04.08.2023) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_103037/ (дата обращения: 27.11.2023).

распространением ложной информации через общедоступные коммуникационные каналы, включая сеть Интернет, что приводит к искажению ценовых показателей и объемов торговли, созданию искусственно искаженных рыночных условий.

В сфере информационной безопасности в уголовном законодательстве предусмотрены самостоятельные составы преступлений, которые включают мошенничество с использованием платежных карт (ст. 159.3 УК РФ) и в информационных технологиях (ст. 159.6 УК РФ). Другие нормы российского уголовного закона (ст. 272–274 УК РФ) предусматривают ответственность за неавторизованный доступ к информации, создание и распространение вредоносного программного обеспечения и нарушение эксплуатации информационных систем, в том числе сетей связи. В то же время для преступлений в IT-секторе характерен ряд специфических действий, охватывающих нелегальный доступ к данным, распространение вирусов, а также преднамеренные действия, изменяющие работу компьютерного оборудования, что ведет к нарушению обработки информации и может привести к незаконному завладению имуществом.

Федеральный закон № 149-ФЗ (ст. 15.2 и 15.3), устанавливает обязанность провайдеров связи, посредников в сфере информационных технологий, а также владельцев доменов или лиц, реально управляющих ими, принимать меры по ограничению доступа к цифровому контенту в сетях связи, в том числе в сети Интернет, в случаях незаконного распространения материалов, нарушающих авторские и смежные права, если такое распространение не было санкционировано правообладателем или не имело других законных оснований, а также при нарушении процедур блокировки контента, содержащего призывы к массовым беспорядкам.

Информационная безопасность включает защиту индивидуальной информации в электронной сфере, включая Big Data и учётные системы, а также сохранение приватности в общении через соцсети и мессенджеры. Статья 15.8 федерального закона № 149-ФЗ запрещает провайдерам анонимных сервисов, в том числе VPN, облегчать доступ к ресурсам в интернете, блокировку которых предписывает российское законодательство.

Защита конфиденциальных данных и неприкосновенность личной информации становятся ключевыми элементами информационной безопасности на фоне растущих киберугроз. Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»[1] устанавливает четкие рамки для обработки личных и биометрических данных.

Мировое сообщество активно развивает нормативную основу, направленную на укрепление информационной безопасности в сетевых пространствах, принимая цифровые стратегии. Например, Еврокомиссия в феврале 2013 года утвердила Европейскую стратегию кибербезопасности, направленную на установление единых стандартов безопасности и координацию действий против киберугроз.

Обращаясь к зарубежному опыту, следует отметить, что Великобритания ежегодно тратит на борьбу с киберпреступностью от 18 до 27 млрд фунтов, что подчеркивает необходимость активных мер со стороны государств для защиты цифрового пространства. В США действуют Закон об авторском праве в цифровую эпоху (1998) и Закон CLOUD (2018), который позволяет американским властям получать данные из-за рубежа [6, с. 31].

С мая 2018 года в ЕС действует Общий регламент по защите данных (GDPR)[2], который стал обязателен для выполнения во всех странах-членах. Увеличение объемов информации и ее глобальный доступ повышают вопросы ее защиты и законного использования, делая информационную безопасность частью национальных стратегий развития.

С 2014 года в России обсуждается проект Концепции стратегии кибербезопасности, представленный в Совете Федерации, что отражает актуальность и значимость этой инициативы в контексте национальной безопасности[3].

Цифровизация активно продвигает технологические инновации, порождающие сложные юридические вопросы в цифровой среде. При этом критическое значение приобретает защита интеллектуальной собственности и интересов правообладателей. Ведущей задачей становится обеспечение надежной защиты интеллектуальной собственности в интернете и сохранение конфиденциальности в мировой информационной сети.

Разработка более совершенной модели интернета, обеспечивающей суверенитет и безопасность, а также уважение к личной жизни, становится ключевой для защиты интеллектуальной собственности в сети. Именно поэтому, представляется целесообразным унифицировать нормы киберзащиты в законодательстве, например, в рамках Федерального закона РФ «Об информации…».

В контексте информационной безопасности России важно определить ключевые направления

[1] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 27.11.2023).

[2] Регламент Европейского Парламента и Совета Европейского союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR) // СПС «Гарант». URL: https://base.garant.ru/71936226/ (дата обращения: 27.11.2023).

[3] Концепция стратегии кибербезопасности Российской Федерации : проект. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 27.11.2023).

госполитики и механизмы реализации в сфере международной кибербезопасности. Двустороннее международное сотрудничество в этой области требует эффективной деятельности по созданию международной конвенции ООН по кибербезопасности, проект которой уже получил поддержку на уровне комитета Генеральной Ассамблеи ООН, благодаря инициативе России в ноябре 2018 года [7, с. 39].

Заключение

Подводя итоги настоящего исследования, необходимо сформулировать вывод о том, что для обеспечения эффективной защиты национальных интересов в сфере информационной безопасности необходим комплексный подход, включающий разработку и усовершенствование инфраструктуры киберзащиты, оптимизацию контроля за распространением контента в соответствии с законодательством РФ и улучшение законодательных рамок, адаптированных к современным технологиям. Кроме того, важна активная роль России в международном сотрудничестве по вопросам кибербезопасности, в частности, через инициативу по созданию международной конвенции ООН. Укрепление правовых механизмов в сфере защиты интеллектуальной собственности и предотвращение угроз информационному пространству выделяются как ключевые аспекты стратегии информационной безопасности России.

Список источников

1. Архипова М. Ю., Соболев М. А. Исследование динамики развития национальной инновационной системы России (часть 1) // Государственное управление. Электронный вестник. 2022. № 90. С. 90–107. DOI: 10.24412/2070-1381-2022-90-90-107

2. Наливайченко Е. В. Развитие цифровой экономики в условиях глобализации. Симферополь : Типография «Ариал», 2019. 276 с.

3. Тарасов И. В. Индустрия 4.0: понятие, концепции, тенденции развития // Стратегии бизнеса. 2018. № 6 (50). С. 57–63.

4. Ватлина Л. В. Культура цифровой трансформации предоставления государственных услуг // Известия СПбГЭУ. 2022. № 1 (133). С. 73–78.

5. Борщевский Г. А. Привлечение бизнеса к участию в государственном управлении: опыт и проблемы // Государственно-частное партнерство. 2016. Т. 3, № 2. С. 79–98. DOI: 10.18334/ppp.3.2.36928

6. Белолипецкая К. С. The Digital Millennium Copyright Act (DMCA) как способ пресечение нарушений авторских и смежных прав в сети «Интернет» // Теория и практика современной науки. 2020. № 11 (65). С. 30–33.

7. Атнашев В. Р., Яхъеева С. Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. 2019. № 3 (29). С. 37–42.

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 17.12.2023.
Дата рецензирования статьи /Revised: 23.01.2024.
Дата принятия статьи к публикации /Accepted: 28.02.2024.