УДК 342.723 DOI 10.21777/2587-9472-2025-4-7-13

КИБЕРБЕЗОПАСНОСТЬ КАК МЕЖОТРАСЛЕВОЙ ПРАВОВОЙ ИНСТИТУТ

Егерева Олеся Александровна[1],
канд. юрид. наук,
e-mail: oegereva@muiv.ru

Слюсаренко Татьяна Валерьевна[1],
канд. юрид. наук, доцент,
e-mail: tslyusarenko@muiv.ru
[1]*Московский университет имени С.Ю. Витте, г. Москва, Россия*

Статья посвящена вопросам нормативно-правового регулирования кибербезопасности в современном цифровом мире, где информационные системы, сети и данные стали объектами постоянных кибератак и угроз. Исследование фокусируется на анализе существующей законодательной базы Российской Федерации, регулирующей сферу кибербезопасности как межотраслевого правового института, и на выявлении тех изменений,которые произошли в данной области в последние годы. Одной из целей работы является также и выборочный анализ зарубежного опыта в области кибербезопасности посредством изучения содержимого соответствующих стратегий для проведения сравнительного анализа с российской действительностью. Кроме того, в данной статье обозначены авторские позиции по дефинициям «информационная безопасность», «кибербезопасность»; анализ действующих редакций правовых норм об информационной безопасности. В целом, проведенный анализ кибербезопасности как межотраслевого правового института вносит вклад в понимание современных проблем и перспектив его дальнейшего развития, и может быть полезен как для специалистов в области кибербезопасности, так и исследователей, интересующихся вопросами обеспечения защиты прав и свобод личности в условиях цифрового общества. По тексту статьи Российская Федерация сокращенно указывается – РФ.

Ключевые слова: кибербезопасность, цифровизация, информационное общество, нормативно-правовые акты, правовая система, киберугрозы

CYBERSECURITY AS AN INTERDISCIPLINARY LEGAL INSTITUTION

Yegoreva O.A.[1],
Candidate of Legal Sciences,
e-mail: oegereva@muiv.ru

Slyusarenko T.V.[1],
Candidate of Legal Sciences, Associate Professor,
e-mail: tslyusarenko@muiv.ru
[1]*Moscow Witte University, Moscow, Russia*

The article is devoted to the issues of regulatory and legal regulation of cybersecurity in the modern digital world, where information systems, networks and data have become the objects of constant cyber attacks and threats. The study focuses on analyzing the existing legislative framework of the Russian Federation regulating the area of cybersecurity as an interdisciplinary legal institution, and on identifying the changes that have occurred in this area in recent years. One of the objectives of the work is also a selective analysis of foreign experience in the area of cybersecurity by examining the contents of relevant strategies for comparative analysis with the Russian reality. In addition, this article outlines the author's positions on the definitions of «information security» and «cybersecurity»; an analysis of current versions of legal norms on information security. In general, the analysis of cybersecurity as an interdisciplinary legal institution contributes to an understanding of current problems

and prospects for its further development, and may be useful for both cybersecurity specialists and researchers interested in ensuring the protection of individual rights and freedoms in a digital society.
In the text of the article, the Russian Federation is abbreviated as RF.

Keywords: cybersecurity, digitalization, information society, regulatory legal acts, legal system, cyber threats

В настоящее время цифровая трансформация общества поставила перед правовыми системами вызовы беспрецедентного масштаба. Классические модели защиты прав человека, сформированные в аналоговую эпоху и опирающиеся на физические границы юрисдикций и материальные объекты регулирования, демонстрируют свою фрагментарную эффективность в пространстве, где действие стирает след, а идентичность становится набором данных. В этом контексте разработка новых моделей и механизмов защиты приобретает характер не эволюционной, а революционной правовой задачи. Российское законодательство, находясь в процессе активного «цифрового правотворчества», пытается сформировать комплексный ответ на эти вызовы, создавая гибридные конструкции, сочетающие традиционные гарантии с цифровыми инструментариями.

Рост количества и сложности кибератак, в том числе на государственную инфраструктуру, образовательные учреждения и работодателей трансформировал кибербезопасность из сугубо технической категории в межотраслевой правовой институт, непосредственно влияющий на реализацию прав и свобод. В фокусе оказываются не только экономические интересы организаций, но и достоинство личности, частная жизнь, право на образование и труд, а в случае посягательств на критическую информационную инфраструктуру – и право на жизнь и здоровье. Стратегические документы РФ в сфере национальной и информационной безопасности исходят из того, что устойчивость цифровой среды является условием осуществления гарантированных прав, а не побочной задачей IT-политики государства, что придает кибербезопасности характер объективной правовой необходимости, уходящей за пределы узкопрофессиональной сферы специалистов по защите информации.

Концепция комплексного регулирования кибербезопасности, охватывающая ключевые аспекты защиты информации, инфраструктуры и борьбы с киберпреступностью, не является новой для международного сообщества и успешно реализована во многих странах и на союзных уровнях, например, в Сингапуре (Cybersecurity Act), Германии (Закон о безопасности информационных технологий (IT-Sicherheitsgesetz)), Европейском союзе (Директива ЕС NIS2), США (Cybersecurity Information Sharing Act) и пр.[1]

В 2020 г. на Всемирном экономическом форуме в Давосе кибербезопасность была признана одной из важнейших глобальных проблем современности[2]. Экспертное сообщество считает киберугрозы даже более опасными, чем терроризм и экологические проблемы. Постоянный рост числа кибератак, наносящих ущерб организациям, подчеркивает острую необходимость усиления мер по обеспечению цифровой безопасности [1, с. 646]. Между тем в российском законодательстве отсутствует определение понятия «кибербезопасность». Юридическая наука при его раскрытии опирается на терминологию, заимствованную из различных областей знаний.

Отсутствие в российском законодательстве легального определения кибербезопасности компенсируется обращением к зарубежным и внутригосударственным концептуальным моделям.

Классическим толкованием кибербезопасности считается определение Национального института стандартов и технологий США (National Institute of Standards and Technology) – «способность защищать или оборонять киберпространство от кибератак»[3].

Лаборатория Касперского описывает кибербезопасность как «совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных си-

[1] *Танкова А.* Правовые механизмы кибербезопасности: общие принципы и секторальное регулирование // ЭЖ-Юрист. – 2025. – №14 (1363). – URL: http://www.kremlin.ru/events/president/news/68451 (дата обращения: 10.10.2025).
[2] *Жданов Ю., Овчинский В.* О киберугрозах в Давосе // Совет по внешней и оборонной политике. – URL: https://svop.ru/mains/31921/ (дата обращения: 14.10.2025).
[3] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments. – URL: https://csrc.nist.gov/glossary/term/cyber_security (дата обращения: 20.10.2025).

стем, сетей и данных»[4]. ПАО «Сбербанк» считает, что кибербезопасность – это направление информационной безопасности, целью которого является защита цифровых данных в киберпространстве[5]. Компания Positive Technologies – российский разработчик комплексных решений в области кибербезопасности – определяет ее как защиту сетевых систем (оборудования, программного обеспечения и данных) от киберугроз. Последние представляют собой совокупность факторов и условий, способных привести к нарушению информационной безопасности[6].

Н.Ш. Козлова и В.А. Довгаль рассматривают кибербезопасность как область информационных технологий, ориентированных на защиту систем, включающих в себя электронные записи, устройства для отслеживания информации, оборудование и программное обеспечение, используемое для оказания услуг и управления ими [2, с. 90].

Необходимо отметить, что в 2014 г. Временной комиссией Совета Федерации по развитию информационного общества был разработан проект концепции стратегии кибербезопасности Российской Федерации, в котором был предпринят шаг в направлении установления официального понятия «кибербезопасность». Согласно данному проекту под кибербезопасностью предполагалось понимать «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями»[7]. Однако документ принят не был.

В то же время в некоторых странах СНГ понятие «кибербезопасность» закреплено в нормативных правовых актах, регулирующих общественные отношения в данной сфере. К примеру, в Законе Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 «О кибербезопасности» она определяется как «состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве» (ст. 3)[8]. В Законе Республики Молдова от 16 марта 2023 г. № 48 «О кибербезопасности» установлено, что это «действия, необходимые для защиты информационных сетей и систем, пользователей таких систем и других лиц, подверженных киберугрозам» (ст. 2)[9].

В Концепции кибербезопасности («Киберщит Казахстан»), утвержденной Постановлением Правительства Республики Казахстан от 30 июня 2017 г. № 407, «под кибербезопасностью понимается состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации» [3, с. 112].

Указом Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» кибербезопасность определена как «состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз».

Несмотря на то, что в российском законодательстве отсутствует понятие «кибербезопасность», в правовом пространстве России используется близкий по смыслу термин – «информационная безопасность РФ» (таблица 1).

---

[4] Что такое кибербезопасность? – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security (дата обращения: 14.10.2025).

[5] Кибербезопасность. Кибрарий – библиотека знаний по кибербезопасности. Все самое важное и полезное о том, как защитить себя в цифровом мире. – URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/kiberbezopasnost (дата обращения: 14.10.2025).

[6] Что такое кибербезопасность. – URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-kiberbezopasnost/ (дата обращения: 13.10.2025).

[7] Образование и занятость: правовые вопросы новой цифровой реальности: монография / Н.С. Волкова, О.Ю. Еремина, О.В. Моцная [и др.]; отв. ред. Н.С. Волкова, Н.В. Путило. – Москва: Юриспруденция, 2025.

[8] Национальная база данных законодательства Республики Узбекистан от 16 апреля 2022 г. № 03/22/764/0313.

[9] Официальный монитор Республики Молдова. – 2023. – № 151–153. – Ст. 225.

Таблица 1 – Соотношение понятий «информационная безопасность» и «кибербезопасность»[10]

Критерий	Информационная безопасность РФ	Кибербезопасность
Базовый источник	Доктрина информационной безопасности РФ, Стратегия национальной безопасности	Проекты Концепции кибербезопасности, акты СНГ, доктрины других государств
Объект защиты	Информация независимо от носителя (бумага, электронные данные и т.д.)	Цифровая информация, сети, системы, киберпространство
Субъекты защиты	Личность, общество, государство	Личность, общество, государство в цифровой среде
Основные угрозы	Внутренние и внешние информационные угрозы	Киберпреступность, кибератаки, кибертерроризм
Цель	Обеспечение реализации конституционных прав и суверенитета РФ	Защита цифровой инфраструктуры и данных от киберугроз
Степень формализации в РФ	Легальное определение закреплено	Легального определения на уровне закона нет
Соотношение	Более широкое понятие	Частный случай, относящийся к цифровому сегменту информационной безопасности

В нашей стране цели и задачи по обеспечению информационной безопасности изложены в документах стратегического планирования. К ним относятся Стратегия национальной безопасности РФ, утвержденная Указом Президента РФ от 2 июля 2021 г. № 400[11], и Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646[12]. Кроме того, Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ»[13] направлен на усиление мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Проанализировав данные акты, можно сделать вывод, что правовое содержание информационной безопасности заключается в защите интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве и является приоритетом в обеспечении кибербезопасности государств [4, с. 83].

Подводя краткий итог изложенному, отметим, что, несмотря на тесную взаимосвязь понятий «информационная безопасность» и «кибербезопасность», данные понятия не являются тождественными.

В соответствии с определением Кембриджского словаря:

1) «информационная безопасность» – состояние защищенности электронных данных от преступного или несанкционированного использования;

2) «кибербезопасность» – способы защиты компьютерных систем от таких угроз, как вирусы [5, с. 184].

В российской практике встречается более широкое понятие «информационная безопасность», связанное с обеспечением безопасности в первую очередь личности, общества и государства.

Так, информационная безопасность представляет собой комплексное понятие, включающее в себя состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства[14].

Данное понятие охватывает все аспекты обеспечения конфиденциальности, целостности и доступности данных. В свою очередь, кибербезопасность призвана защищать цифровую информацию от несанкционированного доступа и кибератак. Она направлена на предотвращение неправомерного разглашения, искажения или уничтожения такой информации третьими лицами, а также на противодействие трем основным категориям угроз, к которым относятся:

[10] Составлено авторами.

[11] Собрание законодательства РФ. – 2021. – № 27 (Ч. II). – Ст. 5351.

[12] Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

[13] Собрание законодательства РФ. – 2022. – № 18. – Ст. 3058.

[14] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50. – Ст. 7074.

1) киберпреступление – противоправные действия, осуществляемые одним или несколькими лицами с целью нарушения функционирования компьютерной системы или получения материальной выгоды за счет ее использования;

2) кибератака – действия, направленные на получение конфиденциальной информации;

3) кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику[15].

Правовое регулирование кибербезопасности имеет многоуровневый характер и базируется на ряде ключевых законодательных актов, определяющих общие принципы информационной безопасности и специальных норм, регулирующих защиту критической информационной инфраструктуры, обработку персональных данных, противодействие киберугрозам [6, с. 83].

Основополагающим правовым актом, задающим парадигму защиты прав человека, остается Конституция РФ. Закрепленные в ее статьях 23, 24, 29, 45 права на неприкосновенность частной жизни, тайну переписки, свободу информации и поиск, получение и распространение информации, а также гарантии государственной защиты прав и свобод получают новое цифровое прочтение. Конституционный Суд РФ в ряде постановлений[16] указал, что конституционные гарантии распространяются на коммуникации, осуществляемые с использованием информационно-телекоммуникационных сетей. Однако абстрактность конституционных норм требует их конкретизации в специальном законодательстве.

Системообразующую роль играет Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[17]. Он вводит базовые понятия: «информация», «информационно-телекоммуникационная сеть», «обладатель информации», «оператор информационной системы». Ключевой моделью, заложенной данным законом, является модель регулирования через определение статуса оператора. Именно на оператора, определяемого как лицо, осуществляющее деятельность по эксплуатации информационной системы, возлагается основной объем обязанностей по обеспечению безопасности и законности обработки данных, что создает точку приложения для контрольно-надзорных мер.

Специальный уровень правового регулирования – это Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[18].

Этот закон представляет собой наиболее продвинутую и детализированную модель регулятивного подхода. Он вводит понятие «критическая информационная инфраструктура» (далее КИИ) – объекты информационных систем и сети электросвязи, используемые для управления процессами в оборонной, энергетической, транспортной, банковской и иных ключевых сферах, нарушение или прекращение функционирования которых ведет к тяжелым последствиям. В контексте прав человека защита КИИ напрямую коррелирует с защитой права на жизнь, здоровье, благоприятную окружающую среду, социальное обеспечение.

Закон устанавливает императивно-разрешительную модель регулирования, включающую:

- государственную регистрацию объектов КИИ и ведение их реестра (ст. 8, 9);

- обязательность лицензирования деятельности по разработке и внедрению средств защиты информации для КИИ (ст. 14);

- установление системы категорирования объектов КИИ и дифференцированных требований по их защите (ст. 7);

- создание Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) (ст. 13). Операторы КИИ обязаны подключаться к ней, что формирует модель централизованного государственного мониторинга угроз для наиболее значимых объектов.

Данный подход демонстрирует главенство публичных интересов (национальная безопасность, общественный порядок) и прямое вмешательство государства в деятельность частных компаний, управляющих КИИ.

---

[15] Что такое кибербезопасность? – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security (дата обращения: 15.10.2025)

[16] Постановление Конституционного Суда РФ от 26.10.2017 № 25-П // Собр. законодательства Рос. Федерации. – 2017. – № 45. – Ст. 6735.

[17] Собрание законодательства РФ. – 2006. – № 31 (Ч. I). – Ст. 3448.

[18] Собрание законодательства РФ. – 2017. – № 31 (Ч. I). – Ст. 4736.

Следующим уровнем конкретизации выступает Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[19].

С точки зрения защиты прав конкретного индивида данный закон является центральным. Он конкретизирует общие требования кибербезопасности применительно к специальному объекту – персональным данным. Ст. 19 закона возлагает на оператора обязанность принимать необходимые организационные и технические меры для защиты данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения. Механизм защиты здесь носит превентивно-распределенный характер: государство (в лице Роскомнадзора) устанавливает требования (утвержденные Постановлением Правительства РФ № 1119 от 01.11.2012)[20], а оператор самостоятельно выбирает и внедряет меры, адекватные угрозам, что подтверждается в ходе проверок регулятора. Важным инструментом является модель оценки соответствия, реализуемая через обязательную оценку уязвимостей и аттестацию информационных систем персональных данных (ст. 22 ФЗ-152, Постановление Правительства РФ № 21 от 18.01.2023).

Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»[21] и Федеральный закон от 27.07.2006 № 149-ФЗ устанавливают модель защиты через обязанности организаторов распространения информации и блогеров, которые, при определенных количественных критериях аудитории, приравниваются к СМИ и несут дополнительные обязанности по хранению и предоставлению данных правоохранительным органам, а также по соблюдению законодательства о распространении информации.

Ключевые нормы, определяющие понятия и меры ответственности за киберпреступления, сосредоточены в главе 28 УК РФ, которая входит в раздел IX «Преступления против общественной безопасности и общественного правопорядка» и Кодексе Российской Федерации об административных правонарушениях. Данные нормы подчеркивают признание защиты цифровой инфраструктуры в качестве элемента национальной безопасности и общественных интересов.

Административная ответственность (гл. 13 КоАП РФ) выполняет функцию оперативного реагирования на менее опасные нарушения. Ключевые статьи: 13.11 (нарушение законодательства в области персональных данных, с детализированными составами), 13.12 (нарушение правил защиты информации), 13.14 (разглашение информации с ограниченным доступом). Данные нормы представляют собой модель административного принуждения, направленную на обеспечение соблюдения регулятивных требований под угрозой крупных штрафов.

Анализ действующего российского законодательства позволяет констатировать, что в стране сформирована комплексная, но внутренне противоречивая система защиты прав человека в цифровом пространстве. Ее доминирующей чертой является сильная публично-правовая, превентивно-ограничительная составляющая, ориентированная на обеспечение государственного суверенитета, информационной безопасности и общественного порядка, иногда в ущерб развитию приватности и индивидуальных цифровых автономий. Модели, связанные с защитой от государства (например, в сфере тотального сбора данных в рамках СМР), развиты слабее, чем модели контроля государства над информационным полем.

В ближайшем будущем потребность в модернизации информационной инфраструктуры и укреплении кибербезопасности будет только возрастать, что обусловлено быстрым развитием новых прорывных технологий [7, с. 745]. В частности, большие возможности в сфере кибербезопасности видятся в контексте использования искусственного интеллекта [8, с. 69] и больших данных [6, с. 88]. Однако это требует обеспечения должного правового регулирования, что, в свою очередь, представляется перспективным направлением дальнейших научных исследований.

Список литературы

1. *Сафонова М.Ф., Кривошей Д.Н.* Аудит информационной и кибербезопасности: нормативное регулирование и проблемы функционирования // Международный бухгалтерский учет. – 2024. – № 6. – С. 644–664.

[19] Собрание законодательства РФ. – 2006. – № 31 (Ч. I). – Ст. 3451.

[20] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01 ноября 2012 № 1119 // Собр. законодательства Рос. Федерации. – 2012. – № 45. – Ст. 6257.

[21] О связи: федер. закон РФ от 07 июля 2003 № 126-ФЗ // Собр. законодательства Рос. Федерации. – 2003. – № 28. – Ст. 2895.

2. *Козлова Н.Ш., Довгаль В.А.* Кибербезопасность и информационная безопасность: сходства и отличия // Вестник Адыгейского государственного университета. Сер. 4: Естественно-математические и технические науки. – 2021. – № 3(286). – С. 88–97.
3. *Ержанова З.А.* Обеспечение кибербезопасности Казахстана и правовые аспекты современной кибербезопасности // Труды XVI Евразийского научного форума: сб. статей, Санкт-Петербург, 12–13 декабря 2024 года. – Санкт-Петербург: Университет при МПА ЕврАзЭС, 2025. – С. 111–119.
4. *Никитина Е.Е.* Информационная безопасность как элемент конституционного статуса личности // Журнал российского права. – 2024. – № 1. – С. 81–94.
5. *Кулжабаева Ж.О.* Законодательное разграничение понятий «кибербезопасность» и «информационная безопасность» // Вестник Института законодательства и правовой информации Республики Казахстан. – 2024. – № 4(79). – С. 178–186.
6. *Прокопьев И.В.* Анализ нормативно-правового обеспечения кибербезопасности в Российской Федерации // Интеграционные процессы в современной науке: новые подходы и актуальные вопросы: Сборник научных трудов по материалам XXXIII Международной научно-практической конференции, Анапа, 27 мая 2025 года. – Анапа: ООО «Научно-исследовательский центр экономических и социальных процессов» в Южном Федеральном округе, 2025. – С. 81–88.
7. *Bertovsky L.V.* High-tech law: concept, genesis and prospects / RUDN Journal of Law. – 2021. – № 25 (4). – Pp. 735–749.
8. *Ересько П.В.* Правовое обеспечение безопасности информационного пространства Российской Федерации в сфере искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2024. – № 10. – С. 69–76.

References

1. *Safonova M.F., Krivoshej D.N.* Audit informatsionnoj i kiberbezopasnosti: normativnoe regulirovanie i problemy funktsionirovaniya // Mezhdunarodnyj bukhgalterskij uchet. – 2024. – № 6. – S. 644–664.
2. *Kozlova N.Sh., Dovgal′ V.A.* Kiberbezopasnost′ i informatsionnaya bezopasnost′: skhodstva i otlichiya // Vestnik Adygejskogo gosudarstvennogo universiteta. Ser. 4: Estestvenno-matematicheskie i tekhnicheskie nauki. – 2021. – № 3(286). – S. 88–97.
3. *Erzhanova Z.A.* Obespechenie kiberbezopasnosti Kazakhstana i pravovye aspekty sovremennoj kiberbezopasnosti // Trudy KhVI Evrazijskogo nauchnogo foruma: sb. statej, Sankt-Peterburg, 12–13 dekabrya 2024 goda. – Sankt-Peterburg: Universitet pri MPA EvrAzES, 2025. – S. 111–119.
4. *Nikitina E.E.* Informatsionnaya bezopasnost′ kak element konstitutsionnogo statusa lichnosti // Zhurnal rossijskogo prava. – 2024. – № 1. – S. 81–94.
5. *Kulzhabaeva Zh.O.* Zakonodatel′noe razgranichenie ponyatij «kiberbezopasnost′» i «informatsionnaya bezopasnost′» // Vestnik Instituta zakonodatel′stva i pravovoj informatsii Respubliki Kazakhstan. – 2024. – № 4(79). – S. 178–186.
6. *Prokop'ev I.V.* Analiz normativno-pravovogo obespecheniya kiberbezopasnosti v Rossijskoj Federatsii // Integratsionnye protsessy v sovremennoj nauke: novye podkhody i aktual′nye voprosy: Sbornik nauchnykh trudov po materialam XKhKhIII Mezhdunarodnoj nauchno-prakticheskoj konferentsii, Anapa, 27 maya 2025 goda. – Anapa: OOO «Nauchno-issledovatel′skij tsentr ekonomicheskikh i sotsial′nykh protsessov» v Yuzhnom Federal′nom okruge, 2025. – S. 81–88.
7. *Bertovsky L.V.* High-tech law: concept, genesis and prospects / RUDN Journal of Law. – 2021. – № 25 (4). – Pp. 735–749.
8. *Eres'ko P.V.* Pravovoe obespechenie bezopasnosti informatsionnogo prostranstva Rossijskoj Federatsii v sfere iskusstvennogo intellekta // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). – 2024. – № 10. – S. 69–76.

Статья поступила в редакцию: 21.09.2025
Статья принята к публикации: 30.11.2025
Received: 21.09.2025
Accepted: 30.11.2025