Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2025. Т. 25, вып. 4. С. 424–436
Izvestiya of Saratov University. Economics. Management. Law, 2025, vol. 25, iss. 4, pp. 424–436
https://eup.sgu.ru https://doi.org/10.18500/1994-2540-2025-25-4-424-436, EDN: QPNPRC

Научная статья
УДК 342+004.056

Правовые проблемы обеспечения информационной безопасности личности в цифровом пространстве

П. В. Ересько

Саратовская государственная юридическая академия, Россия, 410056, г. Саратов, Россия, ул. Вольская, д. 1

Ересько Полина Владимировна, кандидат педагогических наук, доцент кафедры информационного права и цифровых технологий, pv.eresko@yandex.ru, AuthorID: 318985

Аннотация. ***Введение*****.** В условиях развития технологий искусственного интеллекта, больших данных (BigData), нейросетей и повсеместной цифровизации индивид расширяет свои возможности в цифровом пространстве, но при этом возникают угрозы его приватности, автономии и информационной безопасности. Личность в цифровом пространстве становится объектом эксплуатации и манипуляции, что требует адекватного правового ответа, вследствие чего законодательная база в области обеспечения информационной безопасности личности нуждается в совершенствовании и выработке новых подходов. ***Теоретический анализ.*** В российском и международном праве существуют проблемы обеспечения информационной безопасности личности в цифровом пространстве, такие как неэффективная защита персональных данных в сети «Интернет», неадаптированность традиционных правовых институтов к цифровой среде, недооценка приоритета защиты прав личности перед интересами технологического развития и др. Для эффективной защиты прав и свобод человека в современном цифровом пространстве требуется формирование комплексной системы, содержащей правовые и технические средства защиты. В настоящее время в российском праве отсутствует определение «информационная безопасность личности», что создает правовую неопределенность. Решением выявленных проблем может быть разработка и принятие Доктрины информационной безопасности личности. ***Эмпирический анализ*****.** К правовым проблемам обеспечения информационной безопасности личности в цифровом пространстве отнесены проблемы киберпреступности, нарушения неприкосновенности частной жизни, распространения недостоверной информации (фейков) и др. Проанализированная статистика Яндекс до 2024 г. по обращениям о праве на забвение показывает достаточно большое количество отказов – 80%, что обусловливается ограниченным применением нормы права только на операторов поисковых систем, чья деятельность была сопряжена с распространением рекламы, нацеленной на российских потребителей. Усовершенствованная норма права в 2024 г. устранила неравенство между операторами поисковых систем, показала большую эффективность применения права на забвение, усовершенствовала защиту прав пользователя сети «Интернет». ***Результаты*****.** Доказана необходимость совершенствования действующего законодательства в части обеспечения информационной безопасности личности в цифровом пространстве; сформулирован комплекс законодательных предложений, содержащий разработку и принятие Доктрины информационной безопасности личности, законодательное закрепление определения информационной безопасности личности, комплексную систему защиты личности в цифровом пространстве, включающую правовые и технические средства.

Ключевые слова: информационная безопасность личности, цифровое пространство, искусственный интеллект, персональные данные, право на забвение, блокировка вредоносной информации, киберпреступность, фейки

Для цитирования: *Ересько П. В.* Правовые проблемы обеспечения информационной безопасности личности в цифровом пространстве // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2025. Т. 25, вып. 4. С. 424–436. https://doi.org/10.18500/1994-2540-2025-25-4-424-436, EDN: QPNPRC

Article

Legal problems of ensuring personal information security in the digital space

P. V. Eresko

Saratov State Law Academy, 1 Volskaya St., Saratov 410056, Russia

Polina V. Eresko, pv.eresko@yandex.ru, AuthorID: 318985

Abstract. ***Introduction*****.** In the context of the development of artificial intelligence technologies, Big Data, neural networks and widespread digitalization, an individual is expanding his / her capabilities in the digital space, but, at the same time, there are threats to his / her privacy, autonomy and information security. A person in the digital space becomes an object of exploitation and manipulation, which requires an adequate legal response. As a result, the legislative framework in the field of ensuring personal information security needs to be improved and new approaches must be developed. ***Theoretical analysis*****.** In Russian and international law, there are problems with ensuring the information security of individuals in the digital space, such as ineffective protection of personal data on the Internet, the lack of adaptation of traditional legal institutions to the digital environment, the underestimation of the priority of protecting individual rights over the interests of technological

development, etc. To effectively protect human rights and freedoms in the modern digital space, it is necessary to create a comprehensive system that includes legal and technical means of protection. Currently, there is no definition of "information security of individuals" in the Russian law, which creates legal uncertainty. The development and adoption of the Doctrine of Information Security of Individuals may be the solution to these problems. ***Empirical analysis.*** The legal problems of ensuring personal information security in the digital space include the problems of cybercrime, violations of privacy, the spread of false information (fake news), etc. The analyzed statistics from Yandex up to 2024 on applications for the right to oblivion show a fairly high number of refusals – 80%, which is due to the limited application of the law only to search engine operators whose activities involved the distribution of advertising aimed at Russian consumers. The improved legal norm in 2024 eliminated the inequality between search engine operators, demonstrated the greater effectiveness of the right to be forgotten, and improved the protection of Internet users' rights. ***Results.*** The necessity of improving the current legislation in terms of ensuring personal information security in the digital space has been proved; a set of legislative proposals has been formulated, including the development and adoption of the Doctrine of Personal Information Security, legislative consolidation of the definition of personal information security, a comprehensive system of personal protection in the digital space, including legal and technical means.

Keywords: personal information security, digital space, artificial intelligence, personal data, the right to be forgotten, blocking malicious information, cybercrime, fakes, deepfakes

For citation: Eresko P. V. Legal problems of ensuring personal information security in the digital space. *Izvestiya of Saratov University. Economics. Management. Law*, 2025, vol. 25, iss. 4, pp. 424–436 (in Russian). https://doi.org/10.18500/1994-2540-2025-25-4-424-436, EDN: QPNPRC

Введение

Современный этап технологического прогресса, характеризующийся развитием информационных технологий, таких как искусственный интеллект, нейросети, а также использованием больших данных (BigData) и цифровизацией общественных отношений, формирует принципиально новую цифровую среду, в которой происходит реализация прав и свобод человека. Цифровое пространство стало неотъемлемой частью современного общества, трансформируя традиционные формы коммуникации, экономики и государственного управления.

С одной стороны, индивид получает беспрецедентные инструменты для доступа к информации, коммуникации и самореализации. С другой стороны, как справедливо отмечается в научной литературе, эта же среда порождает системные угрозы приватности, личной автономии и информационной безопасности личности [1, с. 156].

Постоянное расширение цифрового пространства порождает новые, ранее не существовавшие угрозы безопасности личности. В цифровую эпоху каждое действие, каждая оставленная пользователем в сети «Интернет» информация раскрывает его интересы, убеждения и привычки. Гражданин, осуществляя действия в сети «Интернет», оставляет при этом на сайтах данные о себе (в том числе персональные), свои мнения, суждения, потребительские предпочтения. Именно поэтому личность в условиях развития информационных технологий, в том числе технологий искусственного интеллекта, стала крайне уязвимой к похищению, копированию, искажению и злонамеренному использованию ее данных.

Вопросами правового обеспечения информационной безопасности занимались многие известные ученые, такие как П. У. Кузнецов, В. Н. Лопатин, О. С. Макаров, А. В. Минбалеев, Т. А. Полякова; проблемами информационной безопасности личности – Т. А. Полякова, А. А. Стрельцов, В. Н. Лопатин, Н. Ю. Белокопытова, А. Д. Анучкина, Т. А. Вепренцева, А. А. Чеботарёва; проблемами правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде – Т. А. Полякова, А. В. Минбалеев, И. С. Бойченко, А. А. Лукошкин; правовыми проблемами защиты прав и свобод личности в информационной сфере – Р. В. Амелин, И. Л. Бачило, И. М. Рассолов, Н. Н. Ковалёва, С. А. Куликова, С. Е. Чаннов и др.

Скорость развития современных информационных технологий объективно опережает скорость адаптации правового регулирования информационной безопасности личности в цифровом пространстве. Это создает ситуацию, когда гражданин зачастую остается один на один с мощными цифровыми платформами и технологиями, не обладая эффективными правовыми механизмами защиты. Защиту информационной безопасности граждан в сети «Интернет» обеспечивает государство. Стремительное развитие информационных технологий и появление новых видов рисков в сети «Интернет» создает потребность в совершенствовании правовых и технических инструментов, а также в формировании принципиально новых подходов к обеспечению информационной безопасности личности.

Теоретический анализ

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 05.12.2016 № 646, опреде-

ляются ключевые приоритеты Российской Федерации в информационном пространстве, идентифицируются главные угрозы и задаются стратегические ориентиры в области защиты информационной безопасности. Под информационной безопасностью понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[1]. Национальными интересами в информационной сфере являются государственные интересы, такие как суверенитет, обороноспособность и территориальная целостность, социально-экономическое развитие, содействие формированию системы международной информационной безопасности, а также гарантии конституционных прав и свобод человека. Тем самым безопасность информационного пространства рассматривается как необходимое условие для достижения достойного качества жизни граждан и устойчивого прогресса страны в целом, что подчеркивает ее многогранный и социально ориентированный характер.

Значимую роль в обеспечении информационной безопасности личности играет Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных)[2]. Его нормы направлены на защиту прав и свобод человека и гражданина при обработке его персональных данных, в том числе на защиту прав на неприкосновенность частной жизни, личную и семейную тайну. Закон вводит ключевые понятия, такие как персональные данные, оператор, обработка, трансграничная передача, устанавливает принципы и условия обработки данных, права субъекта персональных данных и обязанности оператора. Согласно ст. 19 данного Закона, при обработке персональных данных необходимо применять комплекс правовых, организационных и технических мер для их защиты.

Т. А. Полякова, А. В. Минбалеев, И. С. Бойченко подчеркивают комплексный характер проблем правового обеспечения информационной безопасности в процессе использования цифровых технологий и необходимость разработки сбалансированных правовых механизмов, учитывающих как национальные интересы, так и требования глобальной цифровой среды [2, с. 33]. Авторы аргументированно доказывают, что фрагментарность правового регулирования и коллизии юрисдикций создают серьезные препятствия для эффективной защиты прав личности, в частности, в сфере персональных данных. Ими также обоснована необходимость развития международной интеграции и выработки согласованных подходов к обеспечению информационной безопасности, в частности, в рамках Евразийского экономического союза. Таким образом, данное исследование вносит значительный вклад в понимание системных проблем правового регулирования и указывает на необходимость международного сотрудничества для их преодоления. Выделенная авторами проблема стремительного отставания правовых механизмов в условиях глобальной цифровой трансформации и развития таких технологий, как искусственный интеллект, виртуальная и дополненная реальность и другие, напрямую перекликается с выводами Н. Ю. Белокопытовой и А. Д. Анучкиной о несовершенстве традиционных правовых конструкций в Российской Федерации [3, с. 311], а также с исследованиями Д. И. Зуева о вызовах, которые бросает праву на неприкосновенность частной жизни использование цифровых технологий [4, с. 27].

Как справедливо отмечают Н. Ю. Белокопытова и А. Д. Анучкина, недостатки действующего правового регулирования информационной безопасности заключаются в дефиците правовой определенности, неспособности обеспечить реальную защиту приватности, подмене гарантирующей функции государства сервисной, а также в отсутствии целостного подхода, что в совокупности превращает многие правовые гарантии в декларативные нормы.

Использованию цифровых технологий для манипуляции сознанием в качестве информационного оружия уделяется внимание в работах Н. Н. Ковалёвой [5, с. 131], С. А. Куликовой [6, с. 330] и др. Манипуляция сознанием с использованием цифровых инструментов представляет собой не просто этическую проблему, а форму противоправного информационно-психологического воздействия, нарушающего принцип достоверности ин-

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 // Собр. законодательства Рос. Федерации. 2016. № 50, ст. 7074

[2] О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. 1), ст. 3451.

формации и права граждан на ее получение (ст. 29 Конституции РФ[3]) и информационную безопасность личности.

Стремительная цифровая трансформация всех сфер общественной жизни актуализировала необходимость теоретического осмысления правовых проблем обеспечения информационной безопасности личности. Как справедливо отмечают Р. В. Амелин, Т. А. Полякова, С. Е. Чаннов, в условиях цифровой реальности формируется принципиально новая среда для реализации прав и свобод человека, которая одновременно порождает большой спектр вызовов и угроз информационной безопасности в современных условиях, что требует междисциплинарных и межотраслевых подходов [7, с. 133; 8, с. 144–156].

Довольно часто в современном понимании термин «информационная безопасность», «информационная безопасность личности» рассматривают в совокупности с терминами «цифровая среда», «цифровое пространство». Понятие «цифровое пространство» закреплено в Модельном законе о цифровой трансформации отраслей промышленности государств-участников СНГ, принятом в 2023 г. и носящем рекомендательный характер. Под цифровым пространством понимается область, где «осуществляются функционирование и взаимодействие цифровых сетей и цифровых процессов и в которой вместе с данными процессами на основе определенных регулятивных норм и соответствующих пользовательских, организационных и иных управленческих механизмов также объединяются и интегрируются цифровая среда, электронная сеть, информационные ресурсы (включая цифровые документы), информационные, информационно-телекоммуникационные и цифровые технологии»[4].

Широкая трактовка цифрового пространства как зоны интеграции технологий, данных и управленческих механизмов указывает на то, что оно стало новой, важной цифровой средой деятельности человека. Поскольку цифровое пространство – не просто техническая инфраструктура, а сфера интеграции ключевых социальных, экономических и политических процессов, угрозы в нем перестают быть частной проблемой пользователя сети «Интернет». Любые угрозы в цифровом пространстве, от утечек данных до кибермошенничества, наносят прямой ущерб фундаментальным правам и свободам гражданина. Они трансформируются в системные риски для общества и государства (киберпреступность, дезинформация, посягательства на суверенитет). Поэтому защита личности в цифровом пространстве становится вопросом первостепенной важности. В соответствии с этим безопасность личности в цифровом пространстве становится одним из важных компонентов государственной политики в области национальной безопасности.

Современную концепцию существования личности в цифровом пространстве в виде «цифровой личности» как субъекта, наделенного специфическим набором прав, реализуемых исключительно в цифровой среде, выделяют многие ученые, такие как В. О. Демкин, Л. Г. Ефимова и др. У личности в цифровом пространстве появились новые права, реализуемые с помощью цифровых технологий, которые, как обосновывает В. О. Демкин, составляют специальный правовой статус «цифровой личности». Под термином «цифровая личность» он обозначает «индивида, который обладает правами (наличие и возможность реализации которых при этом гарантированы государством), связанными с цифровыми технологиями и цифровым миром» [9, с. 520]. Этот формирующийся комплекс, по классификации Демкина, включает, в частности, право на цифровое забвение, право на переносимость данных, право на «цифровую смерть» и право на «технологическое равенство». Исследователь указывает, что по своей юридической природе они представляют собой либо новое выражение классических прав человека в онлайн-среде (как, например, право быть забытым, производное от права на неприкосновенность частной жизни), либо абсолютно новые правомочия, обусловленные спецификой цифрового взаимодействия. К механизмам защиты «цифровой личности» от неконтролируемого распространения и использования в этом

[3] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ, от 04.10.2022 № 5-ФКЗ, от 04.10.2022 № 6-ФКЗ, от 04.10.2022 № 7-ФКЗ, от 04.10.2022 № 8-ФКЗ) // Собр. законодательства Рос. Федерации. 2014. № 31, ст. 4398 ; 2020. № 11, ст. 1416 ; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 26.09.2025).

[4] Модельный закон О цифровой трансформации отраслей промышленности государств-участников СНГ (принят 14.04.2023 в г. Санкт-Петербурге Постановлением № 55-9 на 55-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2023. № 78 (ч. 2).

контексте можно отнести право на цифровое забвение и право на переносимость данных.

Л. Г. Ефимова в определении цифровой личности делает акцент на способе присутствия субъекта права в киберпространстве и способе «дистанционного взаимодействия с другими субъектами права в мире Интернета» [10, с. 41], что порождает новые риски для информационной безопасности. Это требует развития специальных гарантий и механизмов защиты, адекватных вызовам цифровой эпохи, где угрозы информационной безопасности становятся системными.

Авторская точка зрения на определение роли современной личности в условиях цифрового пространства совпадает с мнением А. А. Чеботарёвой, которая отмечает, что личность выступает и в качестве объекта правового обеспечения информационной безопасности, и в качестве субъекта, участвующего в обеспечении информационной безопасности как составляющей национальной безопасности [11, с. 41]. Личность в современном обществе должна обладать способностью обеспечивать безопасную реализацию своих интересов в информационном обществе, осознавать преимущества от использования информационно-телекоммуникационных технологий, определять угрозы собственной информационной безопасности и оценивать риски.

А. А. Чеботарёвой сформулировано понятие «информационная безопасность личности» как состояние «её защищенности, которое определяется минимизацией для личности в глобальном информационном обществе рисков в виде внутренних и внешних вызовов и угроз в информационной сфере, способностью противостоять им на основе культуры информационной безопасности, а также формированием государственной политики, направленной на создание условий для реализации информационных прав и свобод при условии обеспечения информационной безопасности» [12, с. 14]. Авторская точка зрения коррелирует с мнением А. А. Чеботарёвой о том, что информационная безопасность личности предстает не как пассивная защита, а как комплексное, динамическое состояние. Это состояние определяется активной позицией самого индивида и целенаправленной деятельностью государства, которое выступает гарантом баланса между свободами и безопасностью в цифровом пространстве.

В Доктрине информационной безопасности РФ под информационной безопасностью понимается взаимосвязь трех субъектов – личности, общества и государства, при этом понятие «информационная безопасность» рассматривается в большей степени как информационная безопасность государства. Отсутствие законодательного определения информационной безопасности личности является, на наш взгляд, существенным правовым пробелом, в связи с чем считаем, что необходимо внести изменения в п. 2 раздела Общие положения Доктрины информационной безопасности РФ, включив определение информационной безопасности личности.

Защита информационной безопасности личности обеспечивается комплексом правовых и технических средств, находящихся в тесной взаимосвязи. Правовые средства устанавливают нормативные требования и гарантии, создавая рамки допустимого поведения субъектов информационных отношений. Технические средства, включая криптографические методы защиты и системы контроля доступа, выступают практическим механизмом реализации этих правовых норм, обеспечивая физическую сохранность и конфиденциальность данных. Таким образом, именно системное сочетание императивных правовых предписаний и адекватных технологических решений формирует эффективный режим защиты прав личности в цифровом пространстве.

Многие законодательные конструкции в области информационной безопасности носят рамочный и декларативный характер. И. Л. Бачило в своих работах об основах информационного права заложила методологический подход, согласно которому эффективность правового регулирования напрямую зависит от его способности адекватно реагировать на технологические вызовы. В частности, она указывала, что неопределенность таких понятий, как «общедоступные данные», затрудняет их практическую реализацию и правовую квалификацию [13, с. 183]. Через открытые персональные данные реализуется социальная идентификация граждан, именно такие данные свободно представляют личность, защищаемую законом.

Зарубежные авторы также отмечают важную роль обеспечения информационной безопасности личности в цифровом пространстве. Джули Коэн в своей книге «Между правдой и властью: правовые конструкции информационного капитализма» [14] анализирует ключевые правовые проблемы безопасности личности в цифровом пространстве и приходит к выводу о том, что правовые конструкции информационного капитализма систематически подрывают автономию и приватность индивида. Основное

внимание исследователем уделяется формированию «биополитического публичного домена», в рамках которого персональные данные превращаются в сырьевой ресурс, свободный для присвоения и коммерческой эксплуатации. Коэн демонстрирует, как режимы правовой защиты, основанные на уведомлении и согласии, становятся фиктивными на фоне повсеместного сбора и анализа данных. Особый акцент сделан на проблеме правовых иммунитетов цифровых платформ, которые уклоняются от ответственности за вредоносный контент, используемых ими манипулятивных алгоритмов и уязвимости в системах безопасности.

Законодательства различных стран пытаются выстроить защиту от вызовов, выявленных российскими и международными исследователями. Так, в Российской Федерации базовые начала регулирования закреплены в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации)[5], который устанавливает основные принципы правового регулирования отношений, возникающих при осуществлении права на поиск, получение, передачу, производство и распространение информации. Статья 3 данного Закона определяет объекты и субъекты защиты, закрепляет принципы свободы поиска, получения и распространения информации, а также принцип неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия. Таким образом, закрепленные в ней принципы являются правовыми инструментами, которые легитимизируют право человека на доступ к информации, защищают его от распространения недостоверных и порочащих сведений, создают основу для законодательства о персональных данных, обеспечивающего неприкосновенность частной жизни.

Однако в современных условиях действие этих традиционных правовых гарантий сталкивается с принципиально новыми вызовами. Цифровое пространство порождает такие способы обработки информации, которые законодатель изначально не мог в полной мере предвидеть. В частности, развитие информационных технологий, например, таких как искусственный интеллект, позволяет искать при помощи алгоритмов персональные данные, логины и пароли от аккаунтов и другие данные, оставленные пользователями при использовании сети «Интернет». Поведенческие паттерны, персональные предпочтения и цифровые следы становятся сырьем для алгоритмического анализа, что создает почву для скрытой эксплуатации и манипуляции. Поэтому личность в цифровом пространстве крайне уязвима: ее можно похитить с помощью информационных технологий, скопировать, исказить и использовать против ее самой.

В рамках обеспечения информационной безопасности личности российское законодательство предусматривает ряд специальных инструментов, направленных на минимизацию цифровых рисков, например: защита персональных данных; прекращение выдачи оператором поисковой системы ссылки сайта в сети «Интернет», распространяющего недостоверную информацию с нарушением законодательства Российской Федерации; обязанность операторов обеспечивать конфиденциальность и безопасность обрабатываемых сведений о гражданах; установление ответственности за распространение противоправного контента в сети «Интернет» (клеветы, недостоверной информации).

Проведенный теоретический анализ позволил выделить следующие правовые проблемы обеспечения информационной безопасности личности в цифровом пространстве: неэффективная защита персональных данных в сети «Интернет»; неадаптированность традиционных правовых институтов к цифровой среде; декларативность гарантий прав и свобод при отсутствии действенных механизмов их защиты; недооценка приоритета защиты прав личности перед интересами технологического развития.

Для достижения баланса интересов личности, общества и государства в цифровом пространстве требуется формирование комплексной системы обеспечения информационной безопасности личности, содержащей правовые и технические средства защиты. Нормативно-правовые инструменты, в частности режим защиты персональных данных, механизм реализации права на забвение и процедуры ограничения доступа к противоправному контенту, формируют систему правовых режимов, направленных на минимизацию цифровых рисков для личности.

Проблемой является отсутствие в российском законодательстве легального определения «информационная безопасность личности», что создает правовую неопределенность. Традици-

[5] Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 № 149-ФЗ // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. 1), ст. 3448.

онные правовые конструкции информационной безопасности личности, общества и государства в своей связке не успевают за динамикой развития цифровой среды, в результате чего способы решения проблем, связанных с обеспечением безопасности личности, остаются за рамками закона. Можно предложить решение этой проблемы в принятии Доктрины информационной безопасности личности по аналогии с Доктриной информационной безопасности Российской Федерации, в которой будут определены основные угрозы личности, существующие в цифровом пространстве, и установлены организационные основы обеспечения информационной безопасности личности.

Перспективными направлениями для дальнейших теоретических изысканий и законодательной работы являются развитие принципов информационного права, международная гармонизация законодательства и создание эффективных механизмов защиты прав человека в глобальном цифровом пространстве.

Эмпирический анализ

Информационная безопасность личности в цифровом пространстве охватывает не только сферу цифрового взаимодействия, но и традиционные каналы информационного обмена, такие как средства массовой информации, государственные базы данных, образовательные и иные информационные системы. Опасность нарушения прав личности может возникнуть в результате распространения недостоверной или порочащей информации о гражданине, утечки сведений, неправомерного ограничения доступа к информации, навязывания идеологически окрашенных сообщений, информационно-психологического воздействия, проводимого с целью совершения мошеннических действий. Следовательно, правовое обеспечение информационной безопасности личности должно иметь комплексный характер, включая конституционно-правовые, административные, уголовно-правовые и международно-правовые механизмы защиты.

Несмотря на то, что действующее российское законодательство заложило существенный базис для защиты прав граждан в информационной сфере, на практике он оказывается недостаточно эффективным против новых цифровых угроз, таких как технологии искусственного интеллекта. Искусственный интеллект Указом Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[6] выделен в качестве одного из основных направлений развития российских информационных и коммуникационных технологий.

К основным правовым проблемам, возникшим с развитием технологий искусственного интеллекта, следует отнести: несанкционированный сбор и обработку персональных данных вследствие автоматического сбора больших данных; утечку информации из взломанных аккаунтов; использование произведений различного характера без соблюдения авторских прав.

Заложенный в российском законодательстве правовой базис оказывается недостаточно адаптирован для регулирования применения технологий искусственного интеллекта, которые придают новое качество и масштаб существующим угрозам [15, с. 24].

В рамках настоящей статьи рассмотрим проблемы обеспечения информационной безопасности личности в цифровом пространстве с помощью такого правового инструмента, как реализация права на забвение, выражающегося в процедуре удаления ссылок на неактуальные и порочащие сведения, а также блокировки информации, признанной недостоверной в установленном законом порядке

Правовой институт права на забвение формируется в области пересечения конституционного и информационного права. Его сущность определяется коллизией между гарантиями частной жизни и информационной безопасности индивида, с одной стороны, и принципом свободы распространения информации – с другой.

По мнению В. Н. Середы и М. Ю. Середы, востребованность права быть забытым проистекает из потребности ограничить распространение в прошлом опубликованных сведений о гражданине, если их дальнейшее наличие в цифровом пространстве способно нанести вред его охраняемым законом правам и интересам [16, с. 70].

С конституционно-правовой точки зрения право на забвение является логическим развитием и конкретизацией базовых гарантий, закрепленных в ст. 23 и 24 Конституции РФ[7]. Именно принципы неприкосновенности частной жизни, защиты чести, достоинства и доброго имени создают основу для требования лица удалить устаревшие или порочащие сведения. Конституционные нормы формируют защитный механизм, провозглашая невмешательство в личную сферу.

[6] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 09.05.2017 № 203 // Собр. законодательства Рос. Федерации. 2017. № 20, ст. 2901.

[7] См.: Конституция Российской Федерации...

Информационное право, в свою очередь, наполняет этот механизм динамическим содержанием, регламентируя процедурные аспекты. Оно устанавливает правовые режимы информации, определяет права и обязанности операторов, регулирует процессы обработки и распространения персональных данных (в частности, Закон об информации и Закон о персональных данных).

В Российской Федерации право на забвение (право быть забытым) в 2015 г. закреплено введением новой ст. 10.3 Закона об информации, которая предоставляет гражданину возможность требовать от оператора поисковой системы удаления ссылок на информацию о себе, распространяемую с нарушением законодательства, являющуюся недостоверной или утратившей актуальность в сети «Интернет». Данная статья была введена Федеральным законом от 13.07.2015 № 264-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации»[8] и регулирует деятельность операторов поисковых систем, возлагая на них обязанность прекращать по требованию гражданина выдачу ссылок на информацию о нем, если она распространяется с нарушением законодательства, является недостоверной или утратила актуальность, за исключением сведений о преступлениях, по которым не истекли сроки давности или не снята судимость.

По своей сути, право на забвение представляет собой юридическую возможность гражданина обратиться к владельцу информационного ресурса с требованием об удалении или ограничения доступа к личной информации. Основанием для такого требования служит утрата информацией былой актуальности и общественной значимости, либо ее сохранение в открытом доступе продолжает наносить ущерб репутации и достоинству лица, несмотря на изначально законную публикацию. При этом данное право не носит безусловного характера и должно находиться в гармонии с иными конституционными правами, в частности, со свободой распространения информации и правом общества на получение социально значимой информации.

В формулировке 2015 г. в п. 1 ст. 10.3 Закона об информации был сделан акцент на обязанности прекратить выдачу ссылок только оператора поисковой системы, распространяющего в сети «Интернет» рекламу, «которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации». Таким образом, обязанность применять право на забвение изначально была возложена не на всех операторов поисковых систем, а лишь на тех, чья деятельность была сопряжена с распространением рекламы, нацеленной на российских потребителей.

Новая редакция ст. 10.3, вступившая в силу с 1 октября 2024 г., устранила этот критерий. Норма теперь обращена к оператору поисковой системы без каких-либо дополнительных условий, касающихся рекламной деятельности.

Данная корректировка представляется логичным и последовательным шагом в развитии российского законодательства в цифровом пространстве. Предыдущая редакция Закона об информации создавала неравные условия для различных поисковых систем. Крупные коммерческие операторы, такие как Яндекс и Google, были обязаны исполнять требования о прекращении выдачи ссылок, в то время как нишевые или некоммерческие поисковые сервисы, формально не подпадавшие под критерий распространения рекламы, могли игнорировать такие запросы. Это нарушало принцип равенства всех субъектов, осуществляющих аналогичную деятельность по индексации и выдаче информации на территории РФ. Изменение согласуется с общей тенденцией усиления защиты персональных данных и частной жизни граждан в цифровом пространстве. Теперь механизм защиты прав граждан стал универсальным и применяется ко всем поисковым системам, функционирующим в российском сегменте сети «Интернет», независимо от их хозяйственной деятельности. Это повысило гарантии реализации гражданами своего права на защиту репутации и приватности. Изменение 2024 г. направлено на унификацию правового регулирования и распространение обязанности по соблюдению права на забвение на всех операторов поисковых систем без исключений, что подтверждается статистикой Яндекс.

По результатам статистики Яндекс[9], в числе обращений о праве на забвение за 2019 г. (июль–декабрь) доля отказов обращений по неактуальности – 79%, по недостоверности – 80%, по нарушению закона – 81%. За прошедшие пять лет

[8] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации : федер. закон от 13.07.2015 № 264-ФЗ // Собр. законодательства Рос. Федерации. 2015. № 29 (ч. I), ст. 4390.

[9] Transparency Report // СтатистикаЯндекс. URL: https://yandex.ru/company/privacy/transparencyreport (дата обращения: 26.09.2025).

и с принятием поправки в 2024 г. наблюдается резкое, в несколько раз, уменьшение удовлетворенных заявлений. В 2024 г. (июль–декабрь) по этой категории обращений по закону о праве на забвение произошло уменьшение отказов удовлетворенных обращений по неактуальности до 28% (в 2,8 раза), по недостоверности – 13% (уменьшение в 6,2 раза), по нарушению закона – 16% (в 5,0 раз).

Действующее российское законодательство предусматривает административный и судебный порядок защиты прав граждан от распространения недостоверной информации.

Первоначальным действием для гражданина, чьи права нарушены, является обращение: к владельцу информационного ресурса (сайта, страницы в социальной сети) с требованием удалить недостоверные сведения; к оператору поисковой системы (Яндекс, Google и др.) – с требованием прекратить выдачу ссылки на ресурс, содержащий недостоверную информацию, в соответствии со ст. 10.3 Закона об информации. В случае неисполнения данного требования гражданин вправе обратиться в федеральный орган исполнительной власти – Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Центральной правовой коллизией в рассматриваемом механизме является вопрос о том, кто и каким образом устанавливает факт недостоверности информации. Операторы поисковой системы (Яндекс, Google) с точки зрения закона являются техническими посредниками, предоставляющими сервис индексации и поиска. Они не обладают ни экспертизой, ни правомочностью проводить самостоятельную юридическую и фактологическую проверку содержания миллионов проиндексированных страниц. Их задача – обеспечить функционирование поискового алгоритма. Оператор поисковой системы, получив мотивированное заявление (по ст. 15.7 Закона об информации), обязан в течение 24 часов с момента получения заявления или уточненных заявителем сведений ограничить доступ к информации, указанной в заявлении, и уведомить владельца информационного ресурса (сайта) о примененных мерах. Владелец сайта, в свою очередь, вправе обжаловать такие действия в судебном порядке. Данный внесудебный механизм, предусмотренный ст. 15.7 Закона об информации, призван оперативно пресекать распространение потенциально вредоносного контента. Операторы занимают позицию, согласно которой они не являются арбитрами в установлении истины. Без вступившего в законную силу решения суда, прямо предписывающего удалить конкретную ссылку, они считают требования досрочными и возлагающими на них несвойственную правоприменительную функцию.

Анализ судебной практики по делам, связанным с оспариванием негативных отзывов в сети «Интернет», а также на таких платформах, как «Яндекс.Карты» и «Яндекс.Услуги», демонстрирует формирование единого подхода, основанного на принципах, заложенных в практике Конституционного Суда РФ и Европейского Суда по правам человека (ЕСПЧ).

Например, Хамовнический районный суд г. Москвы в решении от 25 января 2024 г. по делу к ООО «Яндекс», рассмотрев в открытом судебном заседании гражданское дело № 02-852/2024 по иску Воробьева Александра Сергеевича к ООО «Яндекс» о защите деловой репутации[10], указал, что сам факт написания отзыва на адвоката в оскорбительном тоне, без призывов к насилию и иным противоправным действиям, не является достаточным основанием для его удаления. Истец имел возможность дать аргументированный ответ прямо на платформе. Как итог – отрицательный отзыв не был удален, так как текст отзыва составляется и публикуется пользователем самостоятельно.

Суды возлагают на истца (компанию, врача, адвоката) повышенное бремя доказывания недостоверности и порочащего характера информации. Недостаточно просто утверждать, что отзыв ложный. Истец должен доказать, что описанные в отзыве события не происходили. Если пользователь пишет общими фразами («ужасная клиника», «руководство не хочет решать ситуацию» – например, дело № А40-208757/22-15-1602 от 17 марта 2023 г., г. Москва[11]), не раскрывая деталей (точная дата, имя врача, диагноз), суд квалифицирует это как оценочное суждение, а не утверждение о факте. Оспаривание оценочных суждений в исковом порядке практически невозможно.

Практика показывает, что право на забвение в отношении негативных отзывов применяется крайне ограниченно. Как следует из анализа дел (включая дело в Арбитражном суде г. Москвы 2023 г.), простое наличие негативного отзыва,

[10] URL: https://mos-gorsud.ru/rs/hamovnicheskij/cases/docs/content/0d231360-bb7e-11ee-abcd-a3010289f8ad (дата обращения: 26.09.2025).

[11] URL: https://sudact.ru/arbitral/doc/eu5dCb1Othdm/ (дата обращения: 26.09.2025).

даже если он наносит ущерб репутации, не является основанием для его удаления по праву на забвение, если он представляет собой субъективное мнение, а не заведомо ложные факты. Суды указывают, что ущерб от «оттока клиентов» должен компенсироваться не цензурой, а активной работой с репутацией, включая публичные ответы на критику.

Таким образом, современная судебная практика выстроила стройную систему, в рамках которой удаление негативного отзыва является исключительной, а не рядовой мерой. Основной путь защиты для бизнеса и специалистов является не иск об удалении, а активное участие в дискуссии, например, публикация аргументированных ответов, предоставление доказательств своей позиции и использование всех инструментов обратной связи, предоставляемых платформами. Это создает баланс, при котором защита деловой репутации не подменяется цензурой.

Однако если отзывы в сети «Интернет» носят оскорбительный характер и не соответствуют действительности, то иски подлежат удовлетворению. Например, Конституционный Суд РФ в Постановлении № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона “О персональных данных” в связи с жалобой общества с ограниченной ответственностью “МедРейтинг”»[12] в 2021 г. выявил конституционно-правовой смысл оспариваемой нормы, установив, что обработка персональных данных медицинского работника без его согласия допустима для целей информированного выбора врача, поскольку такие сведения, будучи размещенными на сайте медучреждения, признаются имеющими общественный интерес. В ходе повторного рассмотрения дела суд апелляционной инстанции удовлетворил частично исковые требования медицинского работника, обязав оператора сайта прекратить обработку ее персональных данных и удалить профиль, а также взыскав компенсацию морального вреда. Правовым основанием для принятия такого решения послужил вывод о наличии на платформе непроверенных оскорбительных отзывов, порочащих профессиональную репутацию истицы. У истицы не было технической возможности на сайте ответить на оскорбительные отзывы. Суд констатировал отсутствие у последней действенных механизмов для самостоятельной защиты своих прав, что свидетельствует о нарушении баланса между свободой распространения информации и правом на защиту чести и достоинства. Вместе с тем Суд возложил на редакцию сетевого СМИ (адрес сайта в сети «Интернет»: prodoctorov.ru) ООО «МедРейтинг» обязанность обеспечивать баланс прав, не допуская распространения непроверенных, оскорбительных высказываний и предоставляя врачу право на ответ, а также предусмотрев возможность судебного запрета на распространение информации в случае систематических нарушений. Таким образом, правовая позиция Суда направлена на поиск справедливого равновесия между свободой массовой информации и правом на неприкосновенность частной жизни и защиту деловой репутации.

Проведенный анализ позволяет заключить, что право на забвение реализуется через систему взаимодополняющих правовых механизмов. В Российской Федерации был создан уникальный административно-судебный механизм, сфокусированный исключительно на операторах поисковых систем, что отличает его от более общего общеевропейского подхода, основанного на принципах защиты персональных данных.

Другим механизмом обеспечения информационной безопасности личности является блокировка вредоносной информации, распространяемой в сети «Интернет». Его правовая база содержится в Законе об информации в ст. 15.1–15.6, а также в отраслевом законодательстве. По ст. 15.1-2 Закона об информации устанавливается порядок ограничения доступа к недостоверной информации, которая порочит честь и достоинство гражданина или подрывает его репутацию и связана с обвинением гражданина в совершении преступления. Процедура блокировки инициируется уполномоченными государственными органами – Роскомнадзором, прокуратурой – в отношении информации, распространение которой прямо запрещено на территории Российской Федерации.

По итогам 2024 г. Роскомнадзором в рамках осуществления контрольно-надзорных полномочий было ограничено распространение более 44 тысяч интернет-ресурсов, используемых для противоправной деятельности, связанной с мошенничеством[13]. Данные меры применялись на основании положений Закона об информации в целях пресечения противоправных посягательств на имущественные права

[12] По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг» : постановление Конституционного Суда РФ от 25.05.2021 № 22-П // Собр. законодательства Рос. Федерации. 2021. № 22, ст. 3915.

[13] Дмитрий Григоренко: Роскомнадзор заблокировал свыше 44 тыс. мошеннических сайтов в прошлом году. URL: http://government.ru/news/55581/ (дата обращения: 26.09.2025).

граждан. Осуществление блокировок является составной частью государственной политики, направленной на минимизацию киберрисков и обеспечение безопасности личности в цифровом пространстве.

Блокировка сайтов направлена на обеспечение информационной безопасности личности, в частности, обеспечение общественной безопасности (пресечение несанкционированных акций, призывов к массовым беспорядкам); информационно-психологическую защиту (противодействие терроризму, дезинформации); защиту физического здоровья (борьба с суицидами и наркотиками); информацию, оскорбляющую человеческое достоинство и общественную нравственность; информацию, содержащую предложение о финансировании противника в условиях вооруженного конфликта; защиту несовершеннолетних. По ст. 15.3 Закона об информации блокируются «ложные сообщения об актах терроризма и иная недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности». Под такой недостоверной общественно значимой информацией подразумеваются фейки.

Статьи 272, 273, 274 УК РФ[14] формируют уголовно-правовую защиту в сфере компьютерной информации. Однако их диспозиции были сформулированы в эпоху, когда основной угрозой был неправомерный доступ к изолированным компьютерным системам и распространение вирусов. В настоящее время распространены другие виды преступлений в сфере компьютерной информации, такие как фишинг, вишинг, взлом аккаунтов пользователей и др.

Распоряжением Правительства РФ от 30.12.2024 № 4154-р была утверждена Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий[15], которая представляет собой основу для построения целостной государственной системы противодействия киберпреступности, интегрирующую правовые, организационные и технологические компоненты. Концепция акцентирует необходимость создания специализированной цифровой платформы для оперативного межведомственного обмена информацией и адаптации законодательства к новым способам совершения противоправных деяний.

Кибермошенничество (ст. 159.6 УК РФ) эволюционировало от простого взлома аккаунтов до сложных схем социальной инженерии и фишинга, где жертва добровольно передает злоумышленникам доступ к своим средствам. Доказывание умысла и прямого причинения имущественного ущерба в таких схемах, особенно при использовании криптовалют и анонимных платежных систем, представляет значительную сложность для правоохранительных органов. Кибермошенники воздействуют непосредственно на гражданина чаще всего по телефону, оказывая информационно-психологическое воздействие. Объекту воздействия внушают, какие действия он должен произвести – продать квартиру, взять кредит.

В рамках антимошеннических поправок к Федеральному закону от 07.07.2003 № 126-ФЗ «О связи», подготовленных Минцифры, предлагается создать централизованную биометрическую базу для борьбы с телефонным мошенничеством. Ее основой станет единая государственная антифрод-платформа. С правовой точки зрения инициатива вводит особый порядок обработки биометрии. Сбор голосовых данных (в форме цифровых векторов) лиц, причастных к мошенничеству, будет проводиться без их согласия. Это исключение из общего правила, установленного законодательством о персональных данных. Технически сбору подлежат не аудиозаписи, а обезличенный вектор голоса, что является результатом математического преобразования. Голоса из этих фрагментов нельзя будет восстановить до исходного голоса, что не нарушит приватности.

Финансирование проекта оценивается более чем в 6 млрд руб.[16] Платформа будет аккумулировать информацию о правонарушениях от широкого круга субъектов: от правоохранительных органов и ЦБ до операторов связи, хостинг-провайдеров, социальных сетей и граждан. Запуск в эксплуатацию намечен на конец 2026 г.

Выявленные правовые проблемы информационной безопасности личности в цифровом пространстве указывают на необходимость совершенствования правовых норм в сторону

[14] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собр. законодательства Рос. Федерации. 1996. № 25, ст. 2954.

[15] Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий : распоряжение Правительства РФ от 30.12.2024 № 4154-р // Собр. законодательства Рос. Федерации. 2025. № 2, ст. 76.

[16] На госплатформе показался план денег. URL: https://www.kommersant.ru/doc/7197122 (дата обращения: 26.09.2025).

увеличения ответственности в части противодействия киберпреступности, защиты граждан РФ от распространения недостоверной информации и реализации права на забвение.

Проанализированная статистика Яндекс до 2024 г. по обращениям о праве на забвение показывает достаточно большое количество отказов – 80%, что обусловливается ограниченным применением нормы права только на операторов поисковых систем, чья деятельность была сопряжена с распространением рекламы, нацеленной на российских потребителей. Усовершенствованная норма права в 2024 г. устранила неравенство между операторами поисковых систем, показала большую эффективность применения права на забвение, усовершенствовала защиту прав пользователя сети «Интернет».

Существующая модель правового регулирования информационной безопасности личности в цифровом пространстве является фрагментарной. Она не охватывает всю совокупность прав личности, реализуемых с помощью цифровых технологий. В связи с этим необходим переход от обеспечения информационной безопасности личности, общества и государства в совокупности субъектов к комплексному обеспечению информационной безопасности личности.

Результаты

Современное состояние правового регулирования демонстрирует, что защита человека в информационном пространстве требует не только технических, но и правовых решений, затрагивающих основы правосубъектности, конфиденциальности и доверия к цифровому пространству.

Проблема переосмысления традиционных правовых подходов к информационной безопасности личности в цифровом пространстве в цифровую эпоху выходит далеко за рамки защиты от кибермошенничества, фейков и включает в себя право на достоверность информации о себе.

Эмпирический анализ показал, что выстраиванию системы правовой защиты личности от угроз в цифровом пространстве способствует применение специальных юридических инструментов, в частности, норм о персональных данных, права на забвение и института ограничения распространения вредоносной информации.

Комплексный подход сможет обеспечить реализацию фундаментального права человека на безопасность и автономию в цифровом пространстве. Реализовать такой подход можно в разработке и закреплении на законодательном уровне понятия «информационная безопасность личности»; совершенствования составов преступлений в УК РФ с учетом новых цифровых угроз и выработки общих стандартов информационной безопасности личности в цифровом пространстве.

Решением выявленных проблем может быть разработка и принятие Доктрины информационной безопасности личности; законодательное закрепление определения информационной безопасности личности, формирование комплексной системы защиты личности в цифровом пространстве, включающей правовые и технические средства.

Список литературы

1. *Аверьянова Н. Н., Куликова С. А.* Роль модельного законодательства СНГ в законотворческой и правоприменительной практике государств – участников Содружества // Журнал российского права. 2025. Т. 29, № 6. С. 144–157. https://doi.org/10.61205/S160565900032595-8
2. *Полякова Т. А., Минбалеев А. В., Бойченко И. С.* Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде // Вестник Академии права и управления. 2018. № 3 (52). С. 32–36. EDN: YLVHJB
3. *Белокопытова Н. Ю., Анучкина А. Д.* Проблемы правового обеспечения информационной безопасности личности в Российской Федерации // Фундаментальные и прикладные исследования: проблемы и результаты. 2014. № 13. С. 308–312.
4. *Зуев Д. И.* Эволюция права на неприкосновенность частной жизни в эпоху цифровых технологий // Эффективность государственного и муниципального управления: правовые аспекты : материалы 3-й межвуз. науч.-практ. конф. для молодых ученых (Иркутск, 28 февраля 2023 г.) / отв. ред. А. Г. Самусевич. Иркутск : Иркутский ин-т (филиал) ВГУЮ (РПА Минюста России), 2023. С. 26–30.
5. Информационное право : учебник для вузов / под общ. ред. М. А. Федотова. М. : Юрайт, 2021. 353 с. EDN: WGSQPZ
6. Обеспечение защиты прав человека в Российской Федерации / Г. Н. Комкова, М. А. Липчанская, С. А. Куликова [и др.]. М. : Инфра-М, 2022. 339 с. https://doi.org/10.12737/1200563, EDN: SHHOUQ
7. *Полякова Т. А., Минбалеев А. В., Троян Н. А.* Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С. 131–144. https://doi.org/10.31857/S102694520025209-0, EDN: JUISEQ
8. *Амелин Р. В., Чаннов С. Е.* Эволюция права под воздействием цифровых технологий. М. : Норма, 2025. 280 с.
9. *Демкин В. О.* Цифровая личность и цифровой образ человека: характеристика и место понятий в систе-

ме смежных категорий // Вестник РУДН. Серия: Юридические науки. 2024. Т. 28, № 3. С. 512–527. https://doi.org/10.22363/2313-2337-2024-28-3-512-527, EDN: FTBYVW

10. *Ефимова Л. Г.* Цифровая личность как способ присутствия субъекта права в киберпространстве // Вестник Университета имени О. Е. Кутафина (МГЮА). 2025. № 4 (128). С. 32–41. https://doi.org/10.17803/2311-5998.2025.128.4.032-041
11. *Чеботарева А. А.* Информационная безопасность личности в глобальном информационном обществе: теоретико-правовые аспекты // Российская юстиция. 2016. № 8. С. 39–42. EDN: WICVXN
12. *Чеботарева А. А.* Правовое обеспечение информационной безопасности личности в глобальном информационном обществе : дис. … д-ра юрид. наук. М., 2018. 473 с.
13. *Бачило И. Л.* Информационное право : учебник. 5-е изд., пер. и доп. М. : Юрайт, 2019. 419 с.
14. *Cohen J. E.* Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. 368 p. https://doi.org/10.1093/oso/9780190246693.001.0001
15. Правовое регулирование бережного и устойчивого оборота данных / Е. В. Архангельская, А. С. Васильева, Л. О. Гонтарь [и др.]. М. : Инфра-М, 2025. 215 с.
16. *Середа В. Н., Середа М. Ю.* Защита прав и свобод человека и гражданина в сети Интернет. Воронеж : ИПЦ «Научная книга», 2013. 252 с. EDN: RVECCN

References

1. Averyanova N. N., Kulikova S. A. The role of the CIS model legislation in the legislative and law enforcement practice of the commonwealth member states. *Journal of Russian Law*, 2025, vol. 29, № 6, pp. 144–157 (in Russian). https://doi.org/10.61205/S160565900032595-8
2. Polyakova T. A., Minbaleev A. V., Boychenko I. S. Issues of legal support of information safety during use of digital technologies in a global digital environment. *Vestnik Akademii prava i upravleniya* [Bulletin of the Academy of Law and Management], 2018, no. 3 (52), pp. 32–36 (in Russian). EDN: YLVHJB
3. Belokopytova N. Yu., Anuchkina A. D. Problems of legal provision of information security of the individual in the Russian Federation. *Fundamental'nye i Prikladnye Issledovaniia: Problemy i Rezul'taty*, 2014, vol. 13, pp. 308–312 (in Russian).
4. Zuev D. I. The evolution of the right to privacy in the digital age. *Effektivnost' gosudarstvennogo i munitsipal'nogo upravleniya: pravovye aspekty: materialy 3-y mezhvuzovskoy nauchno-prakticheskoy konferentsii dlya molodykh uchenykh* [Samusevich A. G. (ed.) Effectiveness of State and Municipal Nanagement: Legal Aspects: Proceedings of the 3rd Interuniversity scientific and practical conference for young scientists (Irkutsk, February 28, 2023). Irkutsk, Irkutsk Institute (branch) The Supreme Court (RPA of the Ministry of Justice of Russia) Publ., 2023, pp. 26–30 (in Russian).
5. *Informatsionnoe pravo* [Fedotov M. A. (ed.) Information law]. Moscow, Yurayt, 2021. 353 p. (in Russian). EDN: WGSQPZ
6. Komkova G. N., Lipchanskaya M. A., Kulikova S. A. et. al. *Ensuring the protection of human rights in the Russian Federation*. Moscow, Infra-M, 2022. 339 p. (in Russian). https://doi.org/10.12737/1200563, EDN: SHHOUQ
7. Polyakova T. A., Minbaleev A. V., Troyan N. A. Formation of a culture of information security of citizens of the Russian Federation in the face of new challenges: Public law problems. *State and Law*, 2023, iss. 5, pp. 131–144 (in Russian). https://doi.org/10.31857/S102694520025209-0, EDN: JUISEQ
8. Amelin R. V., Channov S. E. *Evolyutsiya prava pod vozdeystviem tsifrovykh tekhnologiy* [The evolution of law under the influence of digital technologies]. Moscow, Norma, 2025. 280 p. (in Russian).
9. Demkin V. O. Digital identity and digital image of an individual: Legal characteristics and the place in the system of related categories. *RUDN Journal of Law*, 2024, vol. 28, no. 3, pp. 512–527 (in Russian). https://doi.org/10.22363/2313-2337-2024-28-3-512-527, EDN: FTBYVW
10. Efimova L. G. Digital personality as a way of legal entity's presence in cyberspace. *Vestnik Universiteta imeni O. E. Kutafina (MGIuA)* [Bulletin of the O. E. Kutafin University (MGUA)], 2025, no. 4 (128), pp. 32–41 (in Russian). https://doi.org/10.17803/2311-5998.2025.128.4.032-041
11. Chebotareva A. A. Information security identity in the global information society: Theoretical and legal aspects. *Rossiyskaya Yustitsiya*, 2016, no. 8, pp. 39–42 (in Russian). EDN: WICVXN
12. Chebotareva A. A. *Legal provision of personal information security in the global information society*. Diss. Dr. Sci. (Jur.). Moscow, 2018. 473 p. (in Russian).
13. Bachilo I. L. *Informatsionnoe pravo* [Information law]. Moscow, Yurayt, 2019. 419 p. (in Russian)
14. Cohen J. E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press, 2019. 368 p. https://doi.org/10.1093/oso/9780190246693.001.0001
15. Arkhangelskaya E. V., Vasilyeva A. S., Gontar L. O. et. al. *Pravovoe regulirovanie berezhnogo i ustoichivogo oborota dannykh* [Legal regulation of careful and sustainable data turnover]. Moscow, Infra-M, 2025. 215 p. (in Russian).
16. Sereda V. N., Sereda M. Yu. *Zashchita prav i svobod cheloveka i grazhdanina v seti Internet* [Protection of human and civil rights and freedoms on the Internet], Voronezh, Publishing and Printing Center Nauchnaya kniga Ltd, 2013. 252 p. (in Russian). EDN: RVECCN

Поступила в редакцию 29.09.2025; одобрена после рецензирования 27.10.2025; принята к публикации 28.10.2025
The article was submitted 29.09.2025; approved after reviewing 27.10.2025; accepted for publication 28.10.2025