

Дата поступления рукописи в редакцию: 28.07.2026 г.
Дата принятия рукописи в печать: 11.09.2026 г.

DOI: 10.24412/2949-0871-2026-4-53-57

КАЗАКОВА Евгения Борисовна,
кандидат юридических наук, доцент,
заведующий кафедрой «Частное и публичное право»
Пензенского государственного университета,
Пенза, Россия,
e-mail: 1-janni@list.ru

НАРМАТОВА Софья Эдуардовна,
студентка Юридического института
Пензенского государственного университета,
Пенза, Россия,
e-mail: narmatova.s@yandex.ru

ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ПРИОРИТЕТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

АННОТАЦИЯ. В настоящей статье проведено исследование правового регулирования информационной безопасности. Делается акцент на том, что информационная безопасность – важная составляющая национальной безопасности. Вектором права служит рассмотрение информационной безопасности в контексте культурной сферы. Вследствие чего в статье были проанализированы правовые аспекты регулирования информационной безопасности, которая является ключом к пониманию защиты прав человека в цифровой среде. По итогам проведенного исследования теоретико-правового регулирования в сфере информационной безопасности сделан вывод о необходимости дальнейшего совершенствования законодательства.

КЛЮЧЕВЫЕ СЛОВА: информационная безопасность, правовое регулирование, стратегический национальный приоритет, сфера культуры, вектор права, культурные права, цифровая среда, угрозы, самозащита, национальная безопасность.

KAZAKOVA Evgeniya Borisovna,
Candidate of Law, Associate Professor,
Head of the Department of Private and Public Law at
Penza State University,
Penza, Russia

NARMATOVA Sofya Eduardovna,
Student of the Law Institute,
Penza State University,
Penza, Russia

LEGAL ASPECTS OF INFORMATION SECURITY REGULATION AS A NATIONAL SECURITY PRIORITY

ANNOTATION. This article contains a study of the legal regulation of information security. The emphasis is on the fact that information security is an important component of national security. The vector of law is the consideration of information security in the context of the cultural sphere. As a result, the article analyzed the legal aspects of information security regulation, which is the key to understanding the protection of human rights in the digital environment. Based on the results of the study of theoretical and legal regulation in the field of information security, it was concluded that further improvement of legislation is necessary.

KEY WORDS: information security, legal regulation, strategic national priority, cultural sphere, vector of law, cultural rights, digital environment, threats, self-defense, national security.

На сегодняшний день особую важность представляет информационная безопасность в условиях технологического развития. Намечалась тенденция, что влияние на гражданские правоотношения оказывает цифровая трансформация через призму национальной безопасности. Цифровые технологии активно развиваются и внедряются в отрасль культуры, и центральное место занимает информационная безопасность как один из приоритетов национальной безопасности.

Несомненно, информационная безопасность прав человека в сфере культуры является правовым ориентиром в рамках национальной безопасности. Следовательно, в данном исследовании крайне важно акцентировать внимание на следующих аспектах: во-первых, информационной безопасности прав человека, а во-вторых, культурной сфере, что в совокупности служит важной составляющей национальной безопасности государства в современных реалиях вызовов общества.

На сегодняшний день ключевое значение представляет культурное многообразие страны, сохранение культурных ценностей, обеспечение культурных прав человека через призму национальной безопасности государства. В целях обеспечения защиты прав человека в цифровой среде в сфере культуры неотъемлемым элементом служит информационная безопасность.

Следует проанализировать взаимодействие культурной сферы и информационной безопасности на основе архитектуры правового регулирования.

23 июня 2026 года Распоряжением Правительства РФ № 1586-р было утверждено Стратегическое направление в области цифровой трансформации отрасли культуры Российской Федерации до 2030 года [4], в котором в пункте 1 раздела III зафиксировано следующее положение: «Ключевым вектором цифровой трансформации в отрасли культуры является достижение технологического суверенитета...» [4]. А также отмечается, что «Эксплуатация зарубежных решений в сфере информационных технологий в государственном секторе сопряжена со следующими критическими рисками...», как зафиксировано в документе: «наличие скрытых (недекларированных) возможностей в закрытом исходном коде...» [4] и другие. Таким образом, особую важность представляет достижение технологического суверенитета в рассматриваемой отрасли. В связи с чем с целью обеспечения технологического суверенитета следует раскрыть место информационной безопасности.

В соответствии со Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 2 июля 2021 года № 400 [3] (далее – Стратегия), среди девяти зафиксированных стратегических национальных приоритетов информационная безопасность от-

мечается в качестве четвертого приоритета. В Стратегии в подпункте 2 пункта 57 раздела «Информационная безопасность» отмечается решение следующей задачи: «развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз» [3].

Рассмотрим подробно вышеуказанную в Стратегии задачу, на основе которой интерпретируем ее значимость, через сопоставление с защитой прав человека в сфере культуры в рамках цифровой среды.

Одной из первых задач является развитие системы прогнозирования, что играет ключевое значение на начальной стадии предвидения угроз информационной безопасности.

Следовательно, особое значение в контексте прогнозирования представляет совокупность приемов и методов посредством аналитического исследования угроз в информационной сфере в раскрытии дальнейшего развития их природы в определенный временной период. Как справедливо отмечается, «аналитика угроз – это процесс выявления и анализа киберугроз» [11]. В связи с чем акцентируем внимание на вызовах в правовой действительности, уделяя внимание угрозам информационной безопасности в культурной сфере.

Одной из проблем в условиях цифровой трансформации общества является анонимность. В научной статье Шаповаловой Г. М. раскрывается данная проблема как угроза культурному суверенитету Российской Федерации [10]. Так, автором отмечаются такие угрозы, как распространение дезинформации, пропаганда чуждых культурных ценностей и идеологий [10, с. 195]. Таким образом, деструктивное воздействие в информационном пространстве в сфере культуры служит угрозой социально-культурному развитию государства, что может нанести ущерб в контексте рассмотрения национальной безопасности.

В правовом поле возрастающее значение представляет защита культурных ценностей, объектов культурного наследия, а также прав человека в сфере культуры: к примеру, право на приобщение к культурным ценностям (статья 12 Основ законодательства Российской Федерации о культуре) [5]. К примеру, приобщение к историческим ценностям – объектам архитектурного наследия, через произведения искусства с целью сохранения культурного многообразия. В условиях цифровой трансформации происходит развитие искусства в цифровом пространстве, что способствует культурному обмену.

Отметим вторую задачу – выявление угроз информационной безопасности. Для начала следует выделить основные свойства, на которых базируется информация: конфиденциальность,

целостность, доступность [8, с. 25].

В научной статье Турянской К. А. отмечается следующая точка зрения: «Основная цель выявления угроз информационной безопасности заключается в установлении текущей вероятности нарушения целостности или конфиденциальности...» [9, с. 151].

В рамках выявления информационных угроз в культурной сфере особый правовой интерес представляет комплексный подход с целью защиты объектов культурных ценностей в информационном пространстве, а также обеспечение безопасности прав граждан в сфере культуры.

В контексте национальной безопасности выявление угроз в культурной отрасли представляет первостепенное значение с целью их определения, которое должно быть реализовано путем установления негативных последствий и источников угроз безопасности информации. Следовательно, правовым ориентиром служит выявление информационных угроз в культурной сфере, их определение и дальнейшее предотвращение с целью защиты национальных интересов.

Третья составляющая рассматриваемой задачи – предупреждение угроз информационной безопасности. Следует уделить внимание комплексному подходу в предупреждении угроз, отметив такие методы, как: во-первых, технические, во-вторых, организационные и, в-третьих, правовые. Подробнее остановимся на последнем.

В соответствии с Приказом от 11 апреля 2025 года № 117 в пункте 34 раздела III зафиксировано 21 мероприятие, которое должно проводиться с целью защиты информации оператором (обладателем информации) [6].

Таким образом, своевременное предупреждение угроз способствует недопущению возможного причинения ущерба национальным интересам.

В контексте культурной сферы предупреждение угроз информационной безопасности представляет вектор права в обеспечении безопасности цифровых объектов культуры; защиты прав человека на доступ к культурным ценностям (часть 2 статья 44 Конституции РФ) [1]; защиты персональных данных в процессе посещения цифровых платформ. В связи с чем уделим внимание самозащите в цифровой среде. Так, в современных реалиях возникают ситуации, в которых действия заинтересованного лица наиболее результативны в защите прав и свобод [7, с. 184].

Акцентируем внимание на следующих мерах самозащиты, что позволяет заинтересованному лицу обезопасить себя собственными действиями. Так, с целью защиты персональных данных, помимо установления сложного пароля в личном кабинете, для пользователя важно безопасное поведение в цифровой среде. Особую важность представляет культура информационной

безопасности.

Пользователю при посещении сайта следует обратить внимание на сертификат безопасности, что свидетельствует о защищенности сайта. В диаметрально противоположном случае, если сертификат безопасности будет не установлен, то соединение будет не защищено, что создает угрозу персональным данным. Также в процессе раскрытия мер самозащиты гражданских прав в цифровой среде следует обратить внимание на развитие цифровой грамотности граждан. Так, в случае если пользователю в его личный кабинет поступила ссылка от непроверенного источника, необходимо быть осведомленным и проверять данную ссылку с целью защиты своего логина и пароля.

Возвращаясь к рассматриваемым задачам в области информационной безопасности, следует отметить четвертую задачу – определение источников угроз информационной безопасности, что представляет актуальность в связи с современными вызовами и эволюционирующими угрозами, на которые оказывают воздействие условия и факторы в реальности. Вследствие чего вытекает последняя неотъемлемая составляющая рассматриваемых задач – оперативная ликвидация последствий реализации угроз. Данная стадия представляет ключевую роль в целях дальнейшего восстановления после нанесенного ущерба национальным интересам.

В соответствии с Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 года № 646 [2] (далее – Доктрина) в разделе II зафиксированы национальные интересы в информационной сфере, среди которых в подпункте «а» пункта 8 подчеркивается «обеспечение и защита конституционных прав и свобод человека и гражданина...» [2].

Таким образом, при раскрытии информационной безопасности, в данном разделе уделяется внимание национальным интересам.

Следует проанализировать стратегические цели и основные направления обеспечения информационной безопасности, зафиксированные в разделе IV Доктрины, которые отмечены в следующих пунктах: 20, 21 – в области обороны страны, 22, 23 – в области государственной и общественной безопасности, 24, 25 – в экономической сфере, 26, 27 – в области науки, технологий и образования, 28, 29 – в области стратегической стабильности и равноправного стратегического партнерства. Таким образом, анализ данных положений позволяет сделать вывод, что в данных пунктах раскрываются стратегические цели и основные направления в рамках рассматриваемой информационной безопасности.

В связи с чем важна проработка вопросов по совершенствованию правового регулирования обеспечения информационной безопасности в сфере культуры. Так, в рассматриваемом IV раз-

деле документа важно предложить закрепление отдельных пунктов, направленных на регламентацию стратегических целей и основных направлений в сфере культуры.

Обобщая вышеизложенное, необходимо резюмировать, информационная безопасность как стратегический приоритет национальной безопасности представляет правовой ориентир в современных реалиях вызовов и угроз. На се-

годняшний день в таких условиях важна защита культурных прав человека в цифровой среде. Особое значение в рассматриваемом исследовании отводится анализу, а также проработке вопросов по совершенствованию правового регулирования обеспечения информационной безопасности в сфере культуры. Таким образом, информационная безопасность – правовой вектор национальной безопасности.

Список литературы:

- [1] Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // Официальный интернет-портал правовой информации URL: <http://www.pravo.gov.ru> (дата обращения: 13.07.2026).
- [2] Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.
- [3] Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. – 2021. – № 27 (часть II). – Ст. 5351.
- [4] Распоряжение Правительства РФ от 23.06.2026 № 1586-р «Об утверждении стратегического направления в области цифровой трансформации отрасли культуры Российской Федерации на период до 2030 года» // Собрание законодательства РФ. – 2026. – № 26. – Ст. 3618.
- [5] Основы законодательства Российской Федерации о культуре (утв. ВС РФ 09.10.1992 № 3612-1) (ред. от 24.06.2025) (с изм. и доп., вступ. в силу с 01.03.2026) // Российская газета. – 1992. – № 248.
- [6] Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (Зарегистрировано в Минюсте России 16.06.2025 № 82619) Официальный интернет-портал правовой информации URL: <http://pravo.gov.ru> (дата обращения: 13.07.2026).
- [7] Казакова Е. Б. Проблема выбора способов самозащиты гражданских прав // Тенденции развития современного общества: экономико-правовой аспект: сборник научных трудов международной научно-практической конференции. – Пенза: Изд-во Пенз. гос. технол. ун-тет., 2016. С. 183-186.
- [8] Какорин И. А. Основные принципы информационной безопасности // Международный журнал гуманитарных и естественных наук. 2023. № 2-2(77). С. 25-27. DOI 10.24412/2500-1000-2023-2-2-25-27.
- [9] Турянская К. А. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса // Международный журнал гуманитарных и естественных наук. 2024. № 2-2(89). С. 151-155.
- [10] Шаповалова Г. М. Анонимность в российском сегменте глобального информационного пространства сети Интернет – угроза культурному суверенитету Российской Федерации // Бизнес. Образование. Право. – 2025. – № 1(70). – С. 194-200. DOI: 10.25683/VOLBI.2025.70.1215.
- [11] Что такое аналитика угроз? Определение и описание // URL: <https://www.kaspersky.ru/resource-center/definitions/threat-intelligence> (дата обращения: 14.07.2026).

References:

- [1] Constitution of the Russian Federation. Adopted by popular vote on December 12, 1993, with amendments approved during the all-Russian vote on July 1, 2020 // Official Internet Portal of Legal Information URL: <http://www.pravo.gov.ru> (accessed: July 13, 2026).
- [2] Decree of the President of the Russian Federation No. 646 dated December 5, 2016, «On Approval of the Information Security Doctrine of the Russian Federation» // Collected Legislation of the Russian Federation. – 2016. – No. 50. – Art. 7074.
- [3] Decree of the President of the Russian Federation No. 400 dated July 2, 2021, «On the National Security Strategy of the Russian Federation» // Collected Legislation of the Russian Federation. – 2021. – No. 27 (Part II). – Art. 5351.
- [4] Directive of the Government of the Russian Federation No. 1586-r dated June 23, 2026, «On Approval of the Strategic Direction for the Digital Transformation of the Cultural Sector of the Russian Federation for the Period up to 2030» // Collected Legislation of the Russian Federation. – 2026. – No. 26. – Art. 3618.
- [5] Fundamentals of the Legislation of the Russian Federation on Culture (approved by the Supreme Council of the Russian Federation on October 9, 1992, No. 3612-1) (as amended on June 24, 2025) (with amendments and additions entering into force on March 1, 2026) // Rossiyskaya Gazeta. – 1992. – No. 248.
- [6] Order of the FSTEC of Russia dated April 11, 2025, No. 117 «On Approval of Requirements for the

Protection of Information Contained in State Information Systems and Other Information Systems of State Bodies, State Unitary Enterprises, and State Institutions» (Registered with the Ministry of Justice of Russia on June 16, 2025, No. 82619). Official Internet Portal of Legal Information. URL: <http://pravo.gov.ru> (accessed: July 13, 2026).

[7] Kazakova E. B. The Problem of Choosing Methods for the Self-Defense of Civil Rights // *Trends in the Development of Modern Society: Economic and Legal Aspects: Collection of Scientific Papers from the International Scientific and Practical Conference*. – Penza: Penza State Technological University Publishing House, 2016. – P. 183–186.

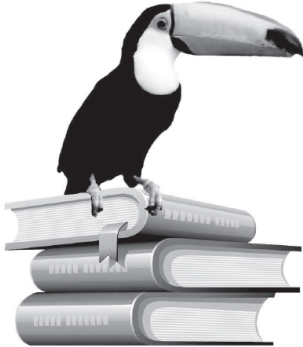
[8] Kakorin I. A. Basic Principles of Information Security // *International Journal of Humanities and Natural Sciences*. – 2023. – No. 2-2(77). – P. 25–27. DOI 10.24412/2500-1000-2023-2-2-25-27.

[9] Turyanskaya K. A. Methods, Models, and Tools for Detecting, Identifying, and Classifying Threats of Information Security Breaches Affecting Objects of Various Types and Classes // *International Journal of Humanities and Natural Sciences*. – 2024. – No. 2-2(89). – P. 151–155.

[10] Shapovalova G. M. Anonymity in the Russian Segment of the Global Internet Information Space: A Threat to the Cultural Sovereignty of the Russian Federation // *Business. Education. Law*. – 2025. – No. 1(70). – P. 194–200. DOI: 10.25683/VOLBI.2025.70.1215.

[11] What is threat intelligence? Definition and description // URL: <https://www.kaspersky.ru/resource-center/definitions/threat-intelligence> (accessed: 14.07.2026).





ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.