

Правовое обеспечение кибербезопасности



**Гульфия Гафиятовна
КАМАЛОВА,**

заведующий кафедрой
информационной
безопасности в управлении
Удмуртского
государственного
университета,
доктор юридических наук,
доцент
gulfia.kamalova@gmail.com
426034, Россия, г. Ижевск,
ул. Университетская, д. 1

Проблемы правового обеспечения доверия и информационной безопасности в цифровую эпоху¹

Аннотация. Статья посвящена информационно-правовым вопросам обеспечения безопасности цифровой среды посредством развития различных регуляторных механизмов, направленных на формирование доверия к информационно-коммуникационным технологиям и результатам их использования. Автором рассматриваются проблемы становления понятия «доверие» как информационно-правовой категории, а также целесообразность развития механизмов обеспечения доверия в цифровой среде, включающих достоверность и конфиденциальность данных, безопасность цифровых технологий и каналов связи. Отмечается, что необходимо повысить определенность в отношении критериев доверенности составляющих цифровой среды, усилить требования в части обеспечения цифрового суверенитета и локализации данных, а также создать правовые условия минимизации инцидентов информационной безопасности. В результате исследования сделан вывод, что лишь сочетание правового и технического регулирования позволит достичь доверия и безопасности в цифровой среде.

Ключевые слова: информационное право, цифровое право, доверие, информационная безопасность, цифровые технологии, цифровая среда, идентификация, конфиденциальность, доверенные технологии, цифровой суверенитет

DOI: 10.17803/2311-5998.2026.142.6.112-119

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 26-18-00897 «Создание правовой модели национального цифрового пространства доверия в целях обеспечения информационной безопасности и государственного суверенитета Российской Федерации».

Gulfia G. KAMALOVA,

Head of the Department of Information Security in Management,

Udmurt State University,

Dr. Sci. (Law), Associate Professor

gulfia.kamalova@gmail.com

1, ul. Universitetskaya, Izhevsk, Russia, 426034

Problems of Legal Assurance of Trust and Information Security in the Digital Age

Abstract. *The article is devoted to information and legal issues of ensuring the security of the digital environment through the development of various regulatory mechanisms aimed at building trust in information and communication technologies and the results of their use. The author examines the problems of the formation of the concept of “trust” as an information and legal category, as well as the expediency of developing trust mechanisms in the digital environment, including the reliability and confidentiality of data, the security of digital technologies and communication channels. It is noted that it is necessary to increase certainty regarding the criteria for the power of attorney of the components of the digital environment, strengthen the requirements for ensuring digital sovereignty and data localization, as well as create legal conditions for minimizing information security incidents. As a result of the study, it was concluded that only a combination of legal and technical regulation will allow to achieve trust and security in the digital environment.*

Keywords: *information law, digital law, trust, information security, digital technologies, digital environment, identification, confidentiality, trusted technologies, digital sovereignty*

Введение

В условиях динамичного внедрения цифровых технологий во все области жизнедеятельности человека и трансформации общественных отношений под их влиянием в научном пространстве активизируются правовые дискуссии о доверии к цифровым технологиям и результатам их применения. Вместе с тем понятие «доверие» как правовая категория пока остается институционально не оформленным и используется в праве на основе общих представлений о нем. В связи с этим в рамках настоящего исследования сделана попытка определить основные теоретические подходы, которые целесообразно рассматривать как основания для оформления понятия доверия в качестве информационно-правовой категории для последующего определения основных правовых средств его обеспечения и формирования механизма обеспечения доверия в цифровой среде.

При проведении исследования основным его стержнем выступила идея о том, что формирование доверия со стороны общества, государства и гражданина к цифровой среде предполагает достижение высокого уровня информационной безопасности цифровых сервисов и платформ, информационных систем



и информационной инфраструктуры в целом. Вместе с тем правовые вопросы достижения доверия к цифровой среде как результата обеспечения информационной безопасности этическими, правовыми, организационными и техническими средствами в настоящее время недостаточно исследованы и требуют научного осмысления. При этом автор исследования в работе исходит из того, что доверие в цифровой среде достижимо при обеспечении высокого качества цифровых данных, цифровой зрелости механизмов обеспечения информационной безопасности объектов цифровой среды, надежности каналов связи и добросовестности участников правоотношений, соответствия функционала цифровых сервисов ожиданиям субъекта правоотношений, что позволит формировать необходимое позитивное отношение к взаимодействию к цифровой среде.

Реализация национального проекта России «Экономика данных и цифровая трансформация государства»², направленного на усиление достигнутых результатов в области цифровой экономики, закономерно включает вопросы обеспечения кибербезопасности. Стратегически также важно, что Указом Президента РФ «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» в приоритетные задачи включено развитие цифровых платформ, управление данными, автоматизация транзакций, внедрение технологий больших данных и искусственного интеллекта, расширение предоставления государственных услуг в электронной форме и др.³ Решение указанных задач представляется невозможным без правового обеспечения доверия к цифровой среде и, соответственно, ее безопасности. В связи с этим целью настоящего исследования является комплексный анализ формирующихся правовых механизмов обеспечения доверия к цифровым технологиям в рамках построения национальной цифровой среды доверия.

Основная часть

Понятие «доверие» является междисциплинарным и вместе с тем наиболее разработанным в психологии, экономике, политологии, философии и социологии⁴. В праве интерес к вопросам доверия, в том числе на уровне диссертационных исследований, связан с вопросами эффективности права, обеспечением народного доверия, ответственности за злоупотребление доверием, доверия к полиции и другими, в том числе в рамках диссертационных исследований⁵. Вместе

² Национальный проект «Экономика данных и цифровая трансформация государства» // Официальный сайт Правительства России. URL: <http://government.ru/rugovclassifier/923/about/> (дата обращения: 06.03.2026).

³ См., например: Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // СЗ РФ. 2024. № 20. Ст. 2584.

⁴ См., например: *Скрипкина Т. П.* Доверие как социально-психологическое явление : дис. ... д-ра психол. наук. Ростов н/Д, 1998.

⁵ См., например: *Напольских И. М.* Доверие как условие эффективности действия права : автореф. дис. ... канд. юрид. наук. М., 2024.

с тем доверие и взаимосвязанные понятия сравнительно широко используются в законодательстве как самостоятельный термин или составная часть различных понятий, включая такие, как доверенность, злоупотребление доверием, доверенная третья сторона. Следовательно, даже сравнительно беглый анализ показывает, что доверие в праве является сложным феноменом, не только охватывающим эмоциональное отношение субъекта к другому субъекту или объекту, но и объективно выраженным в действиях, оно может подкрепляться правовыми гарантиями и влияет на правомерность определенных действий, а также взаимосвязано с правовой культурой и правосознанием участника правоотношений.

Экспоненциальное внедрение информационно-коммуникационных технологий и цифровая трансформация актуализировали вопрос о понятии доверия как информационно-правовой категории, что в области правового регулирования информационных отношений приобрело особое значение в связи с особенностями опосредованного характера информационного взаимодействия в цифровой среде. Хотя некоторые исследователи в области права⁶ обращались к вопросам формирования доверия в цифровой среде, вместе с тем такие исследования пока немногочисленны.

Следует отметить эволюцию концепции доверия в праве, которая проявляется в условиях цифровизации переходом от проявления в рамках исключительно межличностных отношений к необходимости институциональных норм в связи с опосредованным взаимодействием в цифровой среде. Обращает на себя внимание то, что исследователи рассматривают развитие цифровой среды доверия как одно из ключевых условий становления цифровой экономики⁷ и связывают ее с конфиденциальностью данных, достоверностью информации, ролью и правовым статусом субъектов взаимодействия и защищенностью среды взаимодействия. Указанное определяет возможный круг направлений правового воздействия на общественные отношения для формирования и поддержания доверия к цифровой среде, что определяет исследовательский интерес в рамках настоящего исследования.

Доверие в цифровой среде, именуемое порой цифровым доверием, может определяться через уверенность субъектов правоотношений в безопасности используемых информационно-технических средств и технологий, а также через предсказуемость результатов их использования⁸. Это может быть достигнуто путем выполнения установленных нормативными правовыми актами и документами по техническому регулированию требований к цифровым данным, безопасности

⁶ См., например: *Химченко А. И.* Вопросы формирования цифровой среды доверия как структурного элемента цифровизации государственного управления // Правовое государство: теория и практика. 2022. № 3 (69). С. 159—164 ; *Яковлева Е. А.* Правовая природа и сущность цифровой доверенной среды // Безопасность как стратегический национальный приоритет России в условиях современности : материалы Шестого международного транспортно-правового форума. М., 2024. С. 297—301.

⁷ *Терещенко Л. К.* Единая цифровая среда доверия как условие формирования цифровой экономики // Информационное право. 2020. № 4. С. 12—15.

⁸ *Кузнецов В. И., Кабытов П. П.* Теоретические подходы к категории «цифровая среда доверия» // Юридические исследования. 2021. № 2. С. 64—74.



информационных систем и цифровых сервисов, каналов связи, а также посредством определения субъектов взаимодействия в цифровой среде.

Меры обеспечения высокого качества данных, представленных в цифровой форме, играют одну из ключевых ролей в формировании доверия со стороны пользователей. Это напрямую связано с проблемами обеспечения достоверности цифровых данных и противодействия неправомерному распространению недостоверной информации. В связи с этим следует признать справедливым, что информационные угрозы, направленные на манипулирование общественным сознанием, искажение исторической памяти народа, подрыв доверия к государственным институтам и разрушение моральных ориентиров российского общества, являются наиболее опасными и подрывают доверие граждан к информации, представленной в цифровой среде.

Кроме того, значимое место занимает безопасность обработки персональных данных и иной, связанной с личностью человека и представленной в цифровой форме информации, утечка которой прямо или косвенно может нарушить его права. Принципы обработки персональных данных, включая минимизацию объема обрабатываемых данных, установленный законодательством потенциал определенного контроля со стороны субъекта персональных данных служат инструментами укрепления доверия граждан к действиям оператора персональных данных и информационным системам. Федеральные органы исполнительной власти осуществляют активное совершенствование конкретизированных требований к обработке персональных данных⁹. Реализация таких требований предполагает разработку и внедрение оператором широкого круга процедур и технических средств защиты данных. Усиливается юридическая ответственность в данной области.

Вместе с тем проблемы с утечкой персональных данных продолжают сохраняться¹⁰, что указывает на недостаточность существующих мер обеспечения безопасности цифрового оборота персональных данных. Кроме того, формируются дополнительные аспекты обеспечения безопасности персональных данных в цифровой форме в связи с тем, что в настоящее время цифровые платформы и сервисы в целях продвижения бизнеса и государственного управления обрабатывают значительные массивы данных граждан, которые не всегда могут быть строго отнесены к персональным данным, но вместе с тем взаимосвязаны с ними. Однако законодательство России не содержит норм об обязанности оператора платформы или сервиса применять риск-ориентированный подход для защиты цифровых данных пользователей, формирования системы защиты информации

⁹ 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» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 17.06.2025.

¹⁰ См., например: Крупнейшие утечки персональных данных за год // INFOWATCH. URL: <https://www.infowatch.ru/analytics/daydzhesty-i-obzory/krupneyshiye-utechki-personalnykh-dannykh-za-god> (дата обращения: 17.03.2026).

на всех этапах жизненного цикла и критериев определения уровня «цифровой зрелости» безопасности такой системы¹¹.

Отсутствие таких требований и правил обеспечения прозрачности механизмов обработки цифровых данных может усиливать недоверие граждан к современным цифровым платформам и сервисам, используемым в бизнес-процессах и системе государственного управления. Таким образом, необходимо специальное регулирование в области функционирования цифровых платформ и сервисов с целью повышения безопасности, предсказуемости и прозрачности цифровой среды обработки данных. Этой же цели служит предоставление информации о применении рекомендательных технологий¹².

Одним из важнейших условий обеспечения доверия является идентификация и аутентификация пользователей, направленная на повышение их защищенности и ответственности за действия в цифровой среде. Правовое обеспечение идентификации в цифровой среде имеет определенные особенности и предполагает дополнительные меры конфиденциальности информации, что отмечал В. Б. Наумов, который предложил развитие в информационном праве тайны идентификации¹³. Важное значение в связи с этим приобретают Единая система идентификации и аутентификации¹⁴ и Единая биометрическая система.

Институционально цифровое доверие формируется через безопасность информации, обеспечиваемой, наряду с правовыми институтами, посредством выполнения требований документов по стандартизации, сертификации средств защиты информации; процедур мониторинга и аудита; лицензирования деятельности в сфере защиты информации. Указанное позволяет достичь определенной предсказуемости уровня безопасности цифровых сервисов. Однако во многом этот процесс сегодня затрудняет правовая определенность в вопросах статуса операторов цифровых платформ, сервисов и экосистем.

Таким образом, эволюция моделей регулирования цифровой среды для обеспечения доверия к ней должна охватывать совершенствование защиты данных и требований к безопасности информационных систем и цифровых сервисов и включать не только правовые нормы, но и технические стандарты и организационные мероприятия, направленные на защиту данных. В связи с этим технические и организационные меры целесообразно закрепить в нормативных правовых актах как обязательные элементы обеспечения доверия. Формирование

¹¹ Полякова Т. А., Минбалева А. В. Понятие и правовая природа «цифровой зрелости» // Государство и право. 2021. № 9. С. 107—116.

¹² Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2025) «Об информации, информационных технологиях и о защите информации». Статья 10.2-2. // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

¹³ Наумов В. Б. Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. 2019. № 3 (32). С. 70—75.

¹⁴ Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // СЗ РФ. 2011. № 49 (ч. V). Ст. 7284.



доверия к цифровой среде носит комплексный характер и требует сочетания технических мер, организационной практики и правового регулирования, что позволит гарантированно обеспечить целостность, доступность и конфиденциальность информации.

В настоящее время стратегическое значение для обеспечения доверия к безопасности обработки цифровых данных в России имеют локализация данных как инструмент контроля и защиты критических массивов информации и достижение цифрового суверенитета России, что обусловлено потенциалом национального контроля безопасности компонентов цифровой среды¹⁵. В связи с этим целесообразно развитие вопросов юридической ответственности, включая вопросы распределения ответственности между субъектами и ответственности за преднамеренные алгоритмические ошибки. Кроме того, по-прежнему недостаточно развита юридическая ответственность за утечки информации по вине операторов цифровых платформ и информационных систем.

Проблемы в области информационной безопасности цифровых платформ и сервисов могут вызывать алармизм у граждан, усиливать их скептицизм в отношении цифровой трансформации государства, что создает определенные правовые риски. Усиление информационных угроз и усложнение их структуры требуют сегодня формализации процедур реагирования на инциденты информационной безопасности. В связи с этим целесообразно законодательное введение понятия «инцидент информационной безопасности» и установление процедур реагирования на них не только в части защиты персональных данных, но и для других критически важных цифровых данных.

Таким образом, проведенное исследование показало, что для достижения доверия и информационной безопасности в цифровой среде целесообразно решить несколько взаимосвязанных организационно-правовых задач:

- сформировать теоретические основы правового обеспечения доверия в цифровой среде;
- законодательно определить понятие доверия в цифровой среде;
- повысить определенность в отношении критериев доверенности составляющих цифровой среды;
- усилить нормативно-правовые требования к обеспечению цифрового суверенитета и локализации обработки цифровых данных;
- создать правовые условия минимизации рисков инцидентов информационной безопасности.

В завершение следует отметить, что только комплексный подход к регулированию цифровых технологий, обеспечение прозрачности алгоритмов и усиление юридической ответственности операторов цифровых платформ и сервисов, а также сочетание правового и технического регулирования позволят достичь доверия и безопасности в цифровой среде.

¹⁵ Камалова Г. Г. Национальный технологический суверенитет в сфере цифровых технологий: вопросы правового обеспечения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10 (122). С. 52—60.

БИБЛИОГРАФИЯ

1. Камалова Г. Г. Национальный технологический суверенитет в сфере цифровых технологий: вопросы правового обеспечения // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2024. — № 10 (122). — С. 52—60.
2. Кузнецов В. И., Кабытов П. П. Теоретические подходы к категории «цифровая среда доверия» // Юридические исследования. — 2021. — № 2. — С. 64—74.
3. Напольских И. М. Доверие как условие эффективности действия права : автореф. дис. ... канд. юрид. наук. — М., 2024. — 35 с.
4. Наумов В. Б. Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. — 2019. — № 3 (32). — С. 70—75.
5. Полякова Т. А., Минбалева А. В. Понятие и правовая природа «цифровой зрелости» // Государство и право. — 2021. — № 9. — С. 107—116.
6. Скрипкина Т. П. Доверие как социально-психологическое явление : дис. ... д-ра психол. наук. — Ростов н/Д, 1998. — 392 с.
7. Терещенко Л. К. Единая цифровая среда доверия как условие формирования цифровой экономики // Информационное право. — 2020. — № 4. — С. 12—15.
8. Химченко А. И. Вопросы формирования цифровой среды доверия как структурного элемента цифровизации государственного управления // Правовое государство: теория и практика. — 2022. — № 3 (69). — С. 159—164.
9. Яковлева Е. А. Правовая природа и сущность цифровой доверенной среды // Безопасность как стратегический национальный приоритет России в условиях современности : материалы Шестого международного транспортно-правового форума. — М., 2024. — С. 297—301.

