
ЮРИСПРУДЕНЦИЯ (JURISPRUDENCE)

Оригинальная статья/Original article

УДК 340

<https://doi.org/10.26907/2541-7738.2026.3.173-187>

Угрозы российским ценностям в контексте цифрового суверенитета

А.С. Агафонов

*Уральский государственный юридический университет им. В.Ф. Яковлева,
г. Екатеринбург, Россия*

aga.fonov@inbox.ru

Аннотация

Под цифровым суверенитетом понимается способность государства самостоятельно определять параметры регулирования собственного цифрового пространства и соответствующей инфраструктуры. Вопросы, исследуемые в рамках цифрового суверенитета, являются предметом весьма сложной и междисциплинарной научной дискуссии. В настоящей статье через призму сфер общественной жизни (экономической, социальной, политической и духовной) выявлены угрозы российским ценностям в контексте цифрового суверенитета. Сделан вывод о том, что угрозы, которые возникают в контексте цифрового суверенитета, напрямую связаны с конституционными ценностями. Кроме того, подобные угрозы могут привести к кризису всеобщего доверия, который выражается в двух проблемных проявлениях – субъект-объектном и субъект-субъектном.

Ключевые слова: цифровой суверенитет, конституционные ценности, угрозы, цифровые технологии, основы экономического строя, защита прав граждан, цифровая инфраструктура государства, нравственные начала, кризис доверия

Для цитирования: Агафонов А.С. Угрозы ценностям России в контексте цифрового суверенитета // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. 2026. Т. 168, кн. 3. С. 173–187. <https://doi.org/10.26907/2541-7738.2026.3.173-187>.

Threats to Russian values in relation to digital sovereignty

A.S. Agafonov

Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

aga.fonov@inbox.ru

Abstract

Digital sovereignty refers to the ability of a state to independently determine the parameters of regulation of its digital space and related infrastructure. The issues surrounding digital sovereignty have been the subject of extensive discussion from scholars across a wide diversity of disciplines. This article presents

the results of a study on Russia's steps to strengthen its digital sovereignty and threats to its national values in different public areas (economic, social, political, and spiritual) that may be associated with them. The obtained results show that such threats are inseparable from the protection of the core constitutional values and can lead to the general crisis of confidence at the subject–object and subject–subject levels.

Keywords: digital sovereignty, constitutional values, threats, digital technology, foundations of economic system, protection of citizens' rights, national digital infrastructure, ethical principles, crisis of confidence

For citation: Agafonov A.S. Threats to Russian values in relation to digital sovereignty. *Kazan Journal of Historical, Linguistic, and Legal Research*, 2026, vol. 168, no. 3, pp. 173–187. <https://doi.org/10.26907/2541-7738.2026.3.173-187>. (In Russian)

Введение

Исследование вопросов цифрового суверенитета Российской Федерации в части его обеспечения правовым инструментарием представляется в современных реалиях актуальным. Об этом свидетельствуют последние исследования, в которых делается акцент на необходимости определения понятия цифрового суверенитета [1, с. 72], осуществляется поиск его места в системе информационного права [2, с. 14], констатируется недостаточный уровень проработанности вопроса о сущности и средствах его правового обеспечения [3, с. 37] и т. д.

Нормы, определяющие цифровой суверенитет Российской Федерации, на сегодняшний день являются не просто «модным» формирующимся комплексным правовым институтом, а наиболее эффективным правовым механизмом создания и поддержания комфортной и безопасной среды для жизни, обеспечения технологического лидерства и цифровой трансформации, что соотносится с национальными целями страны, которые регламентированы Указом Президента Российской Федерации от 7 мая 2024 г. № 309 (УПРФ309).

Стоит согласиться с Ю.А. Тихомировым в том, что «юридическая наука призвана системно и динамично реагировать на происходящие процессы путем модернизации систематики в праве, повышения качества нормотворческой деятельности и эффективности механизма правоприменения» [4, с. 14]. Потенциал цифрового суверенитета России может быть раскрыт в полной мере только при условии его теоретического осмысления с применением методологии юридической науки и отделки правового материала¹, с учетом ценностной составляющей [5, с. 30].

Процесс развития технологий вновь привел государства к глобальной конкуренции, при которой отстранение или замедление служат предпосылками попадания в зависимость.

В.Д. Зорькин верно отметил, что технологии будут развиваться с нами или без нас. «В этих условиях применительно к сфере новых технологий, – пишет он, – стоит задача защитить государственный суверенитет, национальные интересы и безопасность»².

Именно в контексте защиты различного рода ценностей, в числе которых укрепление государственного суверенитета, информационная безопасность, обеспечение прав и свобод, технологическая автономность и пр., следует рассматривать отечественный научно-техно-

¹ фон Иеринг Р. Юридическая техника. СПб.: Типо-лит. А. Г. Розена (А. Е. Ландау), 1905. С. 35.

² Зорькин В.Д. Лекции о праве и государстве. СПб.: Конституционный Суд Российской Федерации, 2024. С. 236.

логический прогресс, связанный с разработкой и внедрением различных прорывных технологий. Зарубежные производители и правообладатели (в том числе из недружественных государств) не заинтересованы в наличии у Российской Федерации самостоятельных наукоемких и цифровых технологий, которые бы позволяли определять государственную идентичность в цифровой сфере.

Стремление к монополизации новых технологий, основанное на стремлении к различным благам, по верному утверждению В.Д. Могилевского, не монополизировало знания, составляющие основу этих технологий и позволяющие «воссоздать ее в других точках планеты»³. Полное замещение информационных технологий в России означает для зарубежных производителей и правообладателей потерю ряда возможностей, в частности, контролировать информационные потоки, манипулировать мнением масс и информацией, осуществлять хакерские атаки и т. д.

Цифровые технологии открывают инновационные возможности как для общественных отношений в области частного права, так и для совершенствования процесса реализации публичных функций. В то же время любая новая технология может быть использована в разрушительных целях.

Такое положение дел позволяет нам рассматривать сущностные элементы цифрового суверенитета с точки зрения двух возможных коннотаций – позитивной и негативной, что соотносится с позитивными и негативными возможностями, которые выделяет В.С. Степин в связи с появлением новых технологий [6, с. 10].

Позитивная коннотация выражена в положительном влиянии цифровых технологий на общественную жизнь: к примеру, это оптимизация публичных функций в части Единого портала государственных и муниципальных услуг, с помощью которого государство обеспечивает права и свободы граждан России, или разработка многофункционального сервиса обмена информацией в целях повышения доступности услуг в различных сферах жизнедеятельности. Негативная коннотация связана с отрицательным влиянием цифровых технологий на общественную жизнь: например, фишинговые сайты под видом официальных ресурсов государственных органов, за создание которых в Российской Федерации установлена юридическая ответственность, а именно ч. 6 ст. 14.35 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ).

Т.А. Полякова и Н.А. Троян утверждают, что в современных реалиях «необходимо понимание состояния защищенности интересов Российской Федерации, при котором гарантируется защита конституционно значимых ценностей в целях обеспечения суверенитета Российской Федерации» [7, с. 50].

В.Д. Зорькин пишет, что для функционирования государства возникают новые возможности, связанные с использованием цифровых технологий, в целях «защиты основополагающих конституционных ценностей, в том числе таких как фундаментальные права и свободы человека и гражданина (личные, политические и социальные), суверенитет, территориальная целостность и безопасность России»⁴.

Соглашаясь с В.Д. Зорькиным, отметим, что угрозы, которые имеют место в цифровой сфере, напрямую связаны с конституционными ценностями и вызывают необходимость их защиты от деструктивного влияния представителей недружественных государств с использованием современных технологий.

³ Могилевский В.Д. Методология систем: вербальный подход. М.: Экономика, 1999. С. 15.

⁴ Зорькин В.Д. Указ. соч. С. 243.

1. Материалы и методы

К. Маркс – один из первых исследователей, который выдвигал идею о том, что в рамках общественного производства человек вступает в определенные отношения (то есть в производственные отношения)⁵. Рассуждая о том, что совокупность таких отношений составляет экономическую структуру общества, ученый пришел к выводу, в соответствии с которым способ производства материальной жизни обуславливает социальный, политический и духовный процессы жизни вообще. Несмотря на то, что прошло уже почти два века, традиционное разделение сфер жизни (в том числе на сегодняшний день) предполагает экономическую, социальную, политическую и духовную сферы.

Сделаем уточнение. Все сферы общественной жизни являются целостной системой, то есть, согласно воззрениям И. Канта, единством разнообразных знаний, объединенных одной идеей⁶. Из приведенного утверждения следует, что какое-либо изменение в рамках одной из сфер общественной жизни неизбежно влечет за собой изменения в других сферах, так же как, по мысли Н. Макиавелли, всякая перемена прокладывает путь другим переменам⁷, в связи с чем нам представляется возможным систематизировать и далее раскрыть угрозы ценностям России в каждой соответствующей сфере, в том числе используя формально-юридический метод.

Метод контент-анализа и работа с источниками позволили сформировать комплекс материалов (отчеты, аналитические материалы, мнения научно-экспертного сообщества, комментарии должностных лиц и исследования), которые могут быть использованы при изучении соответствующих угроз и обозначении статистических данных. Отметим, что настоящее исследование отличается сбалансированное введение технического и юридического материала, что продиктовано технологическим характером возникновения изучаемых угроз и их реализацией в цифровом пространстве.

2. Результаты и обсуждение

2.1. Экономическая сфера. Согласно ч. 1 ст. 8 Конституции Российской Федерации (КРФ), гарантируются, во-первых, единство экономического пространства; во-вторых, свободное перемещение товаров, услуг и финансовых средств; в-третьих, поддержка конкуренции; в-четвертых, свобода экономической деятельности.

Аналитика зафиксированных инцидентов и угроз в экономической сфере в рамках охраны цифрового суверенитета позволяет обозначить тенденцию роста инструментов, с помощью которых совершаются противоправные деяния; с каждым годом появляются все новые виды таких инструментов: примеру, QR-коды для оплаты несуществующих налогов, использование торговой марки с обещанием оплаты за просмотр рекламы, серые SIM-карты, использование номеров и пин-кодов подарочных сертификатов, анонимные платежные системы, автоматизированные скрипты для нарушения работы сайтов, ZIP-архивы с вредоносными программами для ЭВМ, «зеркала» (копии) пиратских сайтов, вредоносные рассылки, в том числе через Excel-документы, программы-вымогатели и т. д.

Анализ статистики, представленной WAF ГК «Солар», показывает, что количество атак на информационные ресурсы компаний из различных отраслей в 2025 г. выросло на 89 %⁸

⁵ Маркс К. К критике политической экономии. Л.: Госполитиздат, 1949. С. 7.

⁶ Кант И. Критика чистого разума. М.: Чоро, 1994. С. 606.

⁷ Макиавелли Н. Избр. произведения. М.: Худ. лит-ра, 1982. С. 304.

⁸ «Солар»: число веб-атак в 2025 г. на веб-порталы ведущих российских компаний выросло на 89 % // Solar. URL: <https://rt-solar.ru/events/news/6367/>, свободный.

(только за третий квартал 2025 г. – почти на 300 %, по сведениям, представленным WMX⁹). Российские компании часто сталкиваются с утечками данных различного характера, в том числе персональных данных, конфиденциальных данных, данных о секретах производства (ноу-хау) и иных сведений, которые составляют информацию, необходимую для свободы принятия экономических решений. В частности, в ряде случаев речь идет о «формальном» наличии существующих инструментов обеспечения информационной безопасности, которые в ситуации столкновения с вредоносной программой для ЭВМ не способны осуществить защиту цифровой инфраструктуры компании. Ярким примером последствий преступных атак является утечка данных при взломе систем информационной безопасности государственного телекоммуникационного оператора «Ростелеком», в результате которой злоумышленники получили доступ к базам данных клиентов оператора, а часть базы данных была опубликована в качестве доказательства взлома в даркнете (в виде скриншотов таблиц, содержащих 154 тыс. адресов электронной почты и 101 тыс. телефонных номеров)¹⁰.

Из результатов исследования MWS Cloud (входит в MTC Web Services) следует, что 29 % российских компаний не имеют собственного штата специалистов по информационной безопасности, а 42 % компаний сталкиваются с проблемами найма экспертов в этой области¹¹. Согласно исследованию «Киберпротект», «Хабр Карьеры» и АПКИТ, кадровый рынок в обозначенной сфере переживает проблему «доверия», так как большинство кандидатов дополняют свою биографию недостоверными сведениями: неподтвержденными компетенциями (81 %), увеличенным стажем (77 %), фиктивным опытом работы (68 %)¹².

Что касается целевых фишинговых компаний, отметим аналитику IBM¹³, где констатируется, что многие крупные утечки данных начинались с телефонного звонка. Словом, тогда как решения в области безопасности становятся все более модернизированными, а методы обеспечения безопасности более изощренными, хакерам все труднее находить слабые места, которыми можно воспользоваться, поэтому многие злоумышленники переключили свое внимание на более уязвимые цели – людей.

В 2026 г. прогнозируется рост атак на различные инфраструктуры, а также констатируется низкий уровень технологий, направленных на защиту систем квантового распределения ключей [8]. Так, недостаточный уровень регулирования квантовых вычислений и использования квантового компьютера отмечает А.В. Минбалева [9, с. 106].

При этом только опережающее развитие технологий в области цифровых коммуникационных сетей позволит защитить экономические интересы хозяйствующих субъектов, создать для них благоприятную экономическую среду, обеспечить экономическое лидерство государства, то есть не допустить дестабилизацию экономического оборота и нарушение равенства его участников экономического оборота.

⁹ Промышленность столкнулась с кратным ростом веб-атак // WMX. URL: <https://wmx.pro/news/ib-landshaft/promyshlennost-stolknulas-s-kratnym-rostom-vebatak/>, свободный.

¹⁰ Как выкрали данные пользователей у «Ростелекома» // Ведомости. URL: <https://www.vedomosti.ru/technology/articles/2025/01/21/1087478-vikrali-dannie-rosteleкома>, свободный.

¹¹ MWS Cloud: почти треть российских компаний не имеет команды по кибербезопасности // ТАСС. URL: <https://tass.ru/novosti-partnerov/26056115>, свободный.

¹² Итоги исследования по накрутке опыта соискателей // АПКИТ. URL: <https://apkit.ru/news/itogi-issledovaniya-po-nakrutke-opyta-soiskateley/>, свободный.

¹³ Scam (increasingly) likely: What's behind the rise of vishing? // IBM. URL: <https://www.ibm.com/think/insights/rise-of-vishing>, свободный.

2.2. Социальная сфера. Как следует из смысла ст. 2 КРФ, Россия обязана признавать, соблюдать и защищать права и свободы человека и гражданина. Указанная норма права не конкретизирует разновидность прав и свобод, а, наоборот, включает в свое содержание их понимание в широком смысле, то есть гражданские, политические, экономические, социальные, культурные и т. д. При этом к их числу можно уверенно отнести предусмотренное ч. 4 ст. 29 КРФ право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом, которое определяет формы реализации права на информацию и принципы свободы информации [10, с. 66]. Также в их число можно включить право каждого знакомиться с документами и материалами, непосредственно затрагивающими его права и свободы (ч. 2 ст. 24 КРФ) и право на достоверную информацию о состоянии окружающей среды (ст. 42 КРФ), трактуемое Конституционным Судом Российской Федерации в полном соответствии с международными стандартами (ОКСРФ931-0-0), например, в части распространения права на достоверную информацию о состоянии окружающей среды не только на уже функционирующие объекты, но и на проектируемые (ОКСРФ1421-0-0).

Ежедневно человек использует технологии, которые с каждым годом становятся более функциональными по сравнению со своими прошлыми версиями. В то же время чем шире функционал и выше стоимость такой технологии (устройства), тем больше риск, в связи с чем верно полагать, что человек неизбежно сталкивается с различными инструментами, нарушающими его права и свободы. К примеру, технологии дипфейк (в том числе дипфейк-видео, голосовые дипфейки и т. д.), замаскированные веб-страницы (в частности, объявления о продаже автомобиля и др.), замена гиперссылок (на те, что ведут к скачиванию вредоносной программы для ЭВМ), поддельные приложения (клоны), браузерные вирусы, клонирование банковских карт и т. д.

Около 285 млрд руб. удалось похитить мошенникам у россиян в 2025 г., согласно оценке ПАО «Сбербанк России»¹⁴. По результатам исследования «Контур.Эгида», лишь каждый десятый не сталкивался с попытками мошенников завладеть персональными данными, при этом в большинстве случаев уязвимость связана с выбором неудачного способа хранения пароля – 48 % держат их в памяти, 41 % записывают в блокноте, 30 % используют один пароль для всех сервисов, 9 % хранят скриншоты в телефоне и лишь 4 % пользуются менеджерами паролей¹⁵.

Подобное положение дел связано в том числе с недостаточным уровнем цифровой грамотности населения. И.А. Ильин писал, что «технические науки открывают перед человечеством чрезмерные возможности, которые человек не успевает ни продумать, ни подчинить высшим целям своей жизни»¹⁶. Человек прежде всего ввиду незнания базовых технических вещей, а также доверительного отношения к своему устройству как вещи личной (de facto мнимой личной) либо добровольно передает всю информацию посторонним, либо сам создает условия для получения ими необходимых сведений, содержащих в том числе личные, семейные и профессиональные тайны. В свою очередь, в Российской Федерации принима-

¹⁴ Сбербанк оценил объем похищенных мошенниками средств в 2025 г. в 280–285 млрд руб. // Интерфакс. URL: <https://www.interfax.ru/business/1070065>, свободный.

¹⁵ Киберпривычки россиян: хранение паролей, отношений к NDA и использование сервисов // Контур.Эгида. URL: https://kontur.ru/aegis/blog/81894-kiberprivyichki_rossiyan, свободный.

¹⁶ Ильин И.А. Основы борьбы за национальную Россию. Внешние причины русской революции // Ильин И. А. Собрание сочинений. Т. 9-10. М.: Рус. книга, 1999. С. 333.

ются меры, направленные на защиту граждан. Так, в рамках законодательства о защите прав потребителей с 1 сентября 2025 г. стало обязательным предустанавливать российский магазин приложений RuStore на все смартфоны и планшеты, официально продаваемые в России (ЗРФ2300-1). Аналогичный правовой механизм используется для поисковой системы «Яндекс», Rutube и платформы МАХ, выступающей в том числе в качестве сервиса обмена информацией по смыслу Федерального закона от 24 июня 2025 г. № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации» (ФЗ156-ФЗ).

Отставание государства в развитии цифровых технологий не позволяет ему в полной мере исполнять обязанность по защите прав граждан, что уже приводит к различным негативным последствиям, таким как несанкционированный доступ к личным данным, вымогательство денежных средств (в том числе совершение или удержание от совершения каких-либо действий под угрозой распространения информации), отслеживание, преследование, торговля поведенческими продуктами и т. д.

2.3. Политическая сфера. Государственные органы ежедневно используют в своей деятельности цифровые технологии различного характера и уровня сложности. Хакерские атаки на государственные цифровые коммуникационные ресурсы являются проблемой для многих государств. Отметим опыт столкновения с подобными преступными действиями в американском штате Техас, где из-за кибератаки на правительственные системы была отключена часть сетевых ресурсов (в частности, полиция потеряла возможность осуществлять проверку водительских удостоверений и государственных регистрационных знаков)¹⁷. В России аналогичными примерами являются цифровые преступные действия по отношению к государственному аппарату, связанные с продолжительными DDoS-атаками, например, на цифровые ресурсы Роскомнадзора и Министерства обороны Российской Федерации¹⁸, из-за которых стало невозможным получить доступ к официальным ресурсам указанных федеральных ведомств.

В связи с вышеизложенным вопрос о достаточности уровня защищенности информационных ресурсов государственных органов, в том числе о наличии мер, которые в ситуации столкновения с вредоносной программой для ЭВМ способны осуществить защиту их цифровой инфраструктуры, остается открытым. Количество инструментов, с помощью которых реализуются попытки воздействовать на государственную цифровую инфраструктуру, увеличивается с каждым годом, улучшается их качество. К примеру, использование незащищенных каналов в рамках служебной коммуникации (личной электронной почты) позволяют создавать копии приложений государственных органов (клоны), ОТР-боты для кражи кодов 2FA, производить отключение от доменных зон (в том числе международных) и т. д.

К сожалению меры, предпринимаемые государством для защиты цифрового суверенитета, не всегда дают желаемый результат. Такое положение дел, например, послужило основанием для появления прямого правительственного запрета использовать иностранные информационные системы и программы для ЭВМ при предоставлении государственных и муниципальных услуг (ФЗ210), выполнении государственного или муниципального задания (ФЗ584). Кроме того, из проведенной аналитики следует, что свою эффективность доказы-

¹⁷ Texas mayor asks Governor to 'declare a state of emergency' for cyberattack // Gov1. URL: <https://www.gov1.com/technology/texas-mayor-asks-governor-to-declare-a-state-of-emergency-for-cyberattack>, свободный.

¹⁸ Сайты Роскомнадзора и Минобороны подверглись DDoS-атаке // ТАСС. URL: <https://tass.ru/obschestvo/26579501>, свободный.

вают правовые нормы, закрепляющие положения о цифровых платформах. Только Указом Президента Российской Федерации от 31 марта 2023 г. № 231 в части создания и развития государственных информационных систем с использованием платформы «ГосТех» устанавливается ряд правовых инструментов и юридических конструкций, с помощью которых проводится оценка экономической и (или) технологической целесообразности их создания и развития (УПРФ231). Так, в качестве примера правового инструмента приведем «план создания и развития государственных информационных систем на платформе „ГосТех“», а в качестве примера юридической конструкции отметим «соглашение о распределении ответственности между оператором платформы „ГосТех“ с операторами государственных информационных систем», где определяются особенности юридической ответственности за бесперебойное функционирование государственных информационных систем; конфиденциальность и безопасность обрабатываемой в государственных информационных системах информации (включая персональные данные); за сохранение качества предоставления государственных услуг, иных услуг и исполнения государственных функций посредством государственных информационных систем и т. д.

В подобном контексте нельзя игнорировать и закрепление с 1 октября 2026 г. легальной дефиниции «цифровая платформа» в Федеральном законе от 31 июля 2025 г. № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» (ФЗ289-ФЗ), который Конституционный Суд РФ связывает с совершенствованием законодателем правового регулирования (ПКСРФ7-П). Так, в процессе правоприменения под цифровой платформой будет необходимо понимать информационную систему, и (или) сайт в информационно-телекоммуникационной сети «Интернет», и (или) программы для электронных вычислительных машин, обеспечивающие технические, организационные, информационные и иные возможности для взаимодействия неограниченного круга лиц в том числе в целях обмена информацией и ее распространения, продажи товаров, выполнения работ, оказания услуг.

Более того, проведенный правовой анализ положений в области обеспечения технологического лидерства, а именно Федерального закона от 28 декабря 2024 г. № 523-ФЗ «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» (ФЗ523-ФЗ), позволяет отметить концептуальное несоответствие перечня субъектов, осуществляющих формирование технологической политики, и лиц, осуществляющих содействие развитию технологий, традиционной классификации субъектов информационного права, а также регламентацию новых отраслевых принципов [11, с. 87].

Приведенные примеры доказывают, что в Российской Федерации принимается довольно много нормативных правовых актов, которые направлены на защиту отечественных цифровых технологий. Прийти к такому умозаключению кроме прочего помогло создание базы данных «Правовые инструменты обеспечения цифрового суверенитета Российской Федерации»¹⁹.

Что касается угроз, можно констатировать увеличение количества хакерских групп. О системном характере последних свидетельствует анализ, который проведен Kaspersky Cyber Threat Intelligence, где доказывается, что большинство изученных групп тесно взаи-

¹⁹ Свидетельство о государственной регистрации базы данных № 2026620852 Российская Федерация. Правовые инструменты обеспечения цифрового суверенитета Российской Федерации: заявл. 13.02.2026; опубл. 26.02.2026 / А. С. Агафонов.

модействуют друг с другом на примере проукраинских группировок и АРТ-групп, а также отмечается заметный рост числа «политически мотивированных группировок, поведение которых выходит за рамки привычных классификаций»²⁰, что доказывает наличие адаптивности и автономности при выборе тактики атаки.

Деструктивное влияния на цифровую инфраструктуру органов публичной власти влечет за собой следующие риски: ослабление возможности оперативно осуществлять управленческую деятельность, внедрение в аппаратную среду ложных нарративов, порождение у политической и управленческой элиты сомнений в правильности избранного политического и экономического курса.

2.4. Духовная сфера. Преамбула КРФ несет мощный идеологический заряд (ЗКСРФ1-3), воплощаемый в конституционных нормах, что подтвердили поправки к КРФ, внесенные в 2020 году (ЗРФОПКРФ1-ФКЗ). Ее идеологические постулаты содержат универсальные нравственные критерии, позволяющие оказывать влияние на законотворчество, правоприменение, формирование моральных устоев у граждан Российской Федерации.

Уважение к историческому прошлому народа (проявляющееся в передаче предыдущими поколениями любви и уважения к Отечеству, то есть патриотизма), вера в добро и справедливость являются началами и исходными идеями российского конституционализма.

Соглашаясь с А.С. Домченко и О.В. Соболевым, отметим, что право «в первую очередь реализует функцию нормативного закрепления (фиксации)» ценностей, где главная роль отдана КРФ²¹, которая, по утверждению А.Н. Кокотова, предстает не только в качестве правового акта, но также и в качестве культурно-нравственного и политико-идеологического регулятора [12, с. 15].

Так, конституционная реформа, проведенная в 2020 г., в рамках совершенствования регулирования отдельных вопросов организации и функционирования публичной власти носила помимо прочего культурологический смысл [13], что, как верно утверждают М.С. Саликов и М.В. Гончаров, потребует серьезных усилий в целях «определения наиболее сбалансированного и эффективного механизма охраны» [14, с. 66]. Стремление к сбалансированному механизму и господство всевозможных балансов, по утверждению К. Шмитта²², характерно для областей духовной жизни начиная с XVI в. Г.А. Гаджиев указывает, что на идее гармонии строили свою философию Пифагор, Сократ (гармония принципов счастья, пользы, добродетели, долга, подчинения божественной воле), Г. Лейбниц (принцип предустановленной гармонии)²³. Гармоническому равновесию придавал особое значение и В.С. Соловьев²⁴.

Отсутствие подобного сбалансированного механизма ставит государство перед серьезным аксиологическим выбором. Так, например, по подсчетам Г.А. Гаджиева две трети решений Конституционного Суда Российской Федерации связаны с необходимостью делать

²⁰ Аналитический отчет: записки цифрового ревизора: три кластера угроз в киберпространстве // Kaspersky. URL: <https://www.kaspersky.ru/enterprise-security/threat-intelligence>, свободный.

²¹ Домченко А.С., Соболев О.В. Традиционные ценности в контексте правового регулирования // Перспективы продвижения российской модели мировоззренческих ценностей в зарубежной социокультурной среде в условиях информационной безопасности. Екатеринбург: УрГЮУ им. В.Ф. Яковлева, 2024. С. 148.

²² Шмитт К. Политическая теология: сб. М.: КАНОН-пресс-Ц, 2000. С. 194.

²³ Гаджиев Г.А. Онтология права (критическое исследование юридического концепта действительности. М.: Норма: ИНФРА-М, 2021. С. 201.

²⁴ Соловьев В.С. Критика отвлеченных начал. М.: Директ-Медиа, 2012. С. 24.

выбор, «какому же праву, после взвешивания, отдать предпочтение и может ли законодатель, уважая какой-то публичный интерес, ради этого ограничить права человека?» [15, с. 55].

Обозначенный ранее культурологический смысл проявляется в ст. 67.1., ч. 1 ст. 68, ч. 4 ст. 68, ч. 2 и 3 ст. 69, п. «ж1» ст. 72, расширяющих ценностное содержание КРФ²⁵.

В свою очередь, духовная сфера российского общества строится на следующих нравственных началах: уважение к историческому прошлому народа; вера в добро и справедливость; государственное единство; историческая правда; приоритет семейного воспитания; создание условий для развития детей; русский язык – язык государствообразующего народа; культура России – уникальное наследие ее народов; культурная самобытность всех народов и этнических общностей; Российская Федерация – правопреемник (правопродолжатель) Союза ССР; защита семьи, материнства, отцовства и детства; защита института брака как союза мужчины и женщины; создание условий для достойного воспитания детей в семье и осуществления совершеннолетними детьми обязанности заботиться о родителях; жизнь; достоинство; права и свободы человека; гражданственность; служение Отечеству и ответственность за его судьбу; высокие нравственные идеалы; крепкая семья; приоритет духовного над материальным; милосердие; справедливость; созидательный труд; гуманизм; коллективизм; взаимопомощь и взаимоуважение; социально-культурные факторы (культурный суверенитет России). Вышеперечисленное прямо следует из системного анализа положений Указа Президента Российской Федерации от 9 ноября 2022 г. № 809 (УПРФ809), Указа Президента Российской Федерации от 24 декабря 2014 г. № 808 (УПРФ808) и КРФ.

Применительно к духовной сфере аналогичным образом наблюдается рост инструментов, с помощью которых осуществляются попытки воздействия на указанные нравственные начала. К ним можно отнести проникновение в незащищенные каналы для коммуникации (электронные почты, социальные сети), создание дезинформационных каналов с целью распространения ложной исторической информации (в том числе о вкладе России в мировую историю и культуру), каналов для пропаганды (нетрадиционных сексуальных отношений, гендерной идентичности и пр.), замаскированные веб-страницы (в частности, содержащие информацию для детей, причиняющую вред их здоровью и развитию) и т. д.

Современный человек использует цифровую среду для поиска информации, необходимой ему для профессиональной деятельности, личностного развития, однако она далеко не всегда бывает достоверной и объективной.

Дополнительным технологическим инструментом познания для человека стали языковые чат-боты, дезинформирующий характер которых доказан в исследовании Европейского вещательного союза при поддержке BBC, где было отмечено, что более 50 % ответов ChatGPT (от OpenAI), Copilot (от Microsoft), Gemini (от Google) и Perplexity (от Perplexity AI) оказались не соответствующими действительности (искажали факты, допускали неточности, вводили в заблуждение)²⁶. Иными словами, появляется источник недостоверной информации, генерируемой искусственным интеллектом, что чревато не только внедрением

²⁵ Хабриева Т.Я., Клишас А.А. Тематический комментарий к Закону Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти». М.: Норма: ИНФРА-М, 2022. С. 34.

²⁶ AI chatbots distort and mislead when asked about current affairs, BBC finds // The Guardian. URL: <https://www.theguardian.com/technology/2025/feb/11/ai-chatbots-distort-and-mislead-when-asked-about-current-affairs-bbc-finds>, свободный.

в сознание человека ложных данных, но и появлением фантома недоверия в том числе к официальным источникам информации.

И.А. Ильин писал, что государство по своей идее есть живая система всеобщего доверия. Оно может жить при минимальном уровне взаимного доверия (общественного и политического) и заживо разлагается при крайнем максимуме его отсутствия²⁷. Размерами доверия определяется «большая или меньшая степень устанавливающейся близости между общающимися»²⁸.

Процесс получения знаний с помощью современных языковых чат-ботов, связанных с аббревиатурой GPT, привел по крайней мере к двум проблемным проявлениям, подтверждающим кризис доверия.

Первое проявление носит субъект-объектный характер и связано с тем, что человек в ряде случаев не подвергает критическому анализу сведения, получаемые из определенного источника, и доверяет ему [16]. Второе проявление гораздо серьезнее, носит субъект-субъектный характер и заключается в том, что человек перестает доверять человеку [17; 18]. Еще И.А. Ильин писал, что подобного рода недуги «зарождаются незаметно, таятся в оттенках и развиваются постепенно», когда утверждал, что «жить среди людей, не вызывающих к себе доверия, есть всегда несчастье». «Взаимное недоверие, – указывал он, – есть сила, разрушающая правопорядок и государство»²⁹.

Отсутствие возможности защитить вышеназванные нравственные начала может привести к насаждению чуждой российскому народу и разрушительной для российского общества системы идей и ценностей (деструктивной идеологии), включающей культивирование безнравственности, отрицание идеалов патриотизма, разрушение традиционной семьи, подрыв культурного суверенитета Российской Федерации.

Заключение

Изучение угроз по отношению к ценностям России в контексте охраны цифрового суверенитета, а также научно-экспертных подходов к обозначенной проблеме позволило нам прийти к следующим выводам.

Во-первых, сущностные элементы цифрового суверенитета можно и нужно рассматривать с точки зрения двух коннотаций – позитивной (выражена в положительном влиянии цифровых технологий) и негативной (связана с их отрицательным влиянием).

Во-вторых, несмотря на то, что Российская Федерация принимает ряд мер для защиты цифрового суверенитета (в том числе рассмотренных в настоящем исследовании), вопрос об их достаточности остается открытым и дискуссионным. Угрозы, которые возникают в контексте цифрового суверенитета, напрямую связаны с конституционными ценностями, защита которых является одной из важнейших обязанностей государства. Реализация обозначенных угроз приводит:

- 1) к дестабилизации экономического оборота и нарушению равенства его участников (экономическая сфера);
- 2) к несанкционированному доступу к личным данным граждан России, изъятию их денежных средств, а также отслеживанию, преследованию, торговле поведенческими продуктами (социальная сфера);

²⁷ Ильин И.А. Теория права и государства. М.: Зерцало, 2008. С. 521.

²⁸ Ильин И.А. Философия как духовное делание. М.: Изд-во ПСТГУ, 2013. С. 626.

²⁹ Ильин И.А. Собрание сочинений: В 10 т. Т. 4. М.: Русская книга, 1994. С. 382.

3) дестабилизации деятельности органов государственной власти, возможности влияния на настроения политической элиты, созданию условий для формирования деструктивных формирований, целью которых является нарушение целостности России (политическая сфера);

4) насаждению чуждой российскому народу и разрушительной для российского общества системы идей и ценностей, включающей культивирование безнравственности, отрицание идеалов патриотизма, разрушение традиционной семьи, подрыв культурного суверенитета Российской Федерации (духовная сфера).

В-третьих, закладывается основа для кризиса всеобщего доверия, который выражается в двух проблемных проявлениях:

1) первое носит субъект-объектный характер, поскольку связано с тем, что человек в ряде случаев не подвергает критическому анализу получаемые с помощью современных цифровых технологий сведения и доверяет им;

2) второе проявление носит субъект-субъектный характер и заключается в том, что человек перестает доверять человеку.

В то же время следует отметить, что в целях недопущения реализации соответствующих угроз в Российской Федерации принимается довольно много нормативных правовых актов, которые направлены на защиту отечественных цифровых технологий, среди которых цифровые платформы, информационные системы (в том числе государственные), программы для ЭВМ и т. д. Подобный вывод сделан по результатам создания базы данных «Правовые инструменты обеспечения цифрового суверенитета Российской Федерации».

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Conflicts of Interest. The author declares no conflicts of interest.

Источники

УПРФ309 – Указ Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собр. законодательства РФ. 2024. № 20. Ст. 2584.

КоАП РФ – Кодекс Российской Федерации об административных правонарушениях от 30 дек. 2001 г. № 195-ФЗ // СЗ РФ. 2002. № 1 (ч. I). Ст. 1.

КРФ – Конституция Российской Федерации (принята всенародным голосованием 12 дек. 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru/constitution/>, свободный.

ОКСРФ931-0-0 – Определение Конституционного Суда Российской Федерации от 15 июля 2010 г. № 931-0-0 «По жалобе гражданки Андроновой Ольги Олеговны на нарушение ее конституционных прав положениями статей 39 и 40 Градостроительного кодекса РФ, статьи 13 Закона Санкт-Петербурга „О градостроительной деятельности в Санкт-Петербурге“, статей 7 и 8 Закона Санкт-Петербурга „О порядке организации и проведения публичных слушаний и информирования населения при осуществлении градостроительной деятельности в Санкт-Петербурге“» // Вестн. Конституционного Суда РФ. 2011. № 2.

ОКСРФ1421-0-0 – Определение Конституционного Суда Российской Федерации от 30 сент. 2010 г. №1421-0-0 «Об отказе в принятии к рассмотрению жалобы граждан Кулаковой Натальи Анатольевны и Лисицыной Наталии Александровны на нарушение их конституционных прав статьей 11 Федерального закона „Об экологической экспертизе“» // Вестн. Конституционного Суда РФ. 2011. № 2.

ЗРФ2300-1 – Закон РФ от 7 февр. 1992 г. № 2300-1 «О защите прав потребителей» // СЗ РФ. 1996. № 3. Ст. 140.

- ФЗ156-ФЗ – Федеральный закон от 24 июня 2025 г. № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru/document/0001202506240021>, свободный.
- ФЗ210 – Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. 2010. № 31. Ст. 4179.
- ФЗ584 – Федеральный закон от 29 дек. 2022 г. № 584-ФЗ «О внесении изменений в Федеральный закон „Об информации, информационных технологиях и о защите информации“» // СЗ РФ. 2023. № 1 (ч. I). Ст. 31.
- УПРФЗ231 – Указ Президента Российской Федерации от 31 мар. 2023 г. № 231 «О создании, развитии и эксплуатации государственных информационных систем с использованием единой цифровой платформы Российской Федерации „ГосТех“» // СЗ РФ. 2023. № 14. Ст. 2407.
- ФЗ289-ФЗ – Федеральный закон от 31 июля 2025 г. № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» // СЗ РФ. 2025. № 31. Ст. 4643.
- ПКСРФ7-П – Постановление Конституционного Суда Российской Федерации от 17 февр. 2026 г. № 7-П «По делу о проверке конституционности пунктов 3 и 4 статьи 26.1 Закона Российской Федерации „О защите прав потребителей“ в связи с жалобой гражданина Тишкина Петра Николаевича» // СЗ РФ. 2026. № 8. Ст. 990.
- ФЗ523-ФЗ – Федеральный закон от 28 дек. 2024 г. № 523-ФЗ «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2024. № 53 (ч. I). Ст. 8533.
- ЗКСРФ1-3 – Заключение Конституционного Суда Российской Федерации от 16 мар. 2020 г. № 1-3 // СЗ РФ. 2020. № 12. Ст. 1855.
- ЗРФОПКСРФ1-ФКЗ – Закон Российской Федерации о поправке к Конституции РФ от 14 мар. 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти» // СЗ РФ. 2020. № 11. Ст. 1416.
- УПРФЗ809 – Указ Президента Российской Федерации от 9 нояб. 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2022. № 46. Ст. 7977.
- УПРФЗ808 – Указ Президента Российской Федерации от 24 дек. 2014 г. № 808 «Об утверждении Основ государственной культурной политики» // СЗ РФ. 2014. № 52 (ч. I). Ст. 7753.

Литература

1. Полякова Т.А., Троян Н.А. Стратегические задачи обеспечения технологического и цифрового суверенитета: правовые аспекты формирования новой информационной среды // Правовая информатика. 2025. № 1. С. 70–78. <https://doi.org/10.24412/1994-1404-2025-1-70-78>.
2. Агафонов А.С. Место цифрового суверенитета в системе информационного права // Электронное приложение к Российскому юридическому журналу. 2024. № 2. С. 14–18. https://doi.org/10.34076/22196838_2024_2_14.
3. Степанов П.В. Подходы к пониманию цифрового суверенитета России // Журн. рос. права. 2024. Т. 28, № 4. С. 37–51. <https://doi.org/10.61205/jrp.2024.4.1>.
4. Тихомиров Ю.А. Креативные регуляторы в правовом и виртуальном пространстве // Журн. рос. права. 2023. Т. 27. № 3. С. 5–16. <https://doi.org/10.12737/jrp.2023.025>.
5. Кузнецов П.У. Конституционные понятия информационной сферы как ценности методологического порядка // Рос. право: образование, практика, наука. 2017. № 6 (102). С. 29–37.
6. Степин В.С. Цивилизация в эпоху перемен: поиск новых стратегий развития // Журн. Белорус. гос. ун-та. Социология. 2017. № 3. С. 6–11.
7. Полякова Т.А., Троян Н.А. Обеспечение суверенитета в информационном пространстве – стратегическая задача национальной политики // Правовая политика и правовая жизнь. 2024. № 1. С. 41–53. <https://doi.org/10.24412/1608-8794-2024-1-41-53>.

8. Sushchev I., Bugai K., Molotkov S., Bulavkin D., Sidelnikova A., Melkonian D., Vakhrusheva V., Lokhmatov R., Dvoretzkiy D. Realistic vulnerabilities of decoy-state quantum key distribution // *Scientific Reports*. 2025. V. 15, No 1. Art. 44820. <https://doi.org/10.1038/s41598-025-29144-6>.
9. Минбалеев А.В. Основные направления регулирования квантовых технологий // *Вестн. Ун-та им. О.Е. Кутафина (МГЮА)*. 2024. № 10 (122). С. 100–107. <https://doi.org/10.17803/2311-5998.2024.122.10.100-107>.
10. Талапина Э.В. Право на информацию в практике Конституционного Суда Российской Федерации // *Труды Ин-та гос-ва и права РАН*. 2011. № 6. С. 66–82.
11. Агафонов А.С. Правовое регулирование технологической политики в Российской Федерации: трансформация регуляторных подходов в контексте информационного права и цифрового суверенитета // *Рос. право: образование, практика, наука*. 2025. № 4 (148). С. 87–93. <https://doi.org/10.34076/2410-2709-2025-148-4-87-93>.
12. Кокотов А.Н. Конституция России и идеология // *Актуальные проблемы российского права*. 2023. Т. 18, № 12 (157). С. 11–23. <https://doi.org/10.17803/1994-1471.2023.157.12.011-023>.
13. Осинцев Д.В. Культурный код российской Конституции // *Конституционное и муниципальное право*. 2022. № 4. С. 6–10. <https://doi.org/10.18572/1812-3767-2022-4-6-10>.
14. Саликов М.С., Гончаров М.В. Конституционные ценности на новом этапе развития основного закона Российской Федерации // *Herald of the Euro-Asian Law Congress*. 2020. № 1. С. 60–68. <https://doi.org/10.34076/2619-0672-2020-4-1-60-68>.
15. Гаджиев Г.А. Конституция России: двадцать пять лет спустя: конвертация ожиданий и надежд в опыт // *Юрид. вестн. ДГУ*. 2018. Т. 28, № 4. С. 53–59. <https://doi.org/10.21779/2224-0241-2018-28-4-53-59>.
16. Spitale G., Biller-Andorno N., Germani F. AI model GPT-3 (dis)informs us better than humans // *Science Advances*. 2023. V. 9, No 26. Art. eadh1850. <https://doi.org/10.1126/sciadv.adh1850>.
17. Logg J.M., Minson J.A., Moore D.A. Algorithm appreciation: People prefer algorithmic to human judgment // *Organizational Behavior and Human Decision Processes*. 2019. V. 151. P. 90–103. <https://doi.org/10.1016/j.obhdp.2018.12.005>.
18. Bogert E., Schechter A., Watson R.T. Humans rely more on algorithms than social influence as a task becomes more difficult // *Scientific Reports*. 2021. V. 11, No 1. Art. 8028. <https://doi.org/10.1038/s41598-021-87480-9>.

References

1. Polyakova T.A., Troyan N.A. Strategic objectives for ensuring technological and digital sovereignty: Legal aspects of building a new information environment. *Pravovaya Informatika*, 2025, no. 1, pp. 70–78. <https://doi.org/10.24412/1994-1404-2025-1-70-78>. (In Russian)
2. Agafonov A.S. The place of digital sovereignty in the system of information law. *Elektronnoe Prilozhenie k Rossiiskomu Yuridicheskomu Zhurnalu*, 2024, no. 2, pp. 14–18. https://doi.org/10.34076/22196838_2024_2_14. (In Russian)
3. Stepanov P.V. Approaches to understanding Russia's digital sovereignty. *Journal of Russian Law*, 2024, vol. 28, no. 4, pp. 37–51. <https://doi.org/10.61205/jrp.2024.4.1>. (In Russian)
4. Tikhomirov Yu.A. Creative regulators in the legal and virtual Space. *Journal of Russian Law*, 2023, vol. 27, no. 3, pp. 5–16. <https://doi.org/10.12737/jrp.2023.025>. (In Russian)
5. Kuznetsov P.U. Constitutional concepts of the information sphere as methodological values. *Russian Law: Education, Practice, Research*, 2017, no. 6 (102), pp. 29–37. (In Russian)
6. Stepin V.S. Civilization in the age of change: the search for new development strategies. *Journal of the Belarusian State University. Sociology*, 2017, no. 3, pp. 6–11. (In Russian)
7. Polyakova T.A., Troyan N.A. Ensuring sovereignty in the information space – a strategic objective of national policy. *Pravovaya Politika i Pravovaya Zhizn'*, 2024, no. 1, pp. 41–53. <https://doi.org/10.24412/1608-8794-2024-1-41-53>. (In Russian)

8. Sushchev I., Bugai K., Molotkov S., Bulavkin D., Sidelnikova A., Melkonian D., Vakhrusheva V., Lokhmatov R., Dvoretzkiy D. Realistic vulnerabilities of decoy-state quantum key distribution. *Scientific Reports*, 2025, vol. 15, no. 1, art. 44820. <https://doi.org/10.1038/s41598-025-29144-6>.
9. Minbaleev A.V. The main directions of regulation of quantum technologies. *Courier of Kutafin Moscow State Law University*, 2024, no. 10 (122), pp. 100–107. <https://doi.org/10.17803/2311-5998.2024.122.10.100-107>. (In Russian)
10. Talapina E.V. The right to information from the perspective of the Constitutional Court of the Russian Federation. *Proceedings of the Institute of State and Law of the RAS*, 2011, no. 6, pp. 66–82. (In Russian)
11. Agafonov A.S. Legal regulation of technology policy in the Russian Federation: Transformation of regulatory approaches in the context of information law and digital sovereignty. *Russian Law: Education, Practice, Research*, 2025, no. 4 (148), pp. 87–93. <https://doi.org/10.34076/2410-2709-2025-148-4-87-93>. (In Russian)
12. Kokotov A.N. The Constitution of Russia and ideology. *Actual Problems of Russian Law*, 2023, vol. 18, no. 12 (157), pp. 11–23. <https://doi.org/10.17803/1994-1471.2023.157.12.011-023>. (In Russian)
13. Osintsev D.V. The cultural code of the Russian Constitution. *Constitutional and Municipal Law*, 2022, no. 4, pp. 6–10. <https://doi.org/10.18572/1812-3767-2022-4-6-10>. (In Russian)
14. Salikov M.S., Goncharov M.V. Constitutional values at the new stage of development of the fundamental law of the Russian Federation. *Herald of the Euro-Asian Law Congress*, 2020, no. 1, pp. 60–68. <https://doi.org/10.34076/2619-0672-2020-4-1-60-68>. (In Russian)
15. Gadzhiev G.A. The Constitution of Russia: Twenty-five years later: From expectations and hopes to experience. *Yuridicheskii Vestnik DGU*, 2018, vol. 28, no. 4, pp. 53–59. <https://doi.org/10.21779/2224-0241-2018-28-4-53-59>. (In Russian)
16. Spitale G., Biller-Andorno N., Germani F. AI model GPT-3 (dis)informs us better than humans. *Science Advances*, 2023, vol. 9, no. 26, art. eadh1850. <https://doi.org/10.1126/sciadv.adh1850>.
17. Logg J.M., Minson J.A., Moore D.A. Algorithm appreciation: People prefer algorithmic to human judgment. *Organizational Behavior and Human Decision Processes*, 2019, vol. 151, pp. 90–103. <https://doi.org/10.1016/j.obhdp.2018.12.005>.
18. Bogert E., Schechter A., Watson R.T. Humans rely more on algorithms than social influence as a task becomes more difficult. *Scientific Reports*, 2021, vol. 11, no. 1, art. 8028. <https://doi.org/10.1038/s41598-021-87480-9>.

Информация об авторе

Андрей Сергеевич Агафонов, аспирант кафедры информационного права, Уральский государственный юридический университет им. В.Ф. Яковлева

E-mail: aga.fonov@inbox.ru

ORCID: <https://orcid.org/0009-0005-2888-7955>

Author Information

Andrey S. Agafonov, Postgraduate Student, Department of Information Law, Ural State Law University named after V.F. Yakovlev

E-mail: aga.fonov@inbox.ru

ORCID: <https://orcid.org/0009-0005-2888-7955>

Поступила в редакцию 19.03.2026

Поступила после рецензирования 24.06.2026

Принята к публикации 26.06.2026

Received March 19, 2026

Revised June 24, 2026

Accepted June 26, 2026