ПРИНЦИП ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ТЕОРЕТИКО-ПРАВОВЫЕ АСПЕКТЫ

Дубень А.К.[1]

Ключевые слова: *цифровизация, информационные технологии, трансформация права, информационное право, вызовы и угрозы, информационная безопасность, принципы права, теория права, философия права.*

Аннотация

Цель работы *состоит в анализе современных и актуальных проблем правового обеспечения информационной безопасности на национальном и международном уровнях. Обоснование теоретических положений, направленных на определение места и роли принципа достоверности информации как важного элемента по противодействию новых угроз и рисков в системе информационного и международного права.*

Методами исследования *стали следующие общенаучные методы: анализа и синтеза, абстрагирования и моделирования, обобщения, описания, классификации и др. Использовались специальные частноправовые методы познания: сравнительно-правовой, формально-юридический и др.*

Результаты исследования: *в условиях развития информационного общества возрастает роль исследований, рассматривающих принципы правового регулирования общественных отношений на примере отдельной подотрасли права как информационная безопасность. Обоснована необходимость законодательного закрепления принципа достоверности информации в международных нормативно-правовых актах в сфере обеспечения информационной безопасности, а также необходимо выработать подходы к формированию единых стандартов и требований к безопасности в информационной среде, которые позволят определять состояние защищенности информационной инфраструктуры и противодействие распространению недостоверной информации. Констатируя отсутствия специального стратегического регулирования по данному вопросу, важно обратить внимание на принцип достоверности как важного элемента по противодействию новых угроз и рисков. При этом обеспечение достоверности информации следует рассматривать как составную часть состояния защищенности государства, ее информационные ресурсы и технологии. Следовательно, информационная сфера, на сегодняшний день, неизбежно способствует дестабилизации общества и манипулированию общественным и индивидуальным сознанием. Учитывая пребывание информационного пространства в непрерывном состоянии неопределенности и опасности, а также информационный характер любых рисков, для обеспечения информационной безопасности нужен надлежащий государственный механизм, который обеспечит постоянное и бесперебойное противодействие информационным угрозам в современных условиях социально-экономических и геополитических рисков при фундаментальной трансформации мира.*

DOI: 10.24412/1994-1404-2026-3-00-28

Введение

Развитие информационных технологий сопровождается возникновением новых вызовов, угроз и рисков как практического, так и правового характера, в этой связи одной из задач государства является формирование комплексного правового регулирования, способствующего одновременно технологическому развитию общества, а также обеспечению защиты прав граждан. Сегодня в условиях цифровой трансформации цифровые технологии воздействуют на все сферы социальных и экономических отношений, поэтому технологическая революция меняет привычные парадигмы, заставляя искать решения проблем, с которыми человечество еще никогда не сталкивалось [1, с. 164]. В соответствии со стратегическими нормативно-правовыми актами, одной из угроз государства является использование информационно-коммуникационных технологий для вмеша-

[1] ***Дубень Андрей Кириллович****, кандидат юридических наук, старший научный сотрудник Института государства и права Российской академии наук, г. Москва, Россия.*

E-mail: k.duben@mail.ru

тельства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, а также распространение недостоверной информации, в том числе заведомо ложных сообщений, где основным объектом такого деструктивного воздействия является молодежь.

В этой связи, как справедливо отмечает академик РАН А.Н. Савенков в своих фундаментальных работах, российское государство-цивилизация переживает в своей истории многие события, которые оказывают влияние на внутреннее национальное развитие и определяет пути мировой истории на многие десятилетия, сегодня как никогда остро стоит вопрос о том, чтобы концептуально разработать собранные воедино черты русской цивилизации, охватывающей более чем тысячелетний период истории, ее место в мировых процессах, характер взаимоотношений с другими странами и регионами [2, с. 8]. Таким образом, трансформация права и ее последующая цифровизация, имеет как позитивные, так и негативные аспекты, в частности, новые вызовы и угрозы приводят к деструктивному воздействию, а устоявшиеся правовые конструкции, порождают пробелы и коллизии в законодательстве. Следует обратить внимание, что цифровая трансформация представляет собой «комплексный процесс, который связан с радикальными изменениями в бизнес-процессах, культуре организации, организационной структуре, взаимодействии с партнерами и потребителями, инфраструктуре»[2]. Из этого следует, что наиболее активное воздействие цифровая трансформация оказывает на современное информационное право, что отражается на развитии информационных правоотношений и выделении в рамках них цифровых правоотношений, а также развитии его доктрины [3].

Очевидно, стоит констатировать, что современные цифровые технологии, сочетая в себе конвергентность, сквозной и прорывной характер для развития общества и государства, не только создают безграничные возможности, но и формируют новые вызовы и угрозы безопасности в процессе их внедрения и использования. Считаем, что рассматриваемые проблемы в праве свидетельствуют о том, что внедрение и развитие информационных технологий в определенной части порождают новые угрозы, которые еще более усилились в условиях геополитических изменений, следовательно, информационное общество и цифровизация права, во многом определили позиции информационного права как отдельного направления в отечественной юриспруденции, так и ведущей отрасли права, которая динамично и активно развивается в условиях формирования экономики данных, укреплению цифрового суверенитета и формированию независимой правовой инфраструктуры, обеспечивающей устойчивость национальной информационной среды.

Постановка задачи

В доктрине информационного права не раз акцентировалось внимание на том, что стратегический характер имеют задачи обеспечения государственного суверенитета в условиях цифровой трансформации; обеспечения безопасности в киберпространстве [4]. Вместе с тем особую значимость придается данной теме в философии права, теории и истории государства и права, А.Н. Савенков отмечает, что «в условиях… усиливающейся динамики развития информационного общества, «электронного государства», цифровой экономики, роста вызовов и угроз информационной безопасности особую роль играет формирование и реализация государственной политики, направленной на учет современных информационных тенденций развития всех сфер жизни общества и государства, выработку научно обоснованных, выверенных, взвешенных подходов регулирования новых информационных отношений» [5, с. 64].

Согласно анализу и обобщению положений Доктрины информационной безопасности Российской Федерации можно констатировать, что к современным угрозам информационной безопасности можно отнести противоправное создание монополий на формирование и распространение достоверной информации, включая создание условий для масштабного манипулирования информацией, дискриминации. Как подтверждение этому, одной из задач обеспечения информационной безопасности является формирование безопасной среды оборота достоверной информации, повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования, а также развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз[3]. Ряд указанных выше информационных угроз в последнее время приобрел особую значимость. Так, угроза создания монополий на формирование и распространение достоверной информации заключается в противоправной фильтрации информации для формирования враждебного по отношении к России информационно-коммуникационного пространства, которое впоследствии влияет на конкурентоспособность и безопасность государства в инновационной и информационной сфере. Современная повестка дня международной информационной безопасности

[2] Цифровая трансформация. Основные принципы, этапы и результаты реализации. URL: https://roskachestvo.gov.ru/ about/ competence/digital/docs/standart.pdf (дата обращения: 20.08.2026).

[3] П. 57 Указа Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

позволяет констатировать, что в отношении России ведется тотальная информационная и гибридная война, включая санкционную агрессию. В связи с этим можно утверждать, что при глобальной цифровой трансформации информация как непосредственный объект правоотношений перешла из разряда ресурсов в разряд средств враждебной деятельности. В связи с этим особое значение приобретает принцип достоверности информации как основа доверия между государствами.

Общепризнанные принципы международного права в исследуемой сфере деятельности нашли отражение и в резолюциях ООН, посвященных проблемам информационной безопасности и научно-техническому прогрессу[4]. Большинство принципов, закрепленных в международно-правовых документах, согласуются с документами стратегического планирования зарубежных государств и подчеркивают важность открытости и транспарентности деятельности государства в информационном пространстве, а также необходимости формирования глобальной культуры информационной безопасности. Рассматривая международно-правовые принципы, следует обратить внимание на принципы, закрепленные в Окинавской хартии глобального информационного общества, включая развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций[5]. Дальнейшее развитие принципов получило отражение в Декларации принципов (2003 г.), включая принцип укрепления доверия и безопасности при использовании цифровых технологий[6]. Из этого следует, что задекларированные принципы влияют на развитие правовых основ государства для цифровой доверительной среды, включая защиту информационно-технологических сетей и противодействие киберугрозам и киберпреступности. Как справедливо отмечает Т.А. Полякова, принципы права, обеспечивающие безопасность в информационной сфере на международном уровне, имеют устойчивый характер, однако необходима структурированная система данных принципов для эффективной реализации норм международного права в данной сфере[7].

Решение поставленной задачи

Можем констатировать, что обеспечение достоверности информации можно рассматривать как составную часть состояния защищенности государства, ее информационные ресурсы и технологии. При этом ряд авторов рассматривает требование по обеспечению достоверности информации как составную часть наряду с конфиденциальностью при обеспечении информационной безопасности, в частности, видный ученый, доктор юридических наук Г.Г. Камалова делает вывод «…предоставление доверителем сведений, составляющих профессиональную тайну, обусловлено наличием доверия личного характера или связанного с особым профессиональным статусом субъекта профессиональной деятельности, что всегда предполагает, что обе стороны правоотношений в сфере профессиональной тайны рассчитывают на достоверность получаемой и сохраняемой информации» [6, с. 284]. Как отмечает О.В. Петровская, для обеспечения эффективного управления достоверность информации можно рассматривать как неотъемлемое условие и меру соблюдения конфиденциальности информации ограниченного доступа [7, с. 143]. В доктрине информационного права констатируется, что актуальность информации определяется ее постоянным обновлением, так называемой актуализацией состояния [8]. В этой связи справедливо ставится вопрос о том, что развитие принципа достоверности требует дополнительных исследований для совершенствования отечественного законодательства, в т. ч. по вопросам государственной тайны, персональных данных, кредитных историй и т. д. [9]. В этой связи полагаем возможным дополнительно закрепить принцип достоверности для обеспечения и проведения экспертизы в целях обеспечения информационной безопасности. В находящейся в процессе постоянной трансформации системе на многие социальные институты влияет постоянно усиливающийся информационный поток, новые способы и особенности сбора и обработки данных, а также отсутствие быстрой адаптивности к происходящим изменениям [10].

Следовательно, обеспечение достоверности информации прямо вытекает из требования обеспечения конфиденциальности сведений, относящихся к государственной тайне, в которых достоверность, рассматривается через категории точности, достаточности и актуальности информации. Следует отметить, важность принципа достоверности при правовом обеспечении информационной безопасности, т.к. он выступает базовым условием для реализации общественных отношений в сфере информационных технологий и обеспечения безопасности.

Из этого следует, что формирование и закрепление единых международных принципов и норм позволит реализовать в Стратегии национальной безопасности Российской Федерации принципы всеобщей, равной и неделимой безопасности, а также отдельные прин-

---

[4] Например, Резолюция 2450 (XXIII) Генеральной Ассамблеи ООН от 19 декабря 1968 г. «Права человека и научно-технический прогресс» // Официальный сайт ООН. URL: https://undocs.org/ru/A/RES/2450%28XXIII%29 (дата обращения: 28.08.2026).

[5] Окинавская хартия глобального информационного общества (принята на о. Окинава 22 июля 2000 г.) // Дипломатический вестник. 2000. № 8. С. 51—56.

[6] Женевская Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии», принятая 12 декабря 2003 г. // Официальный сайт ООН. URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения: 26.08.2026).

[7] Полякова Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3. С. 17.

ципы, к примеру, исследуемый принцип достоверности, согласно которым безопасность отдельного независимого государства самостоятельна, тем самым другое государство не имеет право прямо или косвенно вмешиваться во внутренние или внешние дела, что актуально в сфере обеспечения международной информационной безопасности. Тем самым, обусловленность правовых принципов обеспечения информационной безопасности системой принципов информационного права и законодательства, которые закономерно привлекали внимание исследователей, отмечавших их дальнейшее развитие в связи с изменениями сферы регулируемых общественных отношений и трансформацией права в условиях цифровизации [11].

Таким образом, в условиях цифровизации усиливается зависимость эффективности правовой политики от информационных рисков. В связи с этим Г. Бехманн отмечает характерную для информационного общества фундаментальную дихотомию между стремлением к устойчивому развитию и ростом риска [12]. Российские ученые сходятся во мнении, что вопросы информационной безопасности являются столь же важными, как вопросы ядерной сферы и это делает их ключевым фактором стратегической стабильности государства [13, с. 135]. Следовательно, информационная сфера, на сегодняшний день, неизбежно способствует дестабилизации общества и манипулированию общественным и индивидуальным сознанием. Учитывая пребывание информационного пространства в непрерывном состоянии неопределенности и опасности, а также информационный характер любых рисков, для обеспечения информационной безопасности нужен надлежащий государственный механизм, который обеспечит постоянное и бесперебойное противодействие информационным угрозам в современных условиях социально-экономических и геополитических рисков при фундаментальной трансформации мира.

Считаем, что одной из задач в области обеспечения международной информационной безопасности является развитие обеспечения достоверности с позиции защиты от распространения ложной и недостоверной информации как масштабной и серьезной информационной угрозы не только на национальном (внутригосударственном), но и на международном уровне, в этой связи необходимо принять универсальный документ, закрепляющий в качестве одной из таких основных угроз распространение недостоверной информации, которая приводит к дестабилизации международного мира, безопасности и стабильности. Данные попытки уже осуществлялись, в частности, в Концепции Конвенции ООН об обеспечении международной информационной безопасности, в числе угроз и факторов информационной безопасности были указаны: публичное распространение под видом достоверных сообщений заведомо ложной информации, приводящее к возникновению угрозы жизни и безопасности граждан или к наступлению тяжких последствий; невозможность точной идентификации источника компьютерных атак или ложной информации, обусловленная технологическими особенностями информационно-коммуникационных технологий, а также отсутствием организационных механизмов обеспечения деанонимизации информационного пространства[8]. Однако в 2024 году была принята Конвенция ООН против киберпреступности, укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, в данном нормативно-правовом акте вышеуказанные угрозы отсутствуют и принцип достоверности не закреплен в качестве универсального положения, который бы определял содержание и направленность правового регулирования общественных отношений, тем самым, отсутствие четкого закрепления принципа достоверности порождает правовые неопределенности в сфере правового обеспечения информационной безопасности и повышает риски распространения недостоверной информации в цифровой среде.

Как справедливо отмечает А.В. Крутских, Россия исторически выступает как государство, которое стремится объединить и укрепить международное сотрудничество в сфере информационной безопасности, в том числе путем выработки правил, норм, принципов ответственного поведения государств, сегодня важно придать нормам об ответственном поведении в киберсреде обязательный характер, поскольку угрозы в информационной среде носят глобальный характер, поэтому поиск решения проблем должен носить универсальный характер[9].

Юридическое сообщество в лице доктрины информационного и международного права, законодателя и других субъектов права с законодательной инициативой должны выработать подходы к формированию единых стандартов и требований к безопасности в информационной среде, которые, в свою очередь, должны определять состояние защищенности информационной инфраструктуры и противодействие распространению недостоверной информации.

[8] Обновленная Концепция Конвенции ООН об обеспечении международной информационной безопасности // Официальный сайт Совета Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (дата обращения: 26.08.2026).

[9] Крутских А.В. Геополитические аспекты глобального использования ИКТ // Инфофорум. URL: https://infoforum.live/ (дата обращения: 30.08.2026).

Выводы

Таким образом, анализ современного состояния правового обеспечения информационной безопасности свидетельствует о том, что отсутствия универсальных международных нормативно-правовых актов, закрепляющий принципы обеспечения кибербезопасности, не позволяет в полной мере развивать правовые средства обеспечения безопасности в информационной среде. Констатируя отсутствия специального стратегического регулирования по данному вопросу, важно обратить внимание на принцип достоверности как важного элемента по противодействию новых угроз и рисков, поскольку достоверность информации выступает как особое требование в целях обеспечения информационной безопасности, так как одним из условий обеспечения безопасности в информационной среде является гарантия достоверности, в том числе целостности и точности информации.

Литература

1. Троян Н.А. О некоторых вопросах применения искусственного интеллекта в государственном управлении в условиях цифровой трансформации: правовые аспекты // Правовая информатика. 2026. № 2. С. 164—171.
2. Савенков А.Н. Российское государство-цивилизация и его беспримерный подвиг в обеспечении мира и безопасности человечества: к 80-летию Победы в Великой Отечественной войне // Государство и право. 2025. № 5. С. 7—15.
3. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75—87.
4. Polyakova T.A., Naumov V.B., Minbaleev A.V. Trust in the law during the digital transformation // Государство и право. 2022. № 11. С. 139—147.
5. Савенков А.Н. Философия права и становление российского государства-цивилизации. М., 2024. 739 с.
6. Камалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: дис. … д-ра юрид. наук. М. : Институт государства и права РАН, 2020. 472 с.
7. Петровская О.В. Принцип достоверности в информационном праве: дис. … к-та юрид. наук. М. : Институт государства и права РАН, 2022. 204 с.
8. Полякова Т.А., Камалова Г.Г. Концептуальные основания развития института доступа к информации в Российской Федерации при применении цифровых технологий // Мониторинг правоприменения. 2020. № 4 (37). С. 22—27.
9. Полякова Т.А. Влияние цифровой трансформации на развитие информационного права: тенденции, проблемы, перспективы // Мониторинг правоприменения. 2020. № 2 (35). С. 53—58.
10. Петровская О.В. Цифровая трансформация и проблемы обеспечения достоверности информации // Аграрное и земельное право. 2020. № 3 (183). С. 130—132.
11. Чубукова С.Г. Внутриотраслевые принципы обработки генетической информации // Актуальные проблемы российского права. 2019. № 5 (102). С. 98—110.
12. Букалерова Л.А., Лапшин В.Ф., Остроушко А.В. Риск-ориентированный подход в области правового регулирования обеспечения информационной безопасности несовершеннолетних // Вестник Сургутского государственного университета. 2021. № 1 (31). С. 76—83.
13. Савенков А.Н. Государство и право в период кризиса современной цивилизации. М., 2020. 448 с.

SECTION:
REGULATORY INFORMATICS

THE PRINCIPLE OF INFORMATION RELIABILITY IN THE FIELD OF INFORMATION SECURITY: THEORETICAL AND LEGAL ASPECTS

Duben A.K.[10]

[10] ***Andrei K. Duben***, *Ph.D. (Law), Senior Researcher at the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia. E-mail: k.duben@mail.ru*

Keywords: *digitalization, information technologies, transformation of law, information law, challenges and threats, information security, principles of law, theory of law, philosophy of law.*

Abstract

The aim of the work *is to analyse modern and pressing issues related to the legal provision of information security at the national and international levels. Justification of theoretical provisions aimed at determining the place and role of the principle of information reliability as an important element in countering new threats and risks in the system of information and international law.*

The following general scientific methods: *analysis and synthesis, abstraction and modelling, generalization, description, classification, etc. Special private-law methods of cognition were also used: comparative legal, formal-legal, etc.*

The results of the study. *In the context of the development of the information society, the role of research examining the principles of legal regulation of social relations — using information security as an example of a specific sub-branch of law — is growing. The necessity of legally enshrining the principle of information reliability in international regulatory legal acts in the field of ensuring information security is substantiated; it is also necessary to develop approaches to forming unified standards and requirements for security in the information environment, which will make it possible to determine the state of protection of information infrastructure and counteract the spread of unreliable information. Noting the absence of special strategic regulation on this issue, it is important to pay attention to the principle of reliability as an important element in countering new threats and risks. At the same time, ensuring the reliability of information should be considered an integral part of the state's security status, along with its information resources and technologies. Consequently, the information sphere today inevitably contributes to the destabilization of society and the manipulation of public and individual consciousness. Given that the information space is in a continuous state of uncertainty and danger, as well as the informational nature of any risks, ensuring information security requires an appropriate state mechanism that will provide continuous and uninterrupted counteraction to information threats in the current context of socio-economic and geopolitical risks amid the fundamental transformation of the world.*

References

1. Troian N.A. O nekotorykh voprosakh primeneniia iskusstvennogo intellekta v gosudarstvennom upravlenii v usloviiakh tsifrovoi transformatsii: pravovye aspekty // Pravovaia informatika. 2026. No. 2. S. 164—171.
2. Savenkov A.N. Rossiiskoe gosudarstvo-tsivilizatsiia i ego besprimernyi podvig v obespechenii mira i bezopasnosti chelovechestva: k 80-letiiu Pobedy v Velikoi Otechestvennoi voine // Gosudarstvo i pravo. 2025. No. 5. S. 7—15.
3. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Novye vektory razvitiia informatsionnogo prava v usloviiakh tsivilizatsionnogo krizisa i tsifrovoi transformatsii // Gosudarstvo i pravo. 2020. No. 5. S. 75—87.
4. Polyakova T.A., Naumov V.B., Minbaleev A.V. Trust in the law during the digital transformation // Gosudarstvo i pravo. 2022. No. 11. S. 139—147.
5. Savenkov A.N. Filosofiia prava i stanovlenie rossiiskogo gosudarstva-tsivilizatsii. M., 2024. 739 c.
6. Kamalova G.G. Pravovoe obespechenie konfidentsial'nosti informatsii v usloviiakh razvitiia informatsionnogo obshchestva: dis. … d-ra iurid. nauk. M. : Institut gosudarstva i prava RAN, 2020. 472 s.
7. Petrovskaia O.V. Printsip dostovernosti v informatsionnom prave: dis. … k-ta iurid. nauk. M. : Institut gosudarstva i prava RAN, 2022. 204 s.
8. Poliakova T.A., Kamalova G.G. Kontseptual'nye osnovaniia razvitiia instituta dostupa k informatsii v Rossiiskoi Federatsii pri primenenii tsifrovykh tekhnologii // Monitoring pravoprimeneniia. 2020. No. 4 (37). S. 22—27.
9. Poliakova T.A. Vliianie tsifrovoi transformatsii na razvitie informatsionnogo prava: tendentsii, problemy, perspektivy // Monitoring pravoprimeneniia. 2020. No. 2 (35). S. 53—58.
10. Petrovskaia O.V. Tsifrovaia transformatsiia i problemy obespecheniia dostovernosti informatsii // Agrarnoe i zemel'noe pravo. 2020. No. 3 (183). S. 130—132.
11. Chubukova S.G. Vnutriotraslevye printsipy obrabotki geneticheskoi informatsii // Aktual'nye problemy rossiiskogo prava. 2019. No. 5 (102). S. 98—110.
12. Bukalerova L.A., Lapshin V.F., Ostroushko A.V. Risk-orientirovannyi podkhod v oblasti pravovogo regulirovaniia obespecheniia informatsionnoi bezopasnosti nesovershennoletnikh // Vestnik Surgutskogo gosudarstvennogo universiteta. 2021. No. 1 (31). S. 76—83.
13. Savenkov A.N. Gosudarstvo i pravo v period krizisa sovremennoi tsivilizatsii. M., 2020. 448 s.