Вопросы безопасности
Правильная ссылка на статью:
Дубень А.К. — Новые вызовы и угрозы в цифровом пространстве: безопасность как критерий развития информационных технологий // Вопросы безопасности. – 2023. – № 3. DOI: 10.25136/2409-7543.2023.3.44062 EDN: YEGPER URL: https://nbpublish.com/library_read_article.php?id=44062

Новые вызовы и угрозы в цифровом пространстве: безопасность как критерий развития информационных технологий

Дубень Андрей Кириллович

научный сотрудник Института государства и права Российской академии наук

119019, Россия, Москва область, г. Москва, ул. Знаменка, 10

k.duben@mail.ru

Статья из рубрики "Стратегия обеспечения национальной безопасности"

DOI:

10.25136/2409-7543.2023.3.44062

EDN:

YEGPER

Дата направления статьи в редакцию:

18-09-2023

Дата публикации:

29-09-2023

Аннотация: Объектом данного исследования являются общественные отношения, связанные с обеспечением информационной безопасности в Российской Федерации в условиях новых вызовов и угроз, а также цифровой трансформации и геополитических изменений. Предмет исследования образует совокупность правовых норм нормативных правовых актов Российской Федерации, регулирующих общественные отношения в сфере обеспечения информационной безопасности, а также положения теоретических междисциплинарных исследований в указанной сфере. Особое внимание уделяется вопросам безопасности, которые занимают одно из ключевых значений во внутренней и внешней политики государства, определяющие в дальнейшем национальные интересы и стратегические национальные приоритеты, цели и задачи государственной политики и устойчивого развития государства на долгосрочную перспективу. Все более актуальной становится вопросы обеспечения информационной безопасности ввиду глобальной цифровой трансформации всех сфер жизнедеятельности, а также обострившиеся

геополитических противоречий и усиления межгосударственного информационного противоборства. Автор делает вывод, что очевидна целесообразность законодательного закрепления на федеральном уровне правовых основ национальной системы обеспечения информационной безопасности в Российской Федерации в целях применения информационно-правовых средств в условиях цифровизации, роста геополитических вызовов и рисков, мирового социально-экономического кризиса, формирования многополярности мира, направленных на повышение защищенности российских информационных ресурсов, информационных систем и объектов информационной инфраструктуры. Автор ставит перед читателями вопрос о возможности включения отдельных правовых норм в отечественное информационное законодательство в той части, в какой такими нормами урегулированы отношения в области исполнения органами публичного управления функций, обеспечивающих безопасность в информационной сфере.

Ключевые слова:

безопасность, информационная безопасность, трансформация, цифровизация, информационное пространство, вызовы, угрозы, риски, стратегические акты, национальная безопасность

Вопросы безопасности занимают одно из ключевых значений во внутренней и внешней политике государства, определяющие национальные интересы и стратегические национальные приоритеты, основные направления устойчивого развития государства на долгосрочную перспективу. Все более актуальной становятся вопросы обеспечения информационной безопасности ввиду глобальной цифровой трансформации всех сфер жизнедеятельности, а также обострившиеся геополитических противоречий и усиления межгосударственного информационного противоборства [1]. Обращает внимание, что каждое государство преимущественно заботится о собственном национальном информационном суверенитете, включая цифровой и технологический аспекты [2, с. 120]. Существенным фактором развития национальной политики государства выступает информационная составляющая. Для подтверждения данной позиции можно привести слова В.Н. Лопатина, которыйв диссертационном исследовании отмечал, что роль информационной безопасности и ее место в системе национальной безопасности формируется государственной информационной политикой, которая взаимосвязана с государственной политикой обеспечения национальной безопасности государства посредством системы информационной безопасности [3, с. 85].

В рамках данной статьи предметом исследования составляют нормы права, регламентирующие общественные отношения в области правового обеспечения информационной безопасности. Методологической основой данной работы является применение диалектического и системного подходов, позволивших всесторонне исследовать поставленные научные и практические проблемы в их развитии и взаимосвязи.

Стратегическое значение информационной безопасности подтверждается целым рядом документов федерального уровня, утвержденных Указом Президента Российской Федерации от 2 июля 2021 года № 400 «О Стратегии национальной безопасности Российской Федерации», имеющих базовое значение на современном этапе развития общества и государства. Эти документы являются основными в системе документов

стратегического планирования, требуют научного осмысления с позиции информационного права, поскольку сегодня в эпоху активных процессов цифровой трансформации, общемирового кризиса, связанного еще и с проблемами, обусловленными пандемией COVID-19 и геополитическим рисками, остро ощутимо их влияние и на систему права, как международного, так и национального [4, с. 131]. Президентом Российской Федерации В.В. Путиным на одном из открытых заседаний консультационно-совещательных органов по вопросам информационной безопасности особо подчеркнуто: «Новые технологические решения порождают новые риски. Мы видим, что глобальное цифровое пространство нередко становится площадкой для жесткого информационного противоборства, для нечестной конкуренции и кибератак <… > Важно сохранить преемственность нашего стратегического курса на предотвращение конфликтов в информационном пространстве» [5]. В условиях нарастающей напряженности между Россией и ее зарубежными политическими противниками подобная констатация со стороны Президента РФ представляется особенно важной, так как, на наш взгляд, содержит призыв к органам публичной власти и обществу на эффективное противодействие агрессивной деятельности иностранных государств, противоречащей стратегическому курсу Российской Федерации.

В настоящее время в связи с событиями в мире и возможностью удаленного информационного воздействия на правосознание и миропонимание людей значительно актуализировался вопрос безопасности в информационной сфере. В частности, обеспечение достоверности информации как основы осуществления деятельности в информационной сфере и формирования системы правомерных действий различных лиц. Однако, как справедливо отметила О.В. Петровская, основным способом недопущения недостоверной информации является установление критериев достоверности информации, которые позволят противодействовать данному процессу в информационной среде. Вместе с тем фейковые новости получают свое дальнейшее развитие при новых мировых процессах, влияющих на сферу жизнедеятельности человека и общества в целом [6, с. 18]. Так, сегодня наблюдается использование разнообразных механизмов неправомерного ограничения доступа граждан к социально значимой информации, в том числе в системе официальных взглядов в Российской Федерации на особенности национальных интересов и порядка их обеспечения. Широкое распространение получила так называемая фейковая информация, продвигаемая недружественными зарубежными государствами, использующими свое цифровое и технологическое преимущество в собственных интересах в ущерб национальным интересам Российской Федерации. Это усиливает значение формирования правовых механизмов информационно-аналитической деятельности для развенчания недостоверной информации, распространяемой в целях неправомерного достижения преимуществ одних стран над другими, а также противодействия указанным процессам.

Считаем, что в целях реализации государственной политики в информационной сфере необходимо определить предметную область российского законодательства и выстроить целостную систему в области обеспечения безопасности. Полагаем, что основными направлениями реализации государственной информационной политики являются: гарантия и реализация конституционных прав человека и гражданина; безопасность информационных сетей; недопущение уязвимости информационных систем; развитие и совершенствование информационной инфраструктуры; дальнейшее межгосударственное сотрудничество по вопросам информационной безопасности и защиты информации.

В настоящее время все более актуальной становится проблема концентрации центров контроля цифровых технологий и разнообразных цифровых платформ организациями,

действующими под юрисдикцией западных государств. В связи с этим одним из острых вопросов сегодня является формирование правовых механизмов международного и межгосударственного контроля за развитием информационно-коммуникационной сети Интернет и цифровых платформ, имеющих важное международное значение в контексте обеспечения мира и правопорядка, также обеспечения национальной информационной безопасности. Таким образом, государственная информационная политика должна строиться на общих принципах права в целях развития и совершенствования информационных технологий, защиты информации и обеспечением информационной безопасности, которые поспособствуют дальнейшему развитию информационного общества внутри государства.

Современные цифровые технологии, имея трансграничное использование, сейчас нередко базируются на программном и программно-аппаратном комплексе производства зарубежных государств, хотя порой в основе они имеют теоретические исследования и опытно-конструкторские разработки российских ученых. Вместе с тем недостаточная практика внедрения результатов научных исследований в информационные продукты оказывает негативное влияние на продуктивность внедрения научно-исследовательских и опытно-констукторских достижений российских исследователей и практиков. Это требует необходимость формирования комплекса организационно-правовых мер в области разработки, внедрения и коммерциализации информационных продуктов отечественного происхождения посредством продвижения их на российском, региональном и мировом рынке, финансирования перспективных проектов.

Важное значение для сферы обеспечения информационной безопасности имеет подготовка компетентных кадров, включая как специалистов в сфере собственно информационных технологий (программистов, тестировщиков, системных администраторов и др.), так и специалистов по защите информации различных профилей и специализаций. Следует отметить, что кадровая подготовка на уровне бакалавриата, специалитета и магистратуры, имея комплексный характер, вместе с тем требует совершенствования, включая учебно-методические материалы, направленные на формирование не только инженерно-технических, компьютерных, но и правовых знаний и правовой культуры. Однако, как правило, подготовка квалифицированных кадров в сфере обеспечения информационной безопасности осуществляется техническими вузами, которые не имеют необходимого профессорско-преподавательского состава в области права. Это ставит задачу закрепления требований к правовым знаниям выпускников на уровне подзаконных актов и федеральных образовательных стандартов.

Важное значение имеет также формирование условий для развития инновационных технологий на базе государственно-частного партнерства, которое в сфере обеспечения информационной безопасности России определяется заинтересованностью сторон в активном развитии национальной информационной инфраструктуры на базе соглашений в рамках действующего российского законодательства. На данный момент, одним из направлений развития государственно-частного партнерства в России является взаимодействие государства и частных субъектов в сфере обеспечения информационной безопасности посредством передачи информации, ведения баз данных, информационного обеспечения систем, защиты критической информационной инфраструктуры и т.д. Считаем, что инструменты данного вида соглашений позволяют эффективно задействовать частный сектор в реализации государственной политики в области обеспечения информационной безопасности.

В рамках положений Доктрины информационной безопасности Российской Федерации, взаимодействие публичных и частных субъектов допустимо в случаях оценки состояния

информационной безопасности, прогнозирование и обнаружение угроз в информационной сфере, координация действий по совершенствованию информационной безопасности, т.е. при реализации риск-ориентированного подхода [7, с. 39]. В этой связи политологи справедливо отмечают, что развитие информационных и телекоммуникационных технологий привело к появлению новых терминов, таких как «информационное оружие» и «информационная война», которые требуют научного осмысления с учетом современной геополитической обстановки, характеризующейся усилением информационных рисков и угроз, в том числе в сфере обеспечения цифрового и технологического суверенитета государства, его конституционного строя и обороны, при этом исследователи неоднократно обращали внимание на возникновение новых видов информационного оружия, которые созданы для противоправных действий внутри отдельных информационных систем [8, с. 141].

Таким образом, государственно-частное партнерство в России формируется на этапе своего развития, основной целью которого является удовлетворение общественно значимых интересов в области обеспечения информационной безопасности. При этом разнообразные формы партнерства обеспечивают эффективные решения приоритетных целей и задач обеспечения национальной безопасности в информационном пространстве.

Сегодня в сфере организационно-правового обеспечения информационной безопасности остро стоит вопрос развития системы технического регулирования. Правовое регулирование и правоприменительная практика в области сертификации, стандартизации средств защиты информации, а также лицензирования, аттестации в деятельности по обеспечению информационной безопасности требует научного осмысления с позиции информационного права и определения места в системе указанной отрасли. Нормативно-правовое регулирование перечисленных вопросов не всегда соответствует требованиям времени. Так, постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» было издано в период действия утратившего силу Закона Российской Федерации «О сертификации продукции и услуг» 1993 г. Кроме того, положения вышеуказанного постановления Правительства Российской Федерации направлены на регулирование отношений, связанных с подтверждением соответствия требованиям, предъявляемым в основном к средствам защиты государственной тайны. Институционально правовое обеспечение информационной безопасности формируется и развивается «на стыке» отраслей информационной сферы и сферы обеспечения безопасности. Следует согласиться с О.С. Макаровым, который отмечает, что «правовое обеспечение информационной безопасности концептуально надстраивается на уже существующие системы информационных правоотношений (базовые системы) и обеспечивает безопасность их поступательного развития» [9, с. 73].

В настоящее время требования об обязательной сертификации средств защиты информации установлены в отношении информационных систем персональных данных, автоматизированной обработки служебной информации ограниченного распространения и иных видов информации ограниченного доступа. В связи с этим требования по сертификации средств защиты конфиденциальной информации применяются во многом формально и без учета специфики различных видов информации ограниченного доступа. Из вышеизложенного можно сделать вывод о том, что назрела необходимость законодательного изменения правовых норм в области обеспечения информационной безопасности посредством формирования единых подходов к организационным и правовым мерам по обеспечению защищенности информационных систем и ресурсов в

условиях геополитических изменений и новых вызовов, угроз в информационной среде. Данные меры должны способствовать противодействию общественно опасных деяний, устранению кибератак и недопущению информационно-психологического воздействия на здоровье и поведение человека.

В науке информационного права отмечено значение Доктрины информационной безопасности Российской Федерации как документа стратегического планирования в рассматриваемой сфере, имеющего структурированное содержание и четкую форму [10, с. 43]. Данный нормативный правовой акт создает организационно-правовую основу для эффективного обеспечения информационной безопасности в государстве, защищенность национальных интересов России и личных интересов граждан в информационной сфере [11, с. 243]. Вместе с тем следует признать, что меняющиеся социально-экономические, геополитические и иные условия осуществления процессов защиты информации требуют принятия для сферы обеспечения информационной безопасности нового акта стратегического планирования.

Для развития российского законодательства в области информационной безопасности необходимо разработка и принятие специального федерального закона об информационной безопасности [12, с. 115]. Хотя в настоящее время действует определенная система нормативных правовых актов, отдельные нормы которых регламентируют правоотношения в области обеспечения информационной безопасности. В частности, к таким нормативным правовым актам можно отнести федеральные законы: «О безопасности критической информационной инфраструктуры Российской Федерации», «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» и ряд иных. В этой связи, полагаем, назрела необходимость в принятии специального федерального закона об информационной безопасности с учетом государственной политики в информационном пространстве, национальных интересов, включая особенности системы органов государственной власти, обладающих полномочиями в данной сфере.

Следовательно, развитие действующего российского законодательства в области информационной безопасности необходимо для повышения эффективности государственного управления и взаимодействия между различными органами государственной власти Российской Федерации. В связи с этим возрастает значение системного решения вопросов, связанных с приоритетом безопасности учитывая приоритетность вопросов безопасности цифровых технологий [13, с. 34]. Вместе с тем присутствуют обоснованные предпосылки к данным законодательным изменениям. В этой связи стоит вопрос о возможности включения отдельных правовых норм в отечественное информационное законодательство в той части, в какой такими нормами урегулированы отношения в области исполнения органами публичного управления функций, обеспечивающих безопасность в информационной сфере.

Таким образом, в рамках данной статьи можно сделать вывод о том, что назрела необходимость законодательного закрепления на федеральном уровне правовых основ национальной системы обеспечения информационной безопасности в Российской Федерации в целях применения информационно-правовых средств в условиях цифровизации, роста геополитических вызовов и рисков, мирового социально-экономического кризиса, формирования многополярности мира, направленных на повышение защищенности российских информационных ресурсов, информационных

систем и объектов информационной инфраструктуры.

Библиография

1. Механизмы и модели регулирования цифровых технологий. М.: Проспект, 2023. 264 с.
2. Цифровая трансформация: вызовы праву и векторы научных исследований: Монография / Под общ. ред. А.Н. Савенкова; отв. ред. Т.А. Полякова, А.В. Минбалеев. М., 2021. 340 с.
3. Лопатин В.Н. Информационная безопасность России: Дисс. … д-ра юрид. наук: 12.00.01. СПб., 2000. 433 с.
4. Полякова Т.А., Минбалеев А.В., Троян Н.А. Формирование культуры информационной безопасности граждан российской федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С. 131-144.
5. Заседание Совета Безопасности // Сайт Президента РФ. Новости, выступления и стенограммы. 26 марта 2021 г. URL.: http://www.kremlin.ru/events/president/news/65231 (дата обращения: 18.09.2023).
6. Петровская О.В. Критерии достоверности информации по российскому законодательству // Информационное право. 2020. № 2. С. 17-19.
7. Осипенко А.Л. Государственно-частное партнерство в сфере противодействия киберпреступности // Вестник Воронежского института МВД России. 2016. № 4. С. 37-44.
8. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции. Дисс. … д-ра полит. наук. М., 2019. 361 с.
9. Макаров О.С. Правовое обеспечение информационной безопасности на примере защиты государственных секретов государств – участников Содружества Независимых Государств: Дисс. ... д-ра юрид. наук. М., 2013. 444 с.
10. Марков А.А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник СПбГУ. 2011. Сер. 12. Вып. 1. С. 43–48.
11. Козырева А.А., Тарасов Д.А. Современное состояние государственной политики в сфере информационной безопасности // Вестник Воронежского института МВД России. 2018. № 4. С. 243–247.
12. Чубукова С.Г. Субъекты информационных отношений в цифровой среде и их правовой статус. В книге: Право цифровой среды. Монография. Под ред.: Т.П. Подшивалова, Е.В. Титовой, Е.А. Громовой. М.: Проспект, 2022. С. 113-121.
13. Полякова Т.А., Камалова Г.Г. Проблемы формирования правовой политики в сфере применения технологии искусственного интеллекта // Правовая политика и правовая жизнь. 2023. № 1. С. 28-36.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Представленная на экспертизу научная статья «Новые вызовы и угрозы в цифровом пространстве: безопасность как критерий развития информационных технологий» посвящена актуальной проблеме современного развития науки информационного права

с учетом современных геополитических рисков в международном информационном пространстве, необходимости совершенствования механизмов правовой защиты от информационных угроз, фейковой информации и т.д.

Авторами справедливо подчеркивается активизация удаленного информационного воздействия на правосознание и правопонимание людей, неправомерное ограничение доступа граждан к социально значимой информации, в том числе, в системе официальных взглядов в Российской Федерации на особенности национальных интересов и порядка их обеспечения.

Авторами проанализированы ряд документов стратегического и доктринального характера, действующее информационное законодательство. Представлены ряд предложений, включая, предложение по разработке федерального закона об информационной безопасности. Предложена структура государственной информационной политики, поставлены задачи правового образования в системе подготовки кадров в сфере информационной безопасности .

Детально рассмотрены вопросы государственно-частного партнерства в сфере информационной безопасности.

Сделан вывод о необходимости законодательного изменения правовых норм в области обеспечения информационной безопасности посредством формирования единых подходов к организационным и правовым мерам по обеспечению защищенности информационных систем и ресурсов в условиях геополитических изменений и новых вызовов, угроз в информационной среде.

Таким образом, можно сделать вывод о предложенной авторами научной новизне и научных результатах. В самом тексте статьи прослеживается постановка цели исследования и ее задачи, несмотря на отсутствие специально выделенного в ней методологического раздела. По сути, статья содержит междисциплинарный компонент, т.к. автор оперирует понятием «государственная информационная политика». Очевидно, что позиции исследователей науки информационного права могли бы быть существенно дополнены позициями представителей научного сообщества смежных наук, например, политических. Считаем, что данное обстоятельство значительно усилило бы представленную научную работу.

В этой связи, обращаем внимание на то, что список использованных источников и литературы в рецензируемой работе выглядит предельно скромным. В свою очередь, это обстоятельство отразилось на отсутствии научной дискуссии в научной статье или ее элементов.

Статья, с одной стороны, носит аналитический характер. С другой стороны, в основном авторами высказываются общие, авторские позиции, предложения и выводы.

Статья не структурирована. Также следует обратить внимание на необходимость более тщательной вычитки текста статьи.

С учётом вышесказанного, считаем, что рецензируемая статья обладает всеми структурно-содержательными компонентами научной статьи и может быть опубликована в журнале, рецензируемом ВАК РФ с учётом реализации предложенных рекомендаций.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования. В качестве предмета исследования рецензируемой статья являются "нормы права, регламентирующие общественные отношения в области правового обеспечения информационной безопасности".

Методология исследования. Как утверждает автор рецензируемой статьи, "методологической основой данной работы является применение диалектического и системного подходов, позволивших всесторонне исследовать поставленные научные и практические проблемы в их развитии и взаимосвязи". В действительности автором применялись многие современные методы научного познания, что позволило провести анализ действующих правовых норм в сфере обеспечения информационной безопасности и сделать ряд самостоятельных выводов, заслуживающих внимания специалистов в области информационного права.

Актуальность исследования. Важность и значимость темы исследования не вызывает сомнения, поскольку вопросы информационной безопасности и ее правовое обеспечение "занимают одно из ключевых значений во внутренней и внешней политике государства, определяющие национальные интересы и стратегические национальные приоритеты, основные направления устойчивого развития государства на долгосрочную перспективу". В качестве аргументации своей позиции по актуальности темы автор рецензируемой статьи приводит "слова В.Н. Лопатина, который в диссертационном исследовании отмечал, что роль информационной безопасности и ее место в системе национальной безопасности формируется государственной информационной политикой, которая взаимосвязана с государственной политикой обеспечения национальной безопасности государства посредством системы информационной безопасности", который писал об этом еще в 2000 году (почти четверть века назад!). Вопросы информационной безопасности остаются нерешенными, что связывается с постоянным развитием информационных технологий. Глобальная цифровизация всех сфер жизнедеятельности человека, по-прежнему, ставит на разрешение проблемы обеспечения информационной безопасности в качестве приоритетных.

Научная новизна. Пожалуй, нельзя сказать, что автор рецензируемой статьи впервые в науке информационного права обратился к проблемам правового обеспечения информационной безопасности. Однако постановка проблемы и предложенное автором ее решение имеет некоторые элементы научной новизны (например, предложение о принятии специального закона или предложение " о возможности включения отдельных правовых норм в отечественное информационное законодательство в той части, в какой такими нормами урегулированы отношения в области исполнения органами публичного управления функций, обеспечивающих безопасность в информационной сфере").

Стиль, структура, содержание. В целом статья написана научным стилем с применением специальной терминологии. Однако статья не лишена стилистических ошибок и недостатков, нарушения грамматических форм и синтаксических конструкций (например, отмечается несогласованность падежей в предложении: "В рамках данной статьи предметом исследования составляют нормы права, регламентирующие общественные отношения в области правового обеспечения информационной безопасности"; отсутствие запятых в предложениях и проч.). Статья должна быть тщательно вычитана автором. Логически статья структурирована, хотя формально на части не разделена. По содержанию тема, заявленная автором, раскрыта. В качестве замечания хотелось отметить, что заключение по статье носит общий (неконкретный) характер, что умаляет ценность проведенного автором исследования. В качестве пожелания автору предлагается сделать более конкретные выводы по проведенному им исследованию. Кроме того, следует вычитать статью и устранить стилистические ошибки (повторы слов в предложении и словосочетаний в соседних предложениях (например, "назрела необходимость", несогласованность падежей и т.д.).

Библиография. Можно отметить, что автором использовано достаточное количество источников по теме статьи, включая публикации последних лет. Автором изучены работы авторитетных ученых в области информационного права (Т.А. Поляковой, А.В.

Минбалеева, Т.А. Троян, О.В. Петровской и др.). Все ссылки на библиографические источники оформлены правильно, в соответствии с требованиями.

Апелляция к оппонентам. В статье представлены разные точки зрения по спорным вопросам темы. Обращения к оппонентам корректное. Все заимствования оформлены ссылками на источник опубликования.

Выводы, интерес читательской аудитории. Статья "Новые вызовы и угрозы в цифровом пространстве: безопасность как критерий развития информационных технологий" рекомендуется к опубликованию, поскольку в целом подготовлена в соответствии с требованиями к научным работам такого рода, является актуальной, имеет практическую значимость и содержит элементы научной новизны. Данная научная работа может представлять интерес для специалистов в области информационного права, а также для преподавателей и обучающихся юридических вузов и факультетов.