Вопросы безопасности
Правильная ссылка на статью:
Дубень А.К. — Приоритетные задачи обеспечения информационной безопасности в условиях современных вызовов и угроз // Вопросы безопасности. – 2023. – № 2. DOI: 10.25136/2409-7543.2023.2.43435 EDN: JWOTFN URL: https://nbpublish.com/library_read_article.php?id=43435

Приоритетные задачи обеспечения информационной безопасности в условиях современных вызовов и угроз

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 "Информационное обеспечение национальной безопасности"

DOI:

10.25136/2409-7543.2023.2.43435

EDN:

JWOTFN

Дата направления статьи в редакцию:

25-06-2023

Дата публикации:

03-07-2023

Аннотация: В статье рассматриваются вопросы обеспечения информационной, цифровой, кибербезопасности, являющейся актуальной, стратегической задачей как на национальном, так и международном уровне. Установлено, что в современных условиях мирового кризиса и геополитических изменений необходимы новые подходы к правовому регулированию информационной безопасности. Выявлена актуальная проблема не только национального, но и международного уровня. В связи с этим требует выявление новых внешних и внутренних угроз в информационной сфере, а также изучение и прогнозирование перспектив развития международного регулирования информационной безопасности. Проведенное исследование позволило сделать вывод о том, что в условиях цифровой трансформации необходимо проработать и укрепить научно-правовые позиции относительно развития правового обеспечения информационной безопасности. В процессе исследования автор сделал вывод, что на современном этапе развития общества и государства среди наиболее актуальных угроз национальной информационной безопасности ввиду динамичности информационной

сферы, можно выделить такие угрозы, как противоправное воздействие на национальные информационные ресурсы, информационно-телекоммуникационные системы и информационную инфраструктуру, включая критически важные информационные структуры; использование средств и методов распространения недостоверной (фейковой) информации в целях дезинформации неопределенного круга людей с использованием противоправных методов и средств, включая когнитивные методы воздействия на психику человека в целях дезорганизации и подавления воли; несанкционированное вмешательство в национальное информационное пространство.

Ключевые слова:

безопасность, информационная безопасность, подотрасль права, новые вызовы, трансформация права, цифровизация, национальная безопасность, правовое регулирование, правовое обеспечение, цифровая эпоха

Информация, являющаяся одним из главных экономических и политических ресурсов, расширяет круг различных способов ее использования в образовательных, социальных, экономических и культурных целях, обеспечения законности и правопорядка, в иных общественно значимых целях.

Предмет исследования образует совокупность норм нормативных правовых актов Российской Федерации, регулирующих общественные отношения в сфере обеспечения информационной безопасности, а также положения теоретических междисциплинарных исследований в указанной сфере. Проблемы правового обеспечения информационной безопасности Российской Федерации в условиях новых вызовов и угроз наиболее глубоко разработаны в научных работах Л.К. Терещенко, Е.С. Зиновьевой, И.М. Попова, М.М. Хамзатова, С.М. Бойко и других ведущих ученых в данной области. Проведенный анализ показывает, что в отечественной науке накоплен существенный багаж знаний по отдельным аспектам информационной безопасности. Методологическую основу исследования составляет междисциплинарный подход к исследованию проблемы, использующий положения философии, юриспруденции, социологии, политологии, военной науки и иных отраслей научного познания. В процессе исследования проблем правового обеспечения информационной безопасности применялись общенаучные методы (абстрагирование, анализ, синтез, аналогия, индукция, дедукция, моделирование).

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. При этом в настоящее время обеспечение национальной безопасности характеризуется как комплексная система, детерминированная действием многообразных факторов и угроз [1, с. 102]. Условия цифровой трансформации в результате бурного развития цифровых технологий, изначально предполагавшие позитивное влияние на все сферы жизнедеятельности при адекватном использовании достижений научно-технического прогресса, вместе с тем могут стать не только эффективным инструментом созидательного преобразования общественных отношений, но и таят в себе определенные риски. Так, за последние годы зафиксировано значительное увеличение количества преступлений, совершенных с использованием компьютерных технологий.

Исследуя статистические данные, следует отметить, что ущерб России от киберугроз в 2018 г. составил более 1 трлн руб., в 2019 г. – 2,5 трлн руб. [2] Вместе с тем в 2020 г. ущерб составил – 3,5 трлн руб., а за 2021 г., по предварительным данным, составляет – 7 трлн руб. [3]. Статистические данные показывают, что количество кибератак с каждым годом увеличивается и результатом их является все более значительный ущерб на отечественную информационную инфраструктуру. Так, экспертами отмечается, что количество информационных атак с каждым годом увеличивается на 6,5% по сравнению с предыдущим [4].

В свою очередь, можем констатировать, что органы публичной власти Российской Федерации адаптируются к новым условиям работы в ИКТ-среде с учетом новых больших вызовов, угроз и рисков. Усиление противоправного воздействия на информационные ресурсы в системе публичного управления потребовали принятия дополнительных мер по обеспечению информационной безопасности [5].

Важность данного вопроса также отметил Министр иностранных дел России С.В. Лавров, который особо подчеркнул, что появление новых информационных технологий влечет за собой смену привычных парадигм, определяет новые правила по использованию информационных систем, придав при этом очередной импульс на переход в цифровую сферу деятельности публичных органов и негосударственных организаций. По его мнению, современные вызовы, угрозы и риски являются результатом агрессивной и многолетней политики отдельных стран Европейского союза и США, которые стремятся сформировать и закрепить свое доминирование во всех технологических процессах информационного пространства. Он также подчеркнул важность мер по противодействию технотронной преступности: «Практически ежедневно мощным кибератакам с применением продвинутых информационных технологий подвергаются российские государственные учреждения, СМИ, объекты критической инфраструктуры, система жизнеобеспечения. Все это – часть скоординированной информационной агрессии против нашей страны. Требуется особое внимание к задачам защиты соответствующих ресурсов органов исполнительной власти, включая Министерство иностранных дел. Предстоит на постоянной основе совершенствовать принимаемые в этих целях меры, наладить повседневный контроль выполнения соответствующих поручений Правительства» [6].

Считаем, что в условиях геополитической нестабильности и трансформации мирового порядка современные кибератаки, имеющие нестандартные методы, способы и средства их совершения, требуют на законодательном уровне оперативности работы по предотвращению и недопущению деструктивного воздействия на отечественные информационные ресурсы и информационную инфраструктуру государственного и частного сектора.

Сегодня состояние информационной безопасности вызывает определенную обеспокоенность ввиду систематичных атак, осуществляемых в целях дестабилизации традиционных общественных отношений в отдельных регионах мира, а также распространения недостоверной информации для продвижения собственных национальных интересов в военно-политических и иных враждебных целях [7, с. 42]. Происходит активизация процессов распространения недостоверной информации «недружественными» государствами, информационное противоборство между ведущими державами мира, в том числе в военно-политических целях. Данные противоправные действия направлены на дестабилизацию деятельности публичных органов власти и

вмешательства во внутренние дела государства посредством использования информационных технологий.

Проведенное исследование показывает, что способы ведения враждебных действий на современном этапе развития цифровых технологий находятся также в процессе перманентного развития. Увеличивается также количество случаев ведения гибридных войн. Гибридные конфликты ведутся «иррегулярными силами, смешанными с регулярными войсками, и характеризуются одновременным применением иррегулярной и регулярной стратегии и тактики действий» [8, с. 344]. При таком типе конфликтов возможность использования информационного оружия еще более возрастает, трансформируя поле враждебных действий и интегрируя их применение в информационной, экономической, политической и иных сферах. Так, постоянный представитель Китая при ООН отметила, что акты произвольных блокировок и замораживаний резервов иностранной валюты тоже ведут к нарушению суверенитета государств [9].

Следует отметить, что формирование системы информационной безопасности с учетом национальных интересов России, предотвращение (урегулирование) межгосударственных конфликтов в глобальном информационном пространстве возможны только на основе соответствующего международно-правового режима, содействие установлению которого определено главной целью государственной политики в области международной информационной безопасности [10, с. 53]. Неотъемлемой частью этого режима должны стать правила поведения государств в информационном пространстве и в условиях вооруженного конфликта. Кроме того, важной угрозой в информационной сфере, влияющей на обеспечение национальной безопасности, является воздействие на критически важную инфраструктуру. Эти угрозы возникают в результате нарушения функционирования информационных систем [11, с. 72].

Обозначенные условия неизбежно влекут меры по усилению позиций России в условиях конкурентоспособной информационной борьбы как с уже существующими, так и с новыми центрами силы, а также по дальнейшему совершенствованию международно-правового регулирования отдельных положений развития средств и методов защиты информации на основе использования передовых цифровых технологий.

В данном исследовании можно выделить современные вызовы и угрозы национальной информационной безопасности, которые делятся на внутренние и внешние.

К внутренним угрозам в информационной сфере следует, на наш взгляд, отнести:

1) систематическое нарушение правил по порядку пользования информации ограниченного доступа;

2) отсутствие либо ненадлежащий уровень квалификации у персонала в использовании информационных и компьютерных устройств и иной продукции, необходимой для обеспечения информационной безопасности;

3) использование зарубежных технологий и технических средств в информационных процессах;

4) нарушение правовых норм по защите авторских прав при создании и внедрении секретных изобретений, созданных, в том числе по государственному заказу;

5) коллизии и правовые пробелы в отечественном законодательстве при регулировании

отношений в сфере информационной безопасности;

6) и иные.

К внешним угрозам в информационной сфере относятся:

1) активные разведывательные и контрнаступательные мероприятия иностранных органов спецслужб;

2) непрерывные информационные акты агрессии посредством кибератак на объекты информационных инфраструктур;

3) применение методов и средств информационных войн посредством использования когнитивного оружия иностранными государствами против национальных интересов Российской Федерации;

4) использование специальных приемов в информационном пространстве, которые затрагивают интересы межгосударственного сотрудничества в области обеспечения информационной безопасности;

5) применение методов фильтрации цифрового контента в сети Интернет в целях ограничения распространения достоверной информации о политике Российской Федерации и продвигаемых ею инициативах;

6) и иные.

Учитывая приведенный перечень современных информационных угроз, считаем необходимым наряду с использованием комплекса правовых средств принятиеорганизационных мер в области обеспечения информационной безопасности:

1) формирование благоприятных условий для совершенствования кадрового потенциала и формирования резерва специалистов в сфере информационных технологий и информационной безопасности;

2) создание отечественного программного продукта по защите информации и выявлению угроз в информационной системе;

3) повышение цифровой и информационно-правовой культуры информационной безопасности граждан для формирования устойчивости к информационно-психологическому воздействию иностранных спецслужб и влиянию деструктивной идеологии;

4) совершенствование нормативно-правовой базы по защите объектов интеллектуальной собственности и российской информационной инфраструктуры;

5) создание эффективных мер по защите информации посредством развития технического регулирования, включая вопросы лицензирования, стандартизации, аттестации и сертификации в данной области;

6) развитие межгосударственного сотрудничества с государствами – партнерами в области обеспечения информационной безопасности посредством интеграционного взаимодействия, формирования общих международных норм в области правового обеспечения информационной безопасности.

Полагаем, что формирование и развитие национальной государственной политики, направленной на обеспечение информационной безопасности будет способствовать

дальнейшему совершенствованию защиты информационных технологий и систем, недопущению уязвимости данных и снижению возникновения информационных угроз. Представляется, что данные меры позволят обеспечить защиту информационного суверенитета России, охрану субъектов и объектов высоких информационных технологий и инновационной инфраструктуры.

Таким образом, на основе проведенного исследования можно сделать вывод о совокупности разнообразных рисков, вызовов и угроз в информационном пространстве, усилившихся в условиях геополитических изменений и дальнейшей цифровизации всех сфер. На современном этапе развития общества и государства среди наиболее актуальных угроз национальной информационной безопасности ввиду динамичности информационной сферы можно выделить такие угрозы, как противоправное воздействие на национальные информационные ресурсы, информационно-телекоммуникационные системы и информационную инфраструктуру, включая критически важные информационные структуры; использование средств и методов распространения недостоверной (фейковой) информации в целях дезинформации неопределенного круга людей с использованием противоправных методов и средств, включая когнитивные методы воздействия на психику человека в целях дезорганизации и подавления воли; несанкционированное вмешательство в национальное информационное пространство. Тем самым трансформация информационного пространства в условиях геополитических изменений и обострение социально-экономических и международных противоречий определили новый вектор развития правового регулирования информационной безопасности.

Библиография

1. Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. 2015. № 8. С. 100–109.
2. Сбербанк прогнозирует ущерб экономике России от киберугроз в 2018 году в 1,1 трлн рублей // Газета «Коммерсант». URL: https://www.kommersant.ru/doc/3676752 (дата обращения: 23.06.2023)
3. Сбербанк подсчитал потери российской экономики в 2021 году от киберпреступности // Интернет-издание «ТАСС». URL: https://tass.ru/ekonomika/8761953 (дата обращения: 23.06.2023).
4. Актуальные киберугрозы: итоги 2021 года // Positive technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения: 23.06.2023).
5. Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // СЗ РФ. 2022. № 18. Ст. 3058.
6. Выступление министра иностранных дел Российской Федерации С.В. Лаврова на пленарной сессии «Международные отношения в условиях цифровизации общественной жизни» международной научно-практической конференции «Цифровые международные отношения 2022», Москва, 14 апреля 2022 г. // Официальный сайт Министерства иностранных дел РФ. URL: https://www.mid.ru/ru/press_service/video/view/1809294/#sel=29:1:BXe,29:101:cfj (дата обращения: 24.06.2023).
7. Дубень А.К. Информационная безопасность как составная часть национальной безопасности Российской Федерации // The Scientific Heritage. 2021. No. 74-4 (74).

P. 41–45.
8. Попов И.М., Хамзатов М.М. Война будущего: Концептуальные основы и практические выводы. Очерки стратегической мысли. М., 2016. 831 с.
9. В КНР потребовали отказаться от заморозки резервов других стран // ОСН. Общественная служба новостей. URL: https://www.osnmedia.ru/world/v-knr-potrebovali-otkazatsya-ot-zamorozki-rezervov-drugih-stran/?utm_source=yxnews&utm_medium=desktop (дата обращения: 25.06.2023).
10. Бойко С.М. Новые стратегические ориентиры России в области международной информационной безопасности // Международная жизнь. 2021. № 6. С. 52–61.
11. Зиновьева Е.С. Международная информационная безопасность: Монография. М., 2013. 192 с.

Результаты процедуры рецензирования статьи

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

Предметом исследования в представленной на рецензирование статье являются, как это следует из ее наименования, вопросы обеспечения информационной безопасности. Автор предполагал сосредоточить свое внимание на постановке соответствующих задач и определении путей их решения. Фактически это не сделано, о чем более подробно будет сказано в дальнейшем.
Методология исследования в тексте статьи не раскрывается, но очевидно, что ученым использовались всеобщий диалектический, логический, статистический, формально-юридический методы исследования.
Актуальность избранной автором темы исследования обоснована следующим образом: "Сегодня все больше исследователей сходятся во мнении, что вопросы информационной безопасности являются столь же важными, чем вопросы ядерной сферы, что делает их ключевым фактором стратегической стабильности [1, с. 284]. Информационная сфера, оставаясь бесконтрольной, неизбежно способствует дестабилизации общества и манипулированию общественным сознанием. Учитывая пребывание информационного пространства в непрерывном состоянии неопределенности и опасности, 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. Кроме того, важно выстраивание надлежащей архитектуры информационной безопасности, без которой сохранение состояния информационной защищенности невозможно, включая комплекс мер организационно-правового обеспечения". Дополнительно ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.
В чем проявляется научная новизна работы, прямо не говорится. Фактически она отсутствует. Автор не предлагает оригинальных дефиниций дискуссионных понятий, не дает конкретных рекомендаций по совершенствованию российского законодательства в сфере обеспечения информационной безопасности и проч. Статья носит описательный, поверхностный характер, представляя собой компиляцию ряда использованных при ее написании источников. В представленном виде она не вносит вклада в развитие отечественной правовой науки.
Научный стиль исследования выдержан автором в полной мере.

Структура статьи вполне логична. Во вводной части статьи ученый обосновывает актуальность избранной темы исследования. В основной части работы с приведением соответствующих примеров описываются основные проблемы в сфере обеспечения информационной безопасности, в общих чертах намечаются некоторые пути их решения. В заключительной части статьи содержатся выводы по результатам проведенного исследования.

Содержание работы не вполне соответствует ее наименованию. Также оно не лишено некоторых других недостатков.

Так, автор пишет: "Информация, став одним из важнейших экономических и политических ресурсов расширяет круг способов для различных способов ее использования в образовательных, социальных, экономических и культурных целях, для целей охраны здоровья граждан, обеспечения законности и правопорядка, в иных общественно значимых целях, при этом открывает широкий диапазон возможностей для ее применения в качестве оружия, разрушающего стабильность общественных отношений и отрицательно влияющего на качество жизни человека", т. е. "Информация ... расширяет круг способов для различных способов..." - предложение содержит тавтологию.

Ученый отмечает: "Вместе с тем количество кибератак с каждым годом увеличивается и приобретает все более значительный ущерб на отечественную информационную инфраструктуру...". Смысл предложения затемнен.

Фактически в статье отсутствует четкое обозначение задач государства в сфере обеспечения информационной безопасности. Как следствие, не названы конкретные пути их решения. Автор пишет, что "Для решения указанных задач экономически развитыми государствами так называемого западного мира создают специализированные структуры ведения подрывной пропаганды в сетевом пространстве и кибератак", но ничего конкретного не предлагает.

Ученый пишет: "... развитие информационных и телекоммуникационных технологий привело к появлению в информационном праве новых терминов таких как: «информационное оружие» и «информационная война», которые требуют научного осмысления с учетом современной геополитической обстановки, характеризующая усилением информационных рисков и угроз, в том числе в сфере обеспечения цифрового и технологического суверенитета государства, его конституционного строя и обороны". Сам автор соответствующие дефиниции понятий «информационное оружие» и «информационная война» не исследует и своих определений не предлагает.

Автор рассуждает "... о многообразии форм и методов ведения информационной войны и необходимости формирования правовых норм в отечественном законодательстве, которые бы регулировали взаимосвязанные общественные отношения в интересах национальной безопасности". Направлений совершенствования отечественного законодательства в данной сфере ученый не называет.

Библиография исследования представлена 12 источниками (нормативным правовым актом, диссертационной работой, монографией, научными статьями, аналитическими и статистическими данными). С формальной точки зрения этого достаточно, но фактически автору не удалось раскрыть тему исследования с необходимой глубиной и полнотой. Статья очень поверхностна по своему содержанию.

Апелляция к оппонентам как таковая отсутствует. Автор ссылается на ряд использованных при написании статьи источников в подтверждение своих суждений или для иллюстрирования отдельных положений работы (С. К. Кузнецов, Е. С. Зиновьева и др.), но в научную дискуссию с конкретными оппонентами не вступает. Положения работы не всегда обосновываются в должной степени.

Выводы по результатам исследования имеются ("... развитие информационных и

телекоммуникационных технологий привело к появлению в информационном праве новых терминов таких как: «информационное оружие» и «информационная война», которые требуют научного осмысления с учетом современной геополитической обстановки... . Современное состояние информационного противоборства между различными субъектами, имеющими собственные национальные интересы, свидетельствует о многообразии форм и методов ведения информационной войны и необходимости формирования правовых норм в отечественном законодательстве, которые бы регулировали взаимосвязанные общественные отношения в интересах национальной безопасности. ... вопросы противодействия современным вызовам и угрозам следует рассматривать на национальном, международном и межгосударственном (региональном) уровнях. Объединение усилий государств позволит выработать единые правовые механизмы противодействия использованию цифровых технологий в противоправных целях и усилить стабильность"), однако они носят общий характер и подлежат уточнению с учетом необходимости доработки основной части статьи.

Статья нуждается в дополнительном вычитывании с привлечением специалиста-филолога. В ней встречаются множественные опечатки, пропуски букв, орфографические, пунктуационные, синтаксические, стилистические ошибки.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере международного права, административного права, информационного права при условии ее существенной доработки: уточнении предмета исследования, раскрытии его методологии, дополнительном обосновании актуальности избранной темы исследования, введении элементов научной новизны и дискуссионности, уточнении отдельных положений работы и выводов по результатам исследования, устранении нарушений в оформлении статьи.

Результаты процедуры повторного рецензирования статьи

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

Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ

на статью на тему «Приоритетные задачи обеспечения информационной безопасности в условиях современных вызовов и угроз».

Предмет исследования.

Предложенная на рецензирование статья посвящена актуальным вопросам обеспечения информационной безопасности в условиях современных вызовов и угроз. Автором обоснованы и сформулированы в качестве перечня совокупность приоритетных задач в сфере обеспечения информационной безопасности в настоящих условиях. В качестве предмета исследования выступили нормы законодательства, мнения ученых, материалы практики.

Методология исследования.

Цель исследования прямо в статье не заявлена. Однако цель исследования может ясно понята, исходя из названия и содержания статьи. Цель исследования может быть обозначена в качестве установления системы приоритетных задач обеспечения информационной безопасности в условиях современных вызовов и угроз. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.

В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и

синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из материалов практики.
Автором отмечено, что «Методологическую основу исследования составляет междисциплинарный подход к исследованию проблемы, использующий положения философии, юриспруденции, социологии, политологии, военной науки и иных отраслей научного познания. В процессе исследования проблем правового обеспечения информационной безопасности применялись общенаучные методы (абстрагирование, анализ, синтез, аналогия, индукция, дедукция, моделирование)».
В частности, автором делаются конкретные выводы на основе статистических данных, что важно в контексте цели исследования. В частности, отметим следующие рассуждения автора: «Исследуя статистические данные, следует отметить, что ущерб России от киберугроз в 2018 г. составил более 1 трлн руб., в 2019 г. – 2,5 трлн руб. [2] Вместе с тем в 2020 г. ущерб составил – 3,5 трлн руб., а за 2021 г., по предварительным данным, составляет – 7 трлн руб. [3]. Статистические данные показывают, что количество кибератак с каждым годом увеличивается и результатом их является все более значительный ущерб на отечественную информационную инфраструктуру. Так, экспертами отмечается, что количество информационных атак с каждым годом увеличивается на 6,5% по сравнению с предыдущим [4]».
Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.
Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема обеспечения информационной безопасности в условиях современных вызовов и угроз сложна и неоднозначна. В ситуации, когда меняются общественные отношения под влиянием процессов цифровизации, органы государственной власти, граждане, иные участники правоотношений должны быстро и эффективно реагировать на возникающие сложности в сфере безопасности. Автор прав в том, что «Информация, являющаяся одним из главных экономических и политических ресурсов, расширяет круг различных способов ее использования в образовательных, социальных, экономических и культурных целях, обеспечения законности и правопорядка, в иных общественно значимых целях».
Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.
Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:
«на основе проведенного исследования можно сделать вывод о совокупности разнообразных рисков, вызовов и угроз в информационном пространстве, усилившихся в условиях геополитических изменений и дальнейшей цифровизации всех сфер. На современном этапе развития общества и государства среди наиболее актуальных угроз национальной информационной безопасности ввиду динамичности информационной сферы можно выделить такие угрозы, как противоправное воздействие на национальные информационные ресурсы, информационно-телекоммуникационные системы и информационную инфраструктуру, включая критически важные информационные структуры; использование средств и методов распространения недостоверной (фейковой) информации в целях дезинформации неопределенного круга людей с использованием противоправных методов и средств, включая когнитивные методы воздействия на психику человека в целях дезорганизации и подавления воли;

несанкционированное вмешательство в национальное информационное пространство. Тем самым трансформация информационного пространства в условиях геополитических изменений и обострение социально-экономических и международных противоречий определили новый вектор развития правового регулирования информационной безопасности».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.

Во-вторых, автором предложены оригинальные обобщения по поводу совокупности приоритетных задач в сфере обеспечения информационной безопасности в настоящих условиях.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Вопросы безопасности», так как она посвящена правовым проблемам, связанным с обеспечением информационной безопасности в России.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели исследования.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.

Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.

Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России и из-за рубежа (Терещенко Л.К., Тиунов О.И., Дубень А.К., Попов И.М., Хамзатов М.М. и другие) Многие из цитируемых ученых являются признанными учеными в области обеспечения национальной безопасности.

Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.

Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.

Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к развитию законодательства и практики его применения в России в сфере обеспечения информационной безопасности.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи

«Рекомендую опубликовать»