

Научная статья

УДК 342

DOI: <https://doi.org/10.30932/2500-1868-2026-59-3-13>

Совершенствование законодательства об общественной безопасности под влиянием цифровых технологий

Ягофарова Инара Дамировна,

кандидат юридических наук, доцент,

Уральский государственный экономический университет,

старший научный сотрудник

Центра исследования проблем безопасности

Российской академии наук,

Екатеринбург, Москва, Россия

ORCID: <https://orcid.org/0000-0002-8508-7920>

РИНЦ SPIN-код: 7216-8150, AuthorID: 488352

Аннотация. В статье обосновывается необходимость модернизации российского законодательства об общественной безопасности в условиях цифровизации. Настоящая статья ставит своей целью выявление основных проблем правового регулирования общественной безопасности в условиях цифровизации, а также разработку рекомендаций по совершенствованию законодательства с учетом новых технологических реалий. В качестве основных методов исследования были использованы сравнительно-правовой метод, исторический анализ, социологическое исследование, а также формально-логический метод. Выявлено, что существующая нормативная база носит фрагментарный характер и не в полной мере адаптирована к цифровым вызовам и угрозам. В связи с этим требуется комплексное совершенствование правового регулирования, предполагающее систематизацию законодательства об общественной безопасности с учетом цифровых аспектов, корректировка уголовного законодательства в части совершенствования санкций за преступления, совершенные с применением информационных и цифровых ресурсов, создание правовой основы для применения искусственного интеллекта в деятельности правоохранительных органов и т.д. Сформулированы выводы о необходимости дальнейшего совершенствования законодательства об общественной безопасности с учетом цифровых вызовов и угроз.

Ключевые слова: общественная безопасность; цифровые технологии; правовое регулирование; искусственный интеллект; цифровые вызовы и угрозы общественной безопасности.

Статья подготовлена в рамках реализации государственного задания «Комплексное исследование проблем общественной безопасности, как стратегического приоритета национальной безопасности Российской Федерации (FFFZ-2025-0001)».

Для цитирования: Ягофарова И. Д. Совершенствование законодательства об общественной безопасности под влиянием цифровых технологий // Транспортное право и безопасность. 2026. № 3(59). С. 158–167. <https://doi.org/10.30932/2500-1868-2026-59-3-13>.

Original article

Improvement of public security legislation under the effect of digital technologies

Inara D. Yagofarova,
Candidate of Law, Associate Professor,
Ural State University of Economics,
Senior Researcher of the
Security Problems Studies Center of RAS,
Ekaterinburg, Moscow, Russia

Abstract. The current paper has substantiated the necessity to modernize Russian legislation on public security in the context of digitalization. The purpose of the current study was to identify key issues regarding the legal regulation of public security in the context of digitalization and to develop recommendations for improving legislation, taking into account new technological realities. The primary research methods of the study included the comparative legal method, historical analysis, sociological research, and the formal-logical method. There has been found that the existing regulatory framework is fragmentary in nature and not fully adapted to digital challenges and threats. In this regard, a comprehensive improvement of the legal framework is of necessity, entailing the systematization of public security legislation taking into account digital aspects, the adjustment of criminal law, specifically regarding sanctions for crimes committed using information and digital resources, and the establishment of a legal basis for the use of artificial intelligence in law enforcement activities, among other measures. There have been drawn conclusions regarding the necessity to further refine public security legislation in light of digital challenges and threats.

Keywords: public security; digital technologies; legal regulation; artificial intelligence; digital challenges and threats to public security.

The current paper has been prepared as part of the implementation of the state assignment “Comprehensive study of public security issues as a strategic priority of national security of the Russian Federation (FFFZ-2025-0001)”.

For citation: Yagofarova I.D. Improvement of public security legislation under the effect of digital technologies // Transport law and security. 2026; (3(59)):158–167.

© Ягофарова И. Д., 2026

Стремительная цифровизация всех сфер общественной жизни сопровождается ростом новых вызовов и угроз общественной безопасности, которые не были в полной мере учтены при разработке действующей нормативно-правовой базы. Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 2 июля 2021 г. № 400) (далее — Стратегия 2021 г.) относит государственную и общественную безопасность к числу стратегических национальных приоритетов (п. 26), однако анализ ее положений показывает, что она лишь контурно обозначает данное направление, не выделяя цифровые вызовы и угро-

зы (кибертерроризм, киберэкстремизм, распространение деструктивного контента и др.) в качестве самостоятельных объектов противодействия.

При этом Концепция общественной безопасности в Российской Федерации (утверждена Президентом РФ 14 ноября 2013 г. № Пр-2685) (далее — Концепция 2013 г.), срок реализации которой закончился в 2020 г., также не содержала положений, адекватно отражающих современные реалии киберпространства. Таким образом, единственный профильный документ стратегического планирования в сфере общественной безопасности не только фактически прекратил свое действие, но и по своему содержанию не соответствовал вызовам цифровой эпохи даже в период своего действия. При этом новый документ стратегического планирования в сфере общественной безопасности до настоящего времени не принят, что оставляет данную область без концептуального ориентира в условиях цифровой трансформации.

Вместе с тем правовое регулирование общественной безопасности в условиях цифровизации осуществляется множеством нормативных правовых актов — Федеральными законами от 28 декабря 2010 г. № 390-ФЗ «О безопасности», от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» и др. Однако данные акты, будучи принятыми в разное время и в ответ на различные угрозы, регулируют отдельные аспекты, не создавая целостной системы, способной адекватно реагировать на новые цифровые вызовы и угрозы. В связи с этим возникает объективная необходимость проанализировать, как законодатель реагировал на появление новых цифровых вызовов и угроз, и выработать конкретные предложения по совершенствованию правового регулирования в данной сфере.

Целью настоящего исследования является анализ динамики развития российского законодательства в сфере общественной безопасности под влиянием цифровых технологий, выявление пробелов правового регулирования, а также разработка предложений по совершенствованию нормативно-правовой базы с учетом новых вызовов и угроз, возникающих в цифровой среде.

Проблема влияния цифровых технологий на правовое регулирование общественной безопасности активно разрабатывается в современной юридической науке. Исследователи анализируют конкретные цифровые угрозы, выявляют проблемы правоприменения и предлагают пути совершенствования законодательства. Так, В. М. Шеншин в своих исследованиях констатирует, что противодействие цифровому экстремизму и терроризму является одной из наиболее значимых государственных задач, однако ее решение затруднено множеством проблем [1]. Автор выделяет трудности блокировки экстремистских ресурсов, использующих анонимные программы (VPN), длительность процедуры признания контента экстремистским, невозможность получения данных от владельцев зарубежных ин-

тернет-ресурсов. В качестве предложения автор предлагает разработать в УК РФ новый состав преступления «кибертерроризм», автоматизировать мониторинг за экстремистскими материалами и активизировать международное сотрудничество в борьбе с киберпреступностью.

В своих исследованиях Е. А. Ларина анализирует феномен киберсталкинга как одну из наиболее агрессивных форм отклоняющегося поведения в сети Интернет. Автор отмечает, что распространение киберсталкинга угрожает личной, информационной и финансовой безопасности граждан. На основе анализа зарубежного опыта (США, Великобритании, Германии, Сингапура и т.д.) делается вывод о целесообразности применения наиболее эффективных мер противодействия киберсталкингу, успешно функционирующих за рубежом, для защиты российского населения в виртуальном пространстве. Автором подчеркивается, что в России данное деяние не криминализировано [2].

Рассматривая проблемы киберпреступности, Г. А. Майстренко отмечает, что для борьбы с этим видом преступности требуется активизация совместных усилий государств в борьбе с данным феноменом [3]. Действительно, рост киберпреступности требует международной кооперации, а анализ сущности и видов таких преступлений является необходимой базой для эффективного законодотворчества и правоприменения. Без этого борьба будет ситуативной и несистемной.

Ряд авторов в своих исследованиях выявляют роль и обосновывают высокую значимость кибервызова как требования по обеспечению безопасности цифровой информации, определяют факторы влияния на киберриски и предлагают вариант построения программы управления киберрисками [4]. Данный подход с практической позиции является значимым, поскольку цифровизация без системного управления рисками ведет к уязвимости.

В. В. Машко акцентирует внимание на том, что в российском законодательстве отсутствует четкое понимание понятий, связанных с регулированием кибертерроризма, а также нет единообразной практики правоприменения, включая трансграничный характер угроз и недостаточную обеспеченность правоохранительных органов техническими средствами [5]. Отсутствие четких дефиниций в российском законодательстве и трансграничность угроз действительно является реальной проблемой. Однако предложенное в работе автором определение кибертерроризма является лишь первым шагом, поскольку без унификации на международном уровне и без реального оснащения правоохранительных органов его ценность ограничена.

Обзор дискуссий свидетельствует о том, что научное сообщество активно исследует различные аспекты влияния цифровых технологий на общественную безопасность. Исследователи анализируют конкретные угрозы (киберсталкинг, кибертерроризм, киберэкстремизм), выявляют проблемы

правоприменения (трансграничный характер угроз, отсутствие легальных дефиниций и т.д.) и предлагают пути совершенствования.

Как уже было отмечено, Концепция 2013 г. не содержала положений, адекватно отражающих цифровые вызовы и угрозы общественной безопасности. В п. 6 Концепции 2013 г. было закреплено понятие «государственная система мониторинга состояния общественной безопасности» как единая межведомственная многоуровневая автоматизированная информационная система. Однако данное понятие касалось исключительно технической стороны мониторинга, а не противодействия киберугрозам как таковым. В перечне угроз общественной безопасности, приведенном во втором разделе Концепции, цифровые угрозы отсутствовали, что объясняется тем, что они в тот период еще не приобрели массового характера.

Анализ законодательства позволяет выделить несколько этапов, в рамках которых происходила постепенная трансформация законодательства в части закрепления мер противодействия цифровым вызовам и угрозам.

Первый этап (1996—2011) связан с формированием базовых норм об ответственности за преступления в сфере компьютерной информации. Глава 28 «Преступления в сфере компьютерной информации» была включена в УК РФ в 1996 г. Однако в тот период законодатель еще не выделял цифровые угрозы как угрозы общественной безопасности в широком смысле, ограничиваясь защитой компьютерной информации как таковой.

Второй этап (2011—2016) ознаменовался осознанием того, что цифровые технологии становятся средством совершения «традиционных» преступлений (терроризм, экстремизм). Федеральным законом от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» были введены квалифицирующие признаки «с использованием информационно-телекоммуникационных сетей» для ряда составов преступлений (ст. 280, 282 и другие УК РФ). Это стало первым прямым признанием законодателем того, что интернет является площадкой для совершения преступлений, посягающих на общественную безопасность.

Третий этап (2016—2021) характеризуется принятием документов стратегического планирования, в которых цифровые угрозы впервые были обозначены на высшем уровне. Доктрина информационной безопасности Российской Федерации. (утверждена Указом Президента РФ от 5 декабря 2016 г. № 646) уже прямо указывает на деятельность террористических и экстремистских организаций, использующих механизмы информационного воздействия, а также на рост компьютерной преступности (п. 12—14).

Четвертый этап (2021—2014) связан с принятием Стратегии 2021 г., которая отнесла информационную безопасность к числу стратегических приоритетов. Однако в Стратегии 2021 г. вопросы противодействия киберугрозам напрямую не выделены.

Пятый этап (с 2024 г. по настоящее время) характеризуется принятием Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий (принята распоряжением Правительства РФ от 30 декабря 2024 г. № 4154-р). Данный документ впервые на уровне правительства определяет принципы, цели, задачи и функции государственной системы противодействия киберугрозам.

Анализ положений законодательства в сфере противодействия цифровым угрозам общественной безопасности позволяет выделить следующие пробелы правового регулирования и проблемы правоприменения:

— *отсутствие системного подхода на уровне стратегического планирования и понятийной определенности.* Концепция общественной безопасности 2013 г. утратила силу, а новый документ стратегического планирования в этой сфере не принят. В результате отсутствует документ, в котором были бы закреплены понятия «цифровые вызовы и угрозы общественной безопасности», обозначены формы их проявления и выстроена система противодействия с учетом их специфики. Нормы, касающиеся данной сферы, рассредоточены по различным нормативным актам, что порождает проблему согласованности и непротиворечивости [6];

— *проблема «догоняющего» характера уголовно-правовых норм.* Анализ изменений, внесенных в УК РФ в 2022—2024 гг., показывает, что законодатель реагирует на уже существующие угрозы, а не упреждает их. Как подчеркивается специалистами, в условиях острого противостояния необходимо использовать превентивные меры уголовного законодательства [7], однако действующий механизм правового регулирования не всегда позволяет это делать эффективно;

— *несоразмерность санкций степени общественной опасности деяний.* В ряде случаев законодатель, криминализируя общественно опасные деяния в сфере общественной безопасности, не учитывает должным образом санкционный аспект. Как отмечают исследователи, в качестве основной меры наказания указан штраф, если указано лишение свободы, то не определен нижний предел, что принижает значимость безопасности государственной власти [8]. Особенно это заметно применительно к преступлениям, совершаемым с использованием цифровых технологий и причиняющих значительный ущерб общественной безопасности. Штрафные санкции, даже в крупных размерах, не всегда выступают адекватной мерой ответственности за деяния, подрывающие основы общественной безопасности;

— *проблема правовой регламентации применения искусственного интеллекта в обеспечении общественной безопасности.* Внедрение технологий искусственного интеллекта (ИИ) в деятельность правоохранительных органов открывает новые возможности для обеспечения общественной безопасности. Однако правовое регулирование применения ИИ в этой сфере находится в зачаточном состоянии. Как обоснованно указано в

научной литературе, несмотря на то что ИИ является наиболее перспективным направлением цифровизации в современный период, есть необходимость детальной технической доработки соответствующих систем для устранения рисков нарушений прав и свобод человека [9]. Особую озабоченность вызывает отсутствие законодательных гарантий против дискриминационного использования алгоритмов ИИ, а также нерешенность вопросов юридической ответственности за ошибки при принятии решений с использованием ИИ [10];

— *трансграничный характер угроз и недостаточная координация.* Киберугрозы не признают государственных границ, что создает дополнительные сложности для правоприменения. Отсутствие унифицированных подходов к квалификации деяний в сфере общественной безопасности, совершаемых с использованием цифровых технологий, затрудняет международное сотрудничество в этой области. На национальном уровне остается нерешенной проблема разграничения компетенций правоохранительных органов при расследовании «цифровых» преступлений против общественной безопасности, а также обмена информацией между ними.

На основе проведенного анализа, с учетом предложений, высказанных в научной литературе, можно выделить следующие направления совершенствования законодательства об общественной безопасности под влиянием цифровых технологий.

1. Необходимо в рамках предлагаемого специалистами по данной проблематике специализированного закона об общественной безопасности предусмотреть отдельную главу (раздел), посвященную мониторингу цифровых вызовов и угроз общественной безопасности [11]. В ней следует определить понятие и виды цифровых вызовов и угроз; порядок их выявления, фиксации и оценки; полномочия субъектов обеспечения общественной безопасности в части мониторинга цифровых угроз; механизмы взаимодействия между государственными органами, владельцами информационных ресурсов. Такой подход позволит создать правовую основу для системного противодействия киберугрозам.

2. Требуется разработка и принятие документа стратегического планирования в сфере общественной безопасности. В указанном документе необходимо закрепить понятия «цифровые вызовы и угрозы общественной безопасности», обозначить основные формы их проявления, также необходимо выстроить систему противодействия с учетом специфики каждого вида угроз. Отличие данного документа от федерального закона заключается в том, что в нем будут содержаться более динамичные понятия, позволяющие оперативно корректировать их содержание с учетом трансформации вызовов и угроз.

3. Требуется внесение изменений в УК РФ в части введения отдельного состава преступления «кибертерроризм» и уточнения квалифицирующих признаков экстремистских преступлений, совершаемых с использованием информационно-телекоммуникационных сетей.

Кроме того, необходимо пересмотреть санкции норм, предусматривающих ответственность за преступления против общественной безопасности, совершаемых с использованием цифровых технологий с учетом их реальной общественной опасности. В частности, представляется необходимым исключить штраф как основной вид наказания за деяния, создающие реальную угрозу причинения тяжкого вреда общественной безопасности, либо установить нижний предел лишения свободы по таким составам.

4. Принять специальный федеральный закон «Об использовании технологий искусственного интеллекта в деятельности правоохранительных органов по обеспечению общественной безопасности». Данный закон должен определять допустимые цели и пределы использования ИИ, требования к алгоритмам ИИ и гарантии соблюдения прав и свобод человека при использовании ИИ (запрет на дискриминационные алгоритмы, право на обжалование решений, принятых с использованием ИИ и т.д.).

5. Необходимо активизировать усилия по гармонизации национального законодательства с международными стандартами в сфере противодействия киберугрозам общественной безопасности. Целесообразно продолжить работу над унификацией понятийного аппарата и процедур взаимодействия, а также рассмотреть вопрос о ратификации дополнительных международных договоров в этой сфере с учетом национальных интересов.

6. Необходимо законодательно закрепить требования к минимальному уровню технической оснащенности правоохранительных органов средствами противодействия киберугрозам. Также обоснованным является обязанность повышения квалификации сотрудниками правоохранительных органов в сфере цифровых технологий не реже одного раза в два года. Кроме того, следует предусмотреть создание специализированных подразделений по противодействию киберугрозам общественной безопасности на всех уровнях.

Цифровая трансформация создает как новые возможности, так и новые вызовы для системы обеспечения общественной безопасности. Современное законодательство не всегда успевает за стремительным развитием технологий и появлением новых форм угроз [12]. В связи с этим требуется комплексное совершенствование правового регулирования, включающее систематизацию законодательства об общественной безопасности с учетом цифровых аспектов; корректировку уголовно-правовых норм и санкций в части ответственности за преступления, совершенные с применением информационных технологий; создание правовой основы для применения искусственного интеллекта в сфере защиты общественной безопасности; развития международного сотрудничества.

Предложенные рекомендации позволят создать более эффективную и сбалансированную систему правового регулирования общественной безопасности, адекватную современным вызовам цифровой эпохи и при этом обеспечивающую соблюдение прав и свобод граждан.

Список источников

1. Шеншин, В. М. Обеспечение общественной безопасности в эпоху цифровизации: некоторые проломные аспекты / В. М. Шеншин // Закон и власть. — 2026. — № 1. — С. 153—156.
2. Ларина, Е. В. Киберсталкинг как современная угроза общественной безопасности: меры противодействия в России и за рубежом / Е. В. Ларина // Социологическая наука и социальная практика. — 2025. — Том 13. — № 1. — С. 170—189.
3. Майстренко, Г. А. Киберпреступность в России: сущность, общественная опасность и методы борьбы / Г. А. Майстренко // Вопросы российского и международного права. — 2022. — Том 12. — № 1А. — С. 181—186.
4. Халин, В. Г. Цифровизация и киберриски / В. Г. Халин, Г. В. Чернова // Управленческое консультирование. — 2023. — № 7. — С. 28—41.
5. Машко, В. В. Кибертерроризм: понятие и проблемы противодействия / В. В. Машков // Мировой политический процесс: информационные войны и «цветные революции». Сборник материалов Международной научно-практической конференции. — Москва, 2022.
6. Колоткина, О. А. Значение унификации понятийно-категориального аппарата национальной безопасности в контексте уточнения содержания категории «общественная безопасность» / О. А. Колоткина // Наука. Общество. Государство. — 2025. — № 3 (51). — С. 49—58.
7. Зиядова, Д. З. Совершенствование законодательства в сфере обеспечения государственной и национальной безопасности в цифровую эпоху / Д. З. Зиядова, М. Г. Диева // Пробелы в российском законодательстве. — 2024. — Том 17. — № 7. — С. 105—111.
8. Пономаренко, Е. В. Обоснованность изменений уголовного законодательства, касающихся отдельных составов преступлений против основ конституционного строя и безопасности государства / Е. В. Пономаренко, К. О. Копшева // Правовая политика и правовая жизнь. Право. — 2023. — № 1. — С. 121—125.
9. Шхагапсоев, З. Л. Актуальные вопросы применения цифровых технологий для обеспечения общественной безопасности / З. Л. Шхагапсоев // Пробелы в российском законодательстве. — 2025. — № 18(7). — С. 50—55.
10. Иринин, К. В. Правовые механизмы обеспечения кибербезопасности государственных информационных систем в условиях цифровизации управления / К. В. Иринин // Проблемы правовой и технической защиты информации. — 2026. — № 13. — С. 50—56.
11. Гирько, С. И. Реальные шаги к институализации общественной безопасности Российской Федерации / С. И. Гирько // Научный портал МВД России. — 2025. — № 1 (69). — С. 33—40.
12. Ягофарова, И. Д. Цифровое государство как среда генерации гибридных угроз общественной безопасности: постановка проблемы / И. Д. Ягофарова // Современные тенденции развития науки и мирового сообщества в эпоху цифровизации (шифр — МКСТР). Сборник материалов 4 (0) Международной научно-практической конференции. — Москва, 2026.

References

1. Shenshin, V. M. Obespecheniye obshchestvennoy bezopasnosti v epokhu tsifrovizatsii: nekotoryye prolomnyye aspekty [Enforcing public security in the era of digitalization: key aspects] / V. M. Shenshin // Zakon i vlast'. — 2026. — № 1. — S. 153—156.

2. Larina, Ye. V. Kiberstalking kak sovremennaya ugroza obshchestvennoy bezopasnosti: mery protivodeystviya v Rossii i za rubezhom [Cyberstalking as a modern threat to public safety: countermeasures in Russia and abroad] / Ye. V. Larina // Sotsiologicheskaya nauka i sotsial'naya praktika. — 2025. — Tom 13. — № 1. — S. 170–189.
3. Maystrenko, G. A. Kiberprestupnost' v Rossii: sushchnost', obshchestvennaya opasnost' i metody bor'by [Cybercrime in Russia: nature, public danger, and methods of combating it] / G. A. Maystrenko // Voprosy rossiyskogo i mezhdunarodnogo prava. — 2022. — Tom 12. — № 1A. — S. 181–186.
4. Khalin, V. G. Tsifrovizatsiya i kiberriski [Digitalization and cyber risks] / V. G. Khalin, G. V. Chernova // Upravlencheskoye konsul'tirovaniye. — 2023. — № 7. — S. 28–41.
5. Mashko, V. V. Kiberterrorizm: ponyatiye i problemy protivodeystviya [Cyberterrorism: concept and challenges of counteraction] / V. V. Mashkov // Mirovoy politicheskiy protsess: informatsionnyye voyny i «tsvetnyye revolyutsii». Sbornik materialov Mezhdunarodnoy nauchno-prakticheskoy konferentsii. — Moskva, 2022.
6. Kolotkina, O. A. Znachenije unifikatsii ponyatiyno-kategorial'nogo apparata natsional'noy bezopasnosti v kontekste utochneniya soderzhaniya kategorii «obshchestvennaya bezopasnost'» [The significance of unifying the conceptual and categorical framework of national security in the context of clarifying the content of the category “public security”] / O. A. Kolotkina // Nauka. Obshchestvo. Gosudarstvo. — 2025. — № 3 (51). — S. 49–58.
7. Ziyadova, D. Z. Sovershenstvovaniye zakonodatel'stva v sfere obespecheniya gosudarstvennoy i natsional'noy bezopasnosti v tsifrovuyu epokhu [Improvement of legislation to enforce state and national security in the digital age] / D. Z. Ziyadova, M. G. Diyeva // Probely v rossiyskom zakonodatel'stve. — 2024. — Tom 17. — № 7. — С. 105–111.
8. Ponomarenko, Ye. V. Obosnovannost' izmeneniy ugolovnogo zakonodatel'stva, kasayushchikhsya otdel'nykh sostavov prestupleniy protiv osnov konstitutsionnogo stroya i bezopasnosti gosudarstva [Justification for amendments to criminal legislation concerning specific offenses against the foundations of the constitutional order and state security] / Ye. V. Ponomarenko, K. O. Kopsheva // Pravovaya politika i pravovaya zhizn'. Pravo. — 2023. — № 1. — S. 121–125.
9. Shkhagapsoyev, Z. L. Aktual'nyye voprosy primeneniya tsifrovyykh tekhnologiy dlya obespecheniya obshchestvennoy bezopasnosti [Current issues regarding the use of digital technologies to ensure public security] / Z. L. Shkhagapsoyev // Probely v rossiyskom zakonodatel'stve. — 2025. — № 18(7). — S. 50–55.
10. Irinin, K. V. Pravovyye mekhanizmy obespecheniya kiberbezopasnosti gosudarstvennykh informatsionnykh sistem v usloviyakh tsifrovizatsii upravleniya [Legal mechanisms for enforcing the cybersecurity of state information systems amidst the digitalization of governance] / K. V. Irinin // Problemy pravovoy i tekhnicheskoy zashchity informatsii. — 2026. — № 13. — S. 50–56.
11. Gir'ko, S. I. Real'nyye shagi k instutualizatsii obshchestvennoy bezopasnosti Rossiyskoy Federatsii [Definite steps toward the institutionalization of public security in the Russian Federation] / S. I. Gir'ko // Nauchnyy portal MVD Rossii. — 2025. — № 1 (69). — S. 33–40.
12. Yagofarova, I. D. Tsifrovoye gosudarstvo kak sreda generatsii gibridnykh ugroz obshchestvennoy bezopasnosti: postanovka problemy [The digital state as an environment for generating hybrid threats to public security: problem statement] / I. D. Yagofarova // Sovremennyye tendentsii razvitiya nauki i mirovogo soobshchestva v epokhu tsifrovizatsii (shifr — MKSTR). Sbornik materialov 4 (0) Mezhdunarodnoy nauchno-prakticheskoy konferentsii. — Moskva, 2026.