Научная статья
УДК 342
https://doi.org/10.33874/2072-9936-2026-0-2-43-55

ОБОСНОВАННЫЙ РИСК В АДМИНИСТРАТИВНО-ДЕЛИКТНОМ ЗАКОНОДАТЕЛЬСТВЕ

Александр Николаевич Кокорев

Всероссийский государственный университет юстиции (РПА Минюста России), 117638, Россия, г. Москва, ул. Азовская, д. 2, корп. 1

rpamucni@gmail.com

Аннотация

В статье рассматривается соотношение института «обоснованного риска» в российском уголовном праве и аналогичной категории административно-деликтного законодательства Содружества Независимых Государств (СНГ) и обосновывается возможность его имплементации в российское законодательство об административной ответственности. Актуальность исследования обусловлена развитием информационных технологий, активно используемых в противоправных целях, и защитой субъектов, противодействующих им, освобождая последних от административной ответственности. Целью работы является внедрение в российское законодательство об административной ответственности «обоснованного риска» как обстоятельства, освобождающего правоприменителя, действующего в целях обеспечения общественного блага, от юридической ответственности. Методологию составили диалектический метод, общенаучные и специально-юридические методы. Полученные выводы свидетельствуют о возможности расширения защитных механизмов в сфере противодействия угрозам в информационной сфере и дальнейшего их развития.

Ключевые слова: обоснованный риск; административно-деликтное законодательство; уголовное право; угрозы; общее благо.

Для цитирования: *Кокорев А. Н.* Обоснованный риск в административно-деликтном законодательстве // Вестник Российской правовой академии. 2026. № 2. С. 43–55. https://doi.org/10.33874/2072-9936-2026-0-2-43-55

Research Article

JUSTIFIED RISK IN ADMINISTRATIVE AND TORT LAW

Alexander N. Kokorev

All-Russian State University of Justice, 2, Bldg. 1 Azovskaia St.,
Moscow, 117638, Russia

rpamucni@gmail.com

Abstract

The article examines the relationship between the institution of "justified risk" in Russian criminal law and the similar category of administrative and tort law in the Commonwealth of Independent States (CIS), and substantiates the possibility of its implementation in Russian legislation on administrative liability. The relevance of the study is due to the development of information technologies, which are actively used for illegal purposes, and the protection of individuals who oppose them, exempting them from administrative liability. The purpose of the work is to introduce the concept of "justified risk" into Russian legislation on administrative liability as a circumstance that exempts a law enforcement officer acting in the interests of the public good from legal responsibility. The methodology includes the use of the dialectical method, general scientific methods, and specific legal methods. The findings suggest the possibility of expanding protective mechanisms in the field of countering threats.

Keywords: reasonable risk; administrative and tort law; criminal law; threats; common good.

For citation: *Kokorev A. N.* Justified Risk in Administrative and Tort Law. *Herald of the Russian Law Academy*, 2026, no. 2, pp. 43–55. (In Russ.) https://doi.org/10.33874/2072-9936-2026-0-2-43-55

Введение

В юридической литературе давно обсуждается вопрос об уголовно-правовой регламентации обоснованного риска в качестве обстоятельства, исключающего преступность деяния. При этом интенсивное развитие информационных технологий и научного прогресса ставят перед обществом и государством, в лице его органов и должностных лиц, а также коммерческих организаций, новые задачи по защите прав и свобод населения страны от противоправных посягательств. Следует отметить, что механизм защиты самих правоприменителей от юридической ответственности при причинении ими вреда охраняемым законом интересам уже давно

выходит за рамки исключительно уголовного права. Так, жизненные обстоятельства и правоприменительная практика ставят перед представительными (законодателями) органами вопросы о закреплении аналогичного института в административно-деликтном законодательстве России. В настоящее время нередки случаи, когда государственные и коммерческие органы и их должностные лица вынуждены прибегать к деятельности, сопряженной с вероятностью причинения ущерба охраняемым нормами административного права интересам физических и юридических лиц, в целях достижения общественно значимой пользы, что по своей сути составляет обстоятельство, исключающее противоправность деяния.

1. Обоснованный риск как обстоятельство, исключающее противоправность деяния, и комплекс мер, связанных с его реализацией

Появление обоснованного риска в уголовном законодательстве как обстоятельства, исключающего деликтность деяния, произошло только в 1996 г. и было продиктовано интенсивным развитием науки и техники, сопряженным с рискованными действиями субъектов общественных отношений и возможностью причинения ими вреда охраняемым законом интересам в целях достижения общественно значимых благ.

При этом, как справедливо отмечает профессор А. В. Наумов, уголовное право не только не должно быть тормозом научного прогресса, но и должно защищать экспериментатора, исключая его ответственность в случаях нарушения им общих оснований уголовной ответственности [1, с. 516].

Однако даже среди исследователей «обоснованного риска» как уголовно-правовой категории, исключающей противоправность деяния, нет единодушия по поводу его юридической природы [2, с. 14] и субъективного состава [3, с. 39] данного правового явления. В то же время все они единодушны в том, что его содержательная основа раскрывается в ст. 41 Уголовного кодекса РФ [4]. Наличие обстоятельств, освобождающих от юридической ответственности, предполагает их расширение в связи с эволюционным ростом технологий и не должно ограничиваться только нормами уголовного права, поскольку риск возможен в любой сфере человеческой деятельности, сопряженной с возможностью причинения вреда. Особенно это проявляется в области *IT*-технологий и дальнейшей информатизации общества.

Стоит подчеркнуть, что отличительной особенностью обоснованного риска является отсутствие в действиях (бездействии) рискующего лица противоправных намерений и его стремление к достижению общего, а не индивидуального блага. Кроме того, данные поведенческие акты, как правило, связаны с профессиональной деятельностью и не нарушают установленного правовой нормой запрета. Таким образом, действия лица происходят в ситуациях неопределенности, а риск обоснован и оправдан общественной необходимостью.

В отличие от крайней необходимости, связанной с предотвращением неминуемой опасности, «обоснованный риск» направлен на защиту действий делинквента, связанных с достижением общественно полезной цели, даже при отсутствии явной угрозы охраняемым нормами права интересам общества и личности.

Как отмечает ряд авторов, подобные угрозы могут возникнуть при научно-изыскательской деятельности, в сфере защиты инфраструктуры, в том числе информационной, персональных данных населения, и иных неординарных ситуациях [5, с. 321–331].

Так, по данным правоохранительных органов и ряда кредитных организаций, количество киберпреступлений (в основном мошенничества) за последние три года возросло на 27% [6], а причиненный только за пять месяцев 2025 г. ущерб российским гражданам составил 81 млрд руб., что выше аналогичного показателя прошлого года [7].

По данным Банка России, основной массив кибермошенничества приходится на телефонные звонки и *SMS*-сообщения (45,6%), атаки через мессенджеры (15,7%), сообщения в социальных сетях (10,3%), письма на электронную почту (7,7%), получение доступа к аккаунту на портале «Госуслуги» (7%) и др. [8].

При этом созданная Роскомнадзором на основе технических средств противодействия угрозам (ТСПУ) и действующая в России с начала 2024 г. Национальная система противодействия *DDoS*-атакам, направленная в первую очередь на защиту критической информационной инфраструктуры российского государственного сектора (финансовые, транспортные, энергетические компании, средства массовой информации (СМИ), операторы связи и госструктуры), не удовлетворяет потребностям общества в информационной безопасности различного рода информационных баз данных и их ресурсов.

Сами *DDoS*-атаки, как отмечают специалисты в сфере информационной безопасности, представляют собой один из весьма грозных методов противоправного воздействия на интернет-ресурсы (сайты или онлайн-сервисы), способные буквально остановить работу компании, кредитной организации, торговой площадки и причинить им огромные убытки. Их целью является перегрузка информационной системы посредством направления с зараженных устройств (компьютеров, серверов, *IT*-гаджетов) многочисленных запросов на целевой ресурс. Этот процесс носит лавинообразный характер, что приводит к замедлению работы сайта / онлайн-сервиса или его блокировке, а пользователь не может получить к нему доступа. Так, по данным одной из крупнейших компаний по кибербезопасности, *Cisco Talos Intelligence Group*, начало 2023 г. ознаменовалось для России ростом отправки спам-писем, количество которых в день превышало 7 млрд, что позволило ей занять шестое место в мире по данному критерию киберпреступности [9].

Чаще других *DDoS*-атакам подвергаются сайты государственных учреждений, крупных корпораций, организаций здравоохранения, игровых сервисов, местных и региональных СМИ, онлайн-кинотеатров, кредитных организаций, хостинг-провайдеров. При этом, как отмечают многие исследователи информационной безопасности, перечень объектов незаконной деятельности из года в год остается неизменным, что свидетельствует о постоянстве киберпреступности.

Рассматривая нормативно-правовую базу технической защиты критической информационной инфраструктуры, следует отметить, что она состоит из законодательных и подзаконных актов. Так, на уровне Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [10]

определяются государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы страны, реестр значимых объектов цифровой инфраструктуры, субъекты государственной власти в области обеспечения безопасности данной сферы, их права и обязанности, а также другие вопросы противодействия компьютерным атакам.

Следует отметить, что применительно к государственным информационным системам в качестве органа, уполномоченного на обеспечение безопасности критической информационной инфраструктуры Российской Федерации, выступает Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [11]. Она реализует следующую систему организационных и технических мер защиты информации в зависимости от угроз безопасности информационным ресурсам:

«а) идентификация и аутентификация;

б) управление доступом;

в) регистрация событий безопасности;

г) защита виртуализации и облачных вычислений;

д) защита технологий контейнерных сред и их оркестрации;

е) защита сервисов электронной почты;

ж) защита веб-технологий;

з) защита программных интерфейсов взаимодействия приложений;

и) защита конечных устройств;

к) защита мобильных устройств;

л) защита технологий интернета вещей;

м) защита точек беспроводного доступа;

н) антивирусная защита;

о) обнаружение и предотвращение вторжений на сетевом уровне;

п) сегментация и межсетевое экранирование;

р) защита от компьютерных атак, направленных на отказ в обслуживании;

с) защита каналов передачи данных и сетевого взаимодействия» [12].

Однако, как было отмечено многочисленными решениями судебных [13; 14] и контрольно-надзорных органов [15], обеспечение информационной безопасности и надежности функционирования программных и технических средств при оказании государственных и коммерческих услуг является обязанностью оператора или обладателя информации.

При этом оператор (обладатель информации), с учетом опасности, создаваемой для информационной среды при обработке и хранении информации, уязвимостей программного обеспечения, программно-аппаратных средств, содержащихся в банке данных угроз безопасности информации ФСТЭК России [16], должен обеспечивать ее защиту на всех этапах преобразования данных в информационных системах.

Реализация указанной задачи преследует цели:

«а) недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации;

б) недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации» [17].

2. Административно-правовые средства противодействия угрозам в информационной сфере и механизм защиты правоприменителей

Рассматривая сферу действия российской системы технической защиты от противоправных посягательств в информационной сфере, следует отметить, что она распространила свое действие на 655 субъектов государственного и частного сектора [18]. В то время как только в финансовой [19] и транспортной сферах [20] их количество достигает порядка 40 тыс., а по данным Роскомнадзора, на октябрь 2025 г. в реестре лицензий в области связи России содержится более 24 тыс. действующих организаций, оказывающих данные услуги [21].

Представленные статистические данные свидетельствуют о недостаточности только технической защиты прав и свобод физических и юридических лиц в информационной сфере. Кроме того, в соответствии с заявлением директора по стратегическим альянсам и взаимодействию с органами государственной власти группы компаний «Гарда» Павла Кузнецова средствами информационной защиты обладает лишь треть компаний. В то время как основными субъектами, подключаемыми к системе технических средств противодействия информационным угрозам, должны быть организации и компании, чья деятельность может негативно отразиться на уровне жизни граждан и наиболее важных отраслях российской промышленности [22].

В то же время основным способом защиты с использованием системы ТСПУ является блокировка запрещенного в России контента и борьба с вредоносным трафиком. Однако, как отмечает начальник Управления Президента РФ по развитию ИКТ и инфраструктуры связи Татьяна Матвеева, «работает указанная система только по отслеживанию паттернов вредоносных пакетов в трафике, то есть откуда он идет, есть ли нетипичные IP-адреса и т.д. Если эти показатели меняются, то система становится неэффективна» [23], а блокировка атак на пул *IP*-адресов возлагается на самих владельцев информационных ресурсов.

Более того, многие исследователи отмечают, что с учетом постоянного развития технологий, используемых в противоправных целях, в настоящий период технический потенциал противодействия им недостаточен, а нормативно-правовая база требует совершенствования. Это касается не только уголовно-правовых средств воздействия и защиты, но и включения в арсенал административно-деликтных способов реагирования [24] с применением институтов защиты от ответственности правоприменителей при причинении ими вреда в целях обеспечения общезначимых благ.

Примеры таких способов административного реагирования можно обнаружить на постсоветском пространстве как в законодательстве, так и в правоприменительной практике разнообразных органов Содружества Независимых Государств (СНГ). Например, анализ административно-деликтного законодательства ряда государств СНГ свидетельствует, что институт «обоснованного риска» как об-

стоятельство, освобождающее от административной ответственности, функционирует на территории Республики Таджикистан [25], Республики Туркменистан [26], Республики Беларусь [27] и Республики Молдова [28] с 2000-х гг. XX в. Для него характерны следующие особенности:

Во-первых, цель применения «обоснованного риска» – достижение общественного блага при причинении вреда охраняемым законом интересам.

Во-вторых, социально значимая цель не может быть достигнута без действий или бездействия рисковавшего, сопряженных с риском (основанным на достижениях науки и опыта), и без принятия им необходимых мер для предотвращения такого вреда.

В-третьих, риск не должен быть сопряжен с угрозой жизни и здоровью индивида, созданием условий социального и экологического бедствия (катастрофы), т.е. не должен посягать на охраняемые нормами уголовного права интересы личности, общества и государства.

Таким образом, риск обоснован и оправдан общественной необходимостью и ее значимостью. Он исключает административную ответственность, расширяя тем самым перечень таких обстоятельств (наряду с институтами крайней необходимости и невменяемости). Анализ приведенных выше особенностей «обоснованного риска», сформировавшегося в административно-деликтном законодательстве и правоприменительной практике ряда стран СНГ, по своей содержательной сущности близок аналогичному институту, содержащемуся в российском уголовном праве. При этом он направлен на защиту действий (бездействия) делинквента, стремящегося к достижению общественно полезной цели, даже при отсутствии явной угрозы охраняемым административно-правовой нормой личным и общественным интересам.

Указанные обстоятельства позволяют осуществить имплементацию норм законодательства об административных проступках ряда государств СНГ в Кодекс РФ об административных правонарушениях (далее – КоАП РФ), дополнив его ст. 2.7.1 «Обоснованный риск» следующего содержания: «Не является административным правонарушением причинение вреда охраняемым законом ценностям лицом при обоснованном риске для достижения общественно полезной цели, если она не могла быть достигнута иным способом и не сопряжена с угрозой жизни и здоровью людей, созданием условий социального и экологического бедствия (катастрофы)».

Как отмечает ряд авторов, угрозы, на пресечение которых направлен институт «обоснованного риска», представляют собой не какие-то эфемерные ситуации, а реальные поведенческие акты, являющиеся выражением внешней противоправной деятельности как отдельных лиц, так и преступных групп.

Согласно данным крупного интернет-провайдера в лице Центризбиркома (ЦИК) работа его серверов в период избирательных кампаний на протяжении длительного времени, начиная с ввода в действие в 2000 г. государственной автоматизированной системы (ГАС) «Выборы», подвергается мощным кибератакам (*DDoS*). Эти атаки способны парализовать работу серверов и создают реальную возможность потери персональных данных миллионов пользователей.

Согласно статистическим данным, приведенным председателем ЦИК Эллой Панфиловой, цифровая платформа ГАС «Выборы» в 2024 г. подвергалась вирусным ата-

кам 398 раз, в то время как в 2023 г. их количество составляло 282, а в 2022 г. – 275 [29]. Эта информация от органа, ответственного за подготовку и проведение выборов всех уровней на территории России, фиксирует рост противоправных посягательств в сфере избирательных прав граждан, в основном с *IP*-адресов недружественных государств. Всего в 2024 г. Центризбиркомом было зафиксировано более 24 млн потенциально вредоносных запросов на ресурсы дистанционного электронного голосования [29], а в ходе выборов в Единый день голосования – 2025 было совершено около 290 тыс. хакерских атак на портал ЦИК РФ [30].

В то же время следует отметить, что в правоприменительной практике различных органов, связанных с формированием и работой с информационными ресурсами как за рубежом, так и на территории России, применяются средства и приемы противодействия потенциальным угрозам в киберсфере. Эти действия регламентируются нормами административного законодательства, а причиняемый при их устранении вред – административно-деликтным законодательством.

Например, при мощной кибератаке (*DDoS*-атаке) на крупного интернет-провайдера, когда под угрозой оказывается работа его серверов или потеря персональных данных пользователей, а иногда и невозможность проведения торгов или отправки заявки на участие в них (в случае с электронными площадками), его служба информационной безопасности принимает решение о временном отключении всего внешнего трафика и установлении фильтрации доступа для всех пользователей.

Таким образом, совершаются действия, формально подпадающие под состав таких административных деликтов (правонарушений), как нарушение оказания услуг связи (ст. 13.42 КоАП РФ) или неправомерное ограничение доступа к информации (ч. 2 ст. 13.27 КоАП РФ), нарушение операторами электронных площадок требований по обеспечению непрерывности проведения закупок в электронной форме, надежности функционирования программно-аппаратных средств, равного доступа участников к участию в электронных торгах и неизменности подписанных усиленной квалифицированной электронной подписью документов (ч. 2 ст. 7.30.6 КоАП РФ). Следовательно, отключение трафика является единственно возможным способом своевременного пресечения кибератаки и утраты данных клиентов, т.е. ограничение доступа к интернет-услугам обеспечивает безопасность информационных ресурсов и минимизирует ущерб для пользователей. Однако подобные действия со стороны оператора электронной площадки, сопряженные с переносом аукциона и уведомлением всех его участников, требуют от последнего истребования специального разрешения у контрольно-надзорных органов на проведение подобных действий и во всех случаях трактуются ими в качестве основания для привлечения к административной ответственности оператора электронной площадки [31; 32]. Необходимо отметить, что судебная практика, связанная с ситуациями, когда суды встают на сторону оператора электронной площадки или участника электронных торгов в связи с *DDoS*-атаками, крайне незначительна [33].

Заключение

Резюмируя вышеизложенное, можно констатировать, что в результате рискованных действий сотрудников службы информационной безопасности, преследующих общественно значимые цели, наличие института «обоснованного риска» в российском административно-деликтном законодательстве исключало бы их привлечение к административной ответственности.

Данные обстоятельства свидетельствуют о необходимости имплементации в КоАП РФ института «обоснованного риска», содержащегося в административно-деликтном законодательстве ряда государств СНГ, как еще одного обстоятельства, освобождающего правоприменителя от административного наказания ввиду направленности его поведения на достижение общественно значимого блага и закрепления сформировавшейся правоприменительной практики.

Пристатейный библиографический список

1. *Наумов А. В.* Российское уголовное право. Общая часть : курс лекций. 6-е изд., перераб. и доп. М. : Проспект, 2017.

2. *Бабурин В. В.* Квалификация уголовно-правового риска : монография. М. : Илекса, 2006.

3. *Попов А. Н.* Обстоятельства, исключающие преступность деяния. СПб., 1998.

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

5. *Рарог А. И., Понятовская Т. Г.* Медицинский риск в уголовном праве // Всероссийский криминологический журнал. 2021. Т. 15. № 3.

6. МВД: 433 млн рублей ежедневно уходит хакерам // SecurityLab.ru : сайт. URL: https://www.securitylab.ru/news/551833.php (дата обращения: 02.08.2025).

7. В МВД оценили ущерб от IT-преступлений // РИА Новости : сайт. URL: https://ria.ru/20250618/it-prestupleniya-2023640268.html (дата обращения: 02.08.2025).

8. Кибермошенничество: портрет пострадавшего // Банк России : сайт. URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 02.08.2025).

9. *Катаева В., Поляков Д.* Россия – одна из стран с очень высоким уровнем киберугроз // Если быть точным : сайт. URL: https://tochno.st/materials/rossiia-odna-iz-stran-s-ocen-vysokim-urovnem-kiberugroz-no-do-policii-doxodit-mense-poloviny-prestuplenii-i-tolko-cetvert-iz-nix-raskryvaiut (дата обращения: 02.08.2025).

10. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

11. Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» // СЗ РФ. 2004. № 34. Ст. 3541.

12. Приказ ФСТЭК от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государс-

твенных унитарных предприятий, государственных учреждений» (п. 61) // СПС «КонсультантПлюс».

13. Постановление Арбитражного суда Московского округа от 19 марта 2024 г. № Ф05-2532/2024 по делу № А40-111179/2023.

14. Постановление Арбитражного суда Западно-Сибирского округа от 17 марта 2023 г. № Ф04-468/2023 по делу № А75-7483/2022.

15. Постановление ФАС России от 19 февраля 2024 г. по делу № 28/04/7.30-181/2024.

16. URL: http://www.bdu.fstec.ru/ (дата обращения: 02.08.2025).

17. Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» // СПС «КонсультантПлюс».

18. Национальная система противодействия DDoS-атакам (НСПА) // Радиоцентр : сайт. URL: https://www.radio-center.ru/blog/nacionalnaya-sistema-protivodeystviya-ddos-atakam-nspa (дата обращения: 02.08.2025).

19. По данным Банка России, список кредитных организаций, зарегистрированных и функционирующих на территории Российской Федерации в 2025 году состоит из 1879 компаний банковского сектора // Банк России : сайт. URL: https://cbr.ru/banking_sector/credit/FullCoList/ (дата обращения: 02.08.2025).

20. В соответствии с Базой данных транспортных компаний России на сентябрь 2025 года в ней состояло 36 200 компаний, осуществляющих грузоперевозки // Парсик : сайт. URL: https://www.parsic.ru/db-transport.html (дата обращения: 02.08.2025).

21. По данным Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций // Роскомнадзор : сайт. URL: https://rkn.gov.ru/activity/connection/register/license/ (дата обращения: 02.08.2025).

22. Ключи от базы: решения для защиты данных есть только у трети компаний // Известия : сайт. URL: https://iz.ru/1918174/valeriia-mishina/klychi-ot-bazi-resheniia-dlia-zashchity-dannykh-est-tolko-u-treti-kompanii (дата обращения: 02.08.2025).

23. К системе по борьбе с DDoS-атаками на базе ТСПУ подключат 160 субъектов // Kommersant : сайт. URL: https://www.kommersant.ru/doc/6323505 (дата обращения: 02.08.2025).

24. *Гекк Б. В.* Борьба с киберпреступностью в РФ: анализ явления и законодательные меры противодействия // Молодой ученый. 2024. № 8 (507).

25. Кодекс Республики Таджикистан об административных правонарушениях от 31 декабря 2008 г. № 455 (ст. 21) // Ахбори Маджлиси Оли Республики Таджикистан. 2008. № 12 (ч. 1). Ст. 990.

26. Кодекс Республики Туркменистан об административных правонарушениях (ст. 36) // Ведомости Меджлиса Туркменистана. 2013. № 3. Ст. 52.

27. Кодекс Республики Беларусь об административных правонарушениях от 6 января 2021 г. № 91-З (ст. 3.4) // Национальный правовой Интернет-портал Республики Беларусь. 2021. № 2/2811.

28. Кодекс Республики Молдова о правонарушениях от 24 октября 2008 г. № 218-XVI (ст. 24) // Официальный монитор Республики Молдова. 2009. № 3-6. Ст. 15.

29. Интернет-ресурсы ЦИК за год подверглись 24 млн вредоносных запросов из-за рубежа // Ведомости : сайт. URL: https://www.vedomosti.ru/politics/articles/2025/04/02/1101975-internet-resursi-tsik-podverglis (дата обращения: 02.08.2025).

30. Памфилова заявила о 290 тысячах атак на ресурсы ЦИК // РИА Новости : сайт. URL: https://ria.ru/20250914/pamfilova-2041796814.html (дата обращения: 02.08.2025).

31. Решение ФАС России от 15 ноября 2017 г. по делу № К-1579/17 // СПС «КонсультантПлюс».

32. Решение ФАС России от 13 октября 2017 г. по делу № К-1339/17 // СПС «КонсультантПлюс».

33. Решение Административного суда Ростовской области от 28 апреля 2023 г. по делу № А53-30836/2022 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/arbitral/doc/CEDqGMher0Zr/ (дата обращения: 02.08.2025).

References

1. *Naumov A. V.* Russian Criminal Law. General Part: Lecture Course. 6th ed. Moscow: Prospekt, 2017. (In Russ.)

2. *Baburin V. V.* Qualification of Criminal-Legal Risk: Monograph. Moscow: Ileksa, 2006. (In Russ.)

3. *Popov A. N.* Circumstances Excluding the Criminality of an Act. St. Petersburg, 1998. (In Russ.)

4. Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ. *Collection of Legislation of the Russian Federation*, 1996, no. 25, art. 2954. (In Russ.)

5. *Rarog A. I., Poniatovskaia T. G.* Medical Risk in Criminal Law. *All-Russian Criminological Journal*, 2021, vol. 15, no. 3. (In Russ.)

6. Ministry of Internal Affairs: 433 Million Rubles Go to Hackers Daily. URL: https://www.securitylab.ru/news/551833.php (date of the application: 02.08.2025). (In Russ.)

7. The Ministry of Internal Affairs Assessed the Damage from IT Crimes. URL: https://ria.ru/20250618/it-prestupleniya-2023640268.html (date of the application: 02.08.2025). (In Russ.)

8. Cyberfraud: Portrait of the Victim. URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (date of the application: 02.08.2025). (In Russ.)

9. *Kataeva V., Poliakov D.* Russia Is One of the Countries with a Very High Level of Cyber Threats. URL: https://tochno.st/materials/rossiia-odna-iz-stran-s-ocen-vysokim-urovnem-kiberugroz-no-do-policii-doxodit-mense-poloviny-prescrimplenii-i-tolko-cetvert-iz-nix-raskryvaiut (date of the application: 02.08.2025). (In Russ.)

10. Federal Law of July 26, 2017 No. 187-FZ "On the Security of Critical Information Infrastructure of the Russian Federation" (SPS "ConsultantPlus"). (In Russ.)

11. Decree of the President of the Russian Federation of August 16, 2004 No. 1085 "Questions of the Federal Service for Technical and Export Control". *Collection of Legislation of the Russian Federation*, 2004, no. 34, art. 3541. (In Russ.)

12. Order of the FSTEC of April 11, 2025 No. 117 "On Approval of the Requirements for the Protection of Information Contained in State Information Systems, Other Information Systems of State Bodies, State Unitary Enterprises, and State Institutions" (clause 61) (SPS "ConsultantPlus"). (In Russ.)

13. Resolution of the Arbitration Court of the Moscow District of March 19, 2024 No. F05-2532/2024 in Case No. A40-111179/2023. (In Russ.)

14. Resolution of the Arbitration Court of the West Siberian District of March 17, 2023 No. F04-468/2023 in Case No. A75-7483/2022. (In Russ.)

15. Resolution of the FAS Russia of February 19, 2024 in Case No. 28/04/7.30-181/2024. (In Russ.)

16. URL: http://www.bdu.fstec.ru/ (date of the application: 02.08.2025). (In Russ.)

17. Order of the FSTEC of Russia of April 11, 2025 No. 117 "On Approval of the Requirements for the Protection of Information Contained in State Information Systems, Other Information Systems of State Bodies, State Unitary Enterprises, and State Institutions" (SPS "ConsultantPlus"). (In Russ.)

18. National System for Combating DDoS Attacks (NSPA). URL: https://www.radio-center.ru/blog/nacionalnaya-sistema-protivodeystviya-ddos-atakam-nspa (date of the application: 02.08.2025). (In Russ.)

19. According to the Bank of Russia, the List of Credit Institutions Registered and Operating in the Russian Federation in 2025 Consists of 1,879 Companies in the Banking Sector. URL: https://cbr.ru/banking_sector/credit/FullCoList/ (date of the application: 02.08.2025). (In Russ.)

20. According to the Database of Transport Companies of Russia, as of September 2025, It Included 36,200 Companies Engaged in Cargo Transportation. URL: https://www.parsic.ru/db-transport.html (date of the application: 02.08.2025). (In Russ.)

21. According to the Federal Service for Supervision of Communications, Information Technology, and Mass Media. URL: https://rkn.gov.ru/activity/connection/register/license/ (date of the application: 02.08.2025). (In Russ.)

22. Keys to the Database: Only a Third of Companies Have Data Protection Solutions. URL: https://iz.ru/1918174/valeriia-mishina/klychi-ot-bazi-resheniia-dlia-zashchity-dannykh-est-tolko-u-treti-kompanii (date of the application: 02.08.2025). (In Russ.)

23. 160 Entities Will Be Connected to the DDoS Attack Prevention System Based on the TSPU. URL: https://www.kommersant.ru/doc/6323505 (date of the application: 02.08.2025). (In Russ.)

24. *Gekk B. V.* The Fight Against Cybercrime in the Russian Federation: Analysis of the Phenomenon and Legislative Countermeasures. *Young Scientist*, 2024, no. 8 (507). (In Russ.)

25. Code of the Republic of Tajikistan on Administrative Offenses of December 31, 2008 No. 455 (Article 21). *Akhbori Majlisi Oli of the Republic of Tajikistan*, 2008, no. 12 (part 1), art. 990. (In Russ.)

26. Code of the Republic of Turkmenistan on Administrative Offenses (Article 36). *Bulletin of the Mejlis of Turkmenistan*, 2013, no. 3, art. 52. (In Russ.)

27. Code of the Republic of Belarus on Administrative Offenses of January 6, 2021 No. 91-3 (Article 3.4). *National Legal Internet Portal of the Republic of Belarus*, 2021, no. 2/2811. (In Russ.)

28. Code of the Republic of Moldova on Offenses of October 24, 2008 No. 218-XVI (Article 24). *Official Monitor of the Republic of Moldova*, 2009, no. 3-6, art. 15. (In Russ.)

29. The Central Election Commission's Internet Resources Were Subject to 24 Million Malicious Requests from Abroad in a Year. URL: https://www.vedomosti.ru/politics/articles/2025/04/02/1101975-internet-resursi-tsik-podverglis (date of the application: 02.08.2025). (In Russ.)

30. Pamfilova Reported 290 Thousand Attacks on the Central Election Commission's Resources. URL: https://ria.ru/20250914/pamfilova-2041796814.html (date of the application: 02.08.2025). (In Russ.)

31. Decision of the FAS Russia of November 15, 2017 in Case No. K-1579/17 (SPS "ConsultantPlus"). (In Russ.)

32. Decision of the FAS Russia of October 13, 2017 in Case No. K-1339/17 (SPS "ConsultantPlus"). (In Russ.)

33. Decision of the Administrative Court of the Rostov Region of April 28, 2023 in Case No. A53-30836/2022. URL: https://sudact.ru/arbitral/doc/CEDqGMher0Zr/ (date of the application: 02.08.2025). (In Russ.)

Сведения об авторе:

А. Н. Кокорев – кандидат юридических наук, доцент.

Information about the author:

A. N. Kokorev – PhD in Law, Associate Professor.

Статья поступила в редакцию 03.09.2025; одобрена после рецензирования 03.11.2025; принята к публикации 20.03.2026.

The article was submitted to the editorial office 03.09.2025; approved after reviewing 03.11.2025; accepted for publication 20.03.2026.