

Рускевич
Евгений Александрович

Russkevich
Evgeny A.



профессор кафедры уголовного
права Московского государственного
юридического университета
имени О.Е. Кутафина (МГЮА),
доктор юридических наук, доцент

Professor of the Department of Criminal
Law of the Kutafin Moscow State
Law University (MSAL),
Dr. Sci. (Law), Associate Professor

Статья поступила
в редакцию:
30.04.2026

одобрена после
рецензирования
26.05.2026

принята
к публикации
15.06.2026

Москва
Российская Федерация

Moscow
Russian Federation

✉ russkevich@mail.ru
SPIN-код (РИНЦ) 5725-1289
ORCID ID: <https://orcid.org/0000-0003-4587-8258>

УДК: 343.3.7

О криминализации обеспечения функционирования цифровой инфраструктуры киберпреступности

On the criminalization of the functioning of digital infrastructure for cybercrime

Аннотация. Актуальность. Статья посвящена теоретическому анализу последних изменений уголовного законодательства об ответственности за преступления в сфере компьютерной информации (ст. 274³–274⁵ УК РФ). Реализованная законотворческая инициатива отражает новый курс отечественной уголовной политики, направленный на противодействие обеспечению функционирования цифровой инфраструктуры киберпреступности.

Целью статьи является критическое осмысление новелл главы 28 УК РФ (ст. 274³–274⁵) и анализ особенностей конструирования данных норм, в том числе их криминообразующих признаков, характеризующихся формальной неопределенностью.

Выводы. Установлено, что новые уголовно-правовые запреты в сфере компьютерной информации имеют важное превентивное значение, однако характеризуются рядом недостатков законодательной техники. Доказано, что ключевым риском будущего правоприменения является расширительное толкование нормы об участии в незаконной передаче абонентских номеров (ч. 2 ст. 274⁴ УК РФ) в тех случаях, когда корыстный сбыт осуществляется при отсутствии признаков организованной деятельности.

Ключевые слова: киберпреступность, цифровая инфраструктура, криминализация, противодействие преступлениям, предупреждение преступлений.

Abstract. Relevance. This article provides a theoretical analysis of the latest amendments to criminal legislation regulating liability for crimes involving computer information (Articles 274³–274⁵ of the Criminal Code of the Russian Federation). This legislative initiative reflects a new course in Russian criminal policy aimed at countering the functioning of the digital infrastructure of cybercrime.

The purpose of this article is to critically examine the new provisions of Chapter 28 of the Criminal Code of the Russian Federation (Arts. 274³–274⁵) and analyze the legislative design of these norms, including their crime-constituting elements characterized by formal uncertainty.

Conclusions. It has been established that the new criminal law prohibitions in the field of computer information possess significant preventive value but are characterized by a number of shortcomings in legislative technique. The study demonstrates that the primary risk for future law enforcement lies in the expansive interpretation of the provision concerning participation in the illegal transfer of subscriber numbers (Part 2, Art. 274⁴ of the Criminal Code of the Russian Federation) in cases where for-profit distribution is carried out in the absence of signs of organized activity.

Keywords: cybercrime; digital infrastructure; criminalization; crime prevention; crime prevention.

Для цитирования: Русскевич Е.А. О криминализации обеспечения функционирования цифровой инфраструктуры киберпреступности // Научные исследования преступления и наказания. № 2 (6). 2026. С. 32–39.

For citation: Russkevich Evgeny A. On the criminalization of the functioning of digital infrastructure for cybercrime // Scientific Crime and Punishment Research Journal. No 2 (6). 2026. P. 32–39.

Введение. Последовательный рост преступлений, совершаемых с использованием информационно-коммуникационных технологий, уже на протяжении длительного времени является одной из самых обсуждаемых тем в отечественной юридической науке [1, 2, 3, 4]. Кажется бы, чтобы его объяснить, достаточно посмотреть по сторонам и убедиться в очевидном: насколько неотрывно современный человек связан с цифровыми устройствами и виртуальной средой. Мысль эта многократно была раскрыта в литературе, причем не только юридической. Спорить с тем, что «компьютеризация жизни» предопределила и «компьютеризаб

Однако это своего рода эволюционный уровень объяснения, который, надо честно признать, мало что дает для выработки практических решений. Действительно, не станем же мы отстаивать необходимость отказа от дальнейшего развития науки и техники, добиваться приостановки всех инновационных проектов, ссылаясь на то, что они потенциально таят угрозу появления новых преступных посягательств на охраняемые законом интересы личности, общества или государства? Человек всегда выбирает прогресс, движение от неведения к знанию, от энтропии к определенности, от хаоса к порядку. Прогресс всегда имеет свою оборотную – негативную – сторону, и человек исторически всегда платит эту цену.

Смирившись с эволюционной предопределенностью цифровых изменений в состоянии и динамике преступности, в прикладном смысле важно заняться осмыслением того, почему те или иные технологии приводят к конкретным негативным колебаниям ее количественно-качественных характеристик. И здесь следует обратить внимание на многое.

Прежде всего до настоящего времени пользователь практически любого цифрового сервиса не может самостоятельно выбирать уровень своего риска с точки зрения распространенных угроз информационной безопасности. У нас под рукой множество интегрированных разработчиком настроек, касающихся получения тех или иных услуг или приобретения товаров, но почти ничего – в части осознанного контроля за своей цифровой безопасностью (положительные исключения крайне редки).

В причинном комплексе цифровых преступлений нельзя обойти и тот фактор, который условно может быть обозначен как *проблема противопоставления стоимости технологии и безопасности*. Безопасность, в том числе компьютерная, стоит дорого. В свою очередь бизнес предсказуемо стремится к снижению издержек и повышению доходности экономической деятельности. Последнее нельзя поставить в укор хозяйствующим субъектам, поскольку такова сама природа предпринимательства. Однако такая экономия негативно сказывается на защищенности пользователей от действий киберпреступников.

Следует обратить внимание и на то, что в предупреждении цифровой преступности значительную роль играют организационно-технические либо сугубо технические составляющие [5, 6]. Предотвращение неправомерного воздействия на компьютерную информацию и компоненты информационно-коммуникационной инфраструктуры прежде всего реализуется за счет разработки и внедрения механизмов программно-технической защиты, в том числе от небрежного поведения субъектов, допущенных к эксплуатации компьютерного оборудования. В данном отношении крайне важным представляется обеспечение неукоснительного соблюдения установленных стандартов информационной безопасности. Известно, что далеко не все организации в силу тех или иных причин стремятся осуществлять свою деятельность на уровне последних стандартов киберзащищенности.

С изрядным запозданием, но законодатель все же обратил внимание еще на один важный компонент в предупреждении преступлений, совершаемых с использованием

информационно-коммуникационных технологий, – собственно на ее *цифровую инфраструктуру*. IT-преступность по своей природе технологична. Это означает, что механизм преступного поведения виновного предполагает операционное взаимодействие с компьютерными технологиями. Характер такого взаимодействия, конечно же, может быть разным. И тут возможны варианты от подготовки и проведения сложных и высокотехнологичных компьютерных атак на хорошо защищенные информационные ресурсы до вполне банального дистанционного мошенничества с использованием современных средств коммуникации. Вместе с тем как в первом, так и во втором случае злоумышленник всегда использует технологии, а успешность его действий во многом предопределена качеством используемых цифровых инструментов. Таким образом, мысль о том, что эффективная стратегия противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, должна предполагать наряду с остальным и комплексное воздействие на практику обеспечения функционирования ее инфраструктуры, «лежит на поверхности».

До последнего времени отечественный уголовный закон в этом отношении содержал довольно мало: положения об ответственности за создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и уголовно-правовой запрет в отношении незаконного оборота специальных технических средств, предназначенных для негласного получения информации (ст. 138¹ УК РФ). Своего рода прологом к этому стали изменения, внесенные 30.11.2024 в Уголовный кодекс Российской Федерации¹, которыми глава 28 УК РФ была дополнена специальной нормой об ответственности за незаконные действия в отношении персональных данных в компьютерной форме (ст. 272¹ УК РФ). Поправки, внесенные Федеральным законом от 31.07.2025 № 282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»², явились уже логическим продолжением выбранного курса уголовной политики.

Обсуждение и результаты. Примечательно, что изначально законопроект не содержал предложений по дополнению главы 28 УК РФ соответствующими нормами. Именно поэтому в пояснительной записке нет объяснения самой необходимости закрепления ст. 274³, 274⁴, 274⁵ УК РФ. Поскольку дополнения были внесены только ко второму чтению (инициатором выступало Правительство Российской Федерации), Верховный Суд Российской Федерации не имел возможности рассмотреть их и дать отзыв. Само по себе это, пожалуй, является поводом для повышенного внимания к внесенным изменениям.

Функционал данных уголовно-правовых инструментов заключается в установлении ответственности за совершение действий, которые, по сути, направлены на создание условий для совершения преступлений в сфере информационной безопасности, а также многих иных преступлений, совершаемых с использованием информационно-коммуникационных технологий (конечно же, здесь прежде всего нужно говорить о дистанционных хищениях). Иными словами, мы имеем дело с дополнением уголовного закона классическими нормами с двойной превенцией.

Статья 274³ УК РФ устанавливает, что деяние заключается в незаконном использовании абонентского терминала пропуска трафика или виртуальной телефонной станции. Содержание данного бланкетного признака прежде всего отсылает к п. 9 ст. 44 Федерального закона Российской Федерации от 07.07.2003 № 126-ФЗ «О связи»³, в соответствии с которой использование абонентских терминалов пропуска трафика, виртуальных телефонных станций с нарушением требований, установленных настоящим законом и (или) правилами

¹ О внесении изменений в Уголовный кодекс Российской Федерации : федеральный закон от 30.11.2024 № 421-ФЗ // Доступ из СПС «КонсультантПлюс».

² О внесении изменений в отдельные законодательные акты Российской Федерации : федеральный закон от 31.07.2025 № 282-ФЗ // Доступ из СПС «КонсультантПлюс».

³ О связи : федеральный закон от 07.07.2003 № 126-ФЗ // Доступ из СПС «КонсультантПлюс».

оказания услуг связи, не допускается. Норма отсылает и к другим документам: постановлению Правительства Российской Федерации от 31.12.2021 № 2607 (ред. от 30.09.2023) «Об утверждении Правил оказания телематических услуг связи»⁴, постановлению Правительства Российской Федерации от 31.12.2021 № 2606 (ред. от 26.12.2024) «Об утверждении Правил оказания услуг связи по передаче данных»⁵, постановлению Правительства Российской Федерации от 30.12.2024 № 1994 (ред. от 31.07.2025) «Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте-физическом лице»⁶ и др.

Криминообразующими признаками преступления, предусмотренного ст. 274³ УК РФ, названы альтернативно: цель совершения другого преступления и тяжкие последствия. Такая модель криминализации сама по себе вызывает вопросы, поскольку в один ряд поставлены принципиально разные критерии – специальная цель и тяжкие последствия. Кроме того, в отличие от ст. 274⁴ и 274⁵ УК РФ отсутствует указание на корыстные побуждения, что также требует своего осмысления. Не секрет, что подавляющее большинство выявляемых случаев незаконного использования сим-боксов или виртуальных станций сопряжены с получением такими лицами вознаграждения за свою деятельность. В реализованном решении правоприменителю необходимо устанавливать и доказывать именно цель на совершение другого преступления либо наступление тяжких последствий. Такие лица, по сути, никогда не стремятся незаконно использовать узел связи именно для совершения другого преступления. Их цель – получение дохода от своей деятельности.

Установление же причинно-следственной связи с тяжкими последствиями в ст. 274³ УК РФ, думается, представляет собой почти неосуществимую задачу. Деятельность незаконного узла связи сама по себе причинить такие последствия не может. То есть, если причинная зависимость и будет установлена, то всегда опосредованно и весьма отдаленно – через противоправные действия третьих лиц, которые пользовались услугами такого узла связи. И здесь возникает вероятность того, что применение указанной нормы именно в модели материального состава с тяжкими последствиями будет всегда балансировать на грани объективного вменения.

С учетом выделения криминообразующего признака в виде специальной цели совершения иного преступления следует сделать вывод, что все новеллы главы 28 УК РФ, введенные в 2025 году, в этой части представляют собой формы криминализации содействия преступной деятельности без признаков соучастия. При этом если указанные деяния имели место при наличии соучастия в другом преступлении, то ст.ст. 274³–274⁵ УК РФ должны применяться по совокупности.

В связи с этим дискуссионным представляется высказанное в литературе суждение, что указание в диспозиции ч. 1 ст. 274³ УК РФ на специальную цель – совершение иного преступления – означает буквально пособничество в совершении этого преступления и детерминирует правовые коллизии и конкуренцию уголовно-правовых норм [7].

Надо признать, что такой подход нашел свою поддержку и на уровне правоприменения. Так, в судебном заседании по обвинению лица в совершении преступления, предусмотренного ч. 5 ст. 33, ч. 4 ст. 159 УК РФ, представитель государственного обвинения просил переqualифицировать действия подсудимого на ч. 1 ст. 274³ УК РФ, ссылаясь на то, что Федеральным законом от 31.07.2025 № 282-ФЗ «О внесении изменений в отдельные

⁴ Об утверждении Правил оказания телематических услуг связи : постановление Правительства Российской Федерации от 31.12.2021 № 2607 // Доступ из СПС «КонсультантПлюс».

⁵ Об утверждении Правил оказания услуг связи по передаче данных : постановление Правительства Российской Федерации от 31.12.2021 № 2606 // Доступ из СПС «КонсультантПлюс».

⁶ Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте-физическом лице : постановление Правительства Российской Федерации от 30.12.2024 № 1994 // Доступ из СПС «КонсультантПлюс».

© Русскевич Е.А.

законодательные акты Российской Федерации»⁷ введена ст. 274³ УК РФ, которая устанавливает ответственность за незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции либо обеспечение функционирования абонентского терминала пропуска трафика или его основных частей, совершенные в целях совершения иного преступления либо повлекшие тяжкие последствия. С учетом установленных по делу обстоятельств и требований закона деяние подсудимого в форме пособничества при совершении преступления в отношении потерпевшего выделено в самостоятельный состав преступления. Приведенные изменения имеют обратную силу в соответствии со ст. 10 УК РФ, согласно которой уголовный закон, устраняющий преступность деяния, смягчающий наказание или иным образом улучшающий положение лица, совершившего преступление, имеет обратную силу, то есть распространяется на лиц, совершивших соответствующие деяния до вступления такого закона в силу⁸. Аргументация стороны защиты о том, что при недоказанности соучастия в совершении мошенничества подсудимый должен быть оправдан за отсутствием состава преступления, поскольку на дату вступления закона в силу такое деяние не признавалось преступлением, была оставлена судом без внимания.

Позиция, согласно которой деяние, предусмотренное ст. 274³ УК РФ, представляет собой специальный вид пособнических действий, представляется крайне спорной. Думается, что ровно наоборот – данная норма есть пример криминализации содействия преступной деятельности без признаков соучастия. Лицо может быть привлечено к уголовной ответственности по ст. 274³ УК РФ и при отсутствии необходимой для соучастия двусторонней субъективной связи, свидетельствующей о наличии сговора о совместном совершении конкретного преступления. Этого не требуется для признания преступными действий владельца и оператора незаконного узла связи. Достаточно лишь установить, что такое лицо *допускало* использование незаконного терминала пропуска трафика для преступной деятельности. В тех же случаях, когда признаки соучастия имели место, содеянное образует совокупность со ст. 274³ УК РФ.

В связи с этим представляются вполне обоснованными доводы стороны защиты о том, что при недоказанности соучастия в мошенничестве, действия лица не могут быть квалифицированы и по ст. 274³ УК РФ, поскольку на тот момент они не признавались преступлением. Таким образом, в приведенном выше судебном решении не учитываются положения ст. 10 УК РФ, поскольку уголовному закону, устанавливающему преступность деяния, придается обратная сила.

Абонентский терминал пропуска трафика технологически предполагает использование множества сим-карт, как правило, оформленных на третьих лиц. В связи с этим вполне логичным представляется вопрос о том, охватывает ли деяние, предусмотренное ст. 274³ УК РФ, организацию деятельности по передаче абонентских номеров, по смыслу ст. 274⁴ УК РФ? Сравнение санкций указывает на то, что не может охватывать, во всяком случае по основному составу. То есть имеются серьезные предпосылки к тому, что ч. 1 ст. 274³ УК РФ предполагает своего рода обязательную совокупность с ч. 1 ст. 274⁴ УК РФ.

Статья 274⁴ УК РФ устанавливает ответственность за организацию деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации. Данная норма в настоящее время выводит в криминальное поле сложившийся с годами целый сегмент рынка услуг в сфере связи – рынок продажи и (или) аренды абонентских номеров, оформленных на третьих лиц. В сети до настоящего времени можно встретить множество подобных предложений. С учетом того, что все это отвечает критерию корыстной

⁷ О внесении изменений в отдельные законодательные акты Российской Федерации : федеральный закон от 31.07.2025 № 282-ФЗ // Доступ из СПС «КонсультантПлюс».

⁸ Приговор Серебряно-Прудского районного суда Московской области от 20.11.2025 № 1-99/2025 (УИД 50RS0043-01-2025-001002-13).

© Русскевич Е.А.

заинтересованности, такая деятельность соответствует признакам нового состава преступления.

Имеющаяся и по понятным причинам пока крайне немногочисленная практика по ст. 274⁴ УК РФ указывает на то, что даже реализация незначительного количества сим-карт позволяет квалифицировать содеянное как преступление. Так, по одному из дел суд указывает: «...М. ...из корыстных побуждений, имея преступный умысел, направленный на осуществление организации деятельности по передаче абонентских номеров, выделенных лицам на основании договоров об оказании услуг подвижной радиотелефонной связи и предоставленных в пользование в рамках указанных договоров, иным лицам в нарушение требований законодательства Российской Федерации, ...приобрел две сим-карты сотового оператора связи ПАО «Вымпелком» с абонентскими номерами «...», «...», выделенные лицам на основании договоров оказания услуг подвижной радиотелефонной связи и активированные 03 октября 2025 года на имена ... После чего, М... , действуя с прямым умыслом, достоверно зная о том, что абонентские номера зарегистрированы на третьих лиц, которые фактически не будут пользоваться в дальнейшем вышеуказанными абонентскими номерами ..., находясь в помещении торгового павильона..., из корыстных побуждений, реализовал вышеуказанные сим-карты физическому лицу, участвующему в оперативно-розыскном мероприятии «проверочная закупка», за безналичный расчет, без проведения кассовой операции...»⁹.

Организация деятельности по передаче абонентских номеров по смыслу ч. 1 ст. 274⁴ УК РФ, конечно же, не может сводиться только к их непосредственной реализации. Все-таки организация деятельности в отличие от участия в ней должна характеризоваться действиями именно организационного характера – это создание и (или) поддержание функционирования онлайн-ресурса по распространению таких сим-карт, привлечение клиентов и лиц, поставляющих «серые» абонентские номера, организация хранения сим-карт и иного необходимого оборудования, а также налаживание и контроль за сбытом абонентских номеров с привлечением курьеров и т.п. Во всем этом должна присутствовать систематичность и необходимый уровень организованности.

В соответствии с ч. 2 ст. 274⁴ УК РФ установлена ответственность за участие в деятельности, указанной в части первой данной статьи. Редакция нормы позволяет выделить несколько возможных подходов к ее толкованию: 1) данное участие предполагается в самой организации; 2) речь идет, собственно, о незаконной передаче абонентских номеров; и 3) такое участие следует понимать как выполнение заранее отведенной роли именно в рамках уже организованной деятельности.

Первое толкование – участие как вовлеченность в процесс организации – хотя и является гипотетически возможным, явно не соответствует законодательной цели ст. 274⁴ УК РФ. Второе – участие как сама деятельность по незаконной передаче абонентских номеров – очевидно выбивается из общего смысла используемой терминологии, предполагающей именно вовлеченность в какую-то деятельность, то есть уже кем-то осуществляемую и кем-то организуемую. Следовательно, заслуживает поддержки третий подход – участие как вовлеченность в уже организованную деятельность по распространению абонентских номеров. Понятно, что при таком толковании пределы криминализации существенно сужаются, поскольку однократная продажа «серой» сим-карты не будет отвечать признакам участия именно в организованной кем-то деятельности по передаче абонентских номеров.

В статье 274⁵ УК РФ законодатель установил ответственность за организацию функционирования площадок, через которые распространяются идентификаторы доступа к информационным ресурсам. В соответствии с редакцией нормы, предметом данного преступления является не только информация, необходимая для авторизации (логин, пароль),

⁹ Постановление Дорогомиловского районного суда города Москвы от 05.02.2026 № 1-77/2026 (УИД 77MS0210-01-2025-012300-26).

© Русскевич Е.А.

но и для регистрации. Здесь возникает определенная неясность относительно характера таких сведений. Если регистрационные данные сводятся к персональным данным пользователя (фамилия, имя, телефон, адрес проживания и пр.), то возникает очевидная конкуренция между ст. 274⁵ и 272¹ УК РФ, и предпочтение здесь должно быть отдано последней. Вместе с тем самостоятельное применение ст. 274⁵ УК РФ в этом отношении не исключается, поскольку к информации, необходимой для регистрации, может относиться ссылка либо код верификации, которые требуются для завершения регистрации пользователя на информационном ресурсе сети «Интернет».

В литературе было высказано суждение, что общественная опасность деяний, закрепленных в ст. 274⁵ УК РФ, неочевидна [7]. Сложно с этим согласиться. Организованные формы распространения идентификаторов доступа пользователей сети «Интернет» позволяют злоумышленникам успешно осуществлять компьютерные атаки с самыми разными целями (хищение, шантаж, вымогательство, коммерческий шпионаж и др.). При этом лица не могут не понимать, что такая информация будет использована именно в противоправной деятельности. С точки зрения информационной безопасности, теневой рынок сетевых идентификаторов представляет собой экзистенциальную угрозу.

Более того, в отечественной науке отмечается, что даже специальное закрепление ст. 274⁵ УК РФ является недостаточной мерой по борьбе с незаконным оборотом сетевых идентификационных данных. Так, по мнению В.В. Дорошкова, в свете принятия Конвенции ООН против киберпреступности¹⁰ потребуются криминализация действий, связанных с покупкой, продажей и использованием паролей, реквизитов доступа, электронных подписей или аналогичных данных, позволяющих получить доступ ко всей информационно-коммуникационной системе или любой ее части, поскольку действующая редакция ст. 274⁵ УК РФ устанавливает ответственность лишь за организацию деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети «Интернет». Покупка, однократная продажа и использование авторизационных данных состава преступления сейчас не образуют [8].

Заключение. В завершение следует еще раз отметить позитивный характер внесенных в главу 28 УК РФ изменений. Эффективное противодействие киберпреступности невозможно без установления и реализации уголовной ответственности за отдельные наиболее опасные нарушения в сфере связи.

Сохраняющееся долгое время состояние почти открытого оборота абонентских номеров, оформленных на подставных лиц, масштабного функционирования незаконных узлов связи и распространения сетевых идентификаторов пользователей имело самое негативное влияние на динамику преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Новеллы главы 28 УК РФ 2025 г. в юридико-техническом отношении, пожалуй, небезупречны и потребуют самого внимательного обсуждения с учетом формирующегося правоприменения. Как представляется, самым существенным риском является квалификация по ч. 2 ст. 274⁴ УК РФ отдельных случаев незаконной передачи абонентских номеров из корыстных побуждений при отсутствии каких-либо признаков организованности такой деятельности.

¹⁰ Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям : принята резолюцией 79/243 Генеральной Ассамблеи от 24 декабря 2024 года // Официальный сайт ООН. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243?ysclid=mhw115h7bq17697241> (дата обращения: 17.04.2026).

© Русскевич Е.А.

Список используемой литературы

1. Дремлюга Р.И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение: монография. М.: Юрлитинформ, 2022. 328 с. EDN: HSBXRM.
2. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография. М.: Юрлитинформ, 2018. 312 с. EDN: ZIHCGI.
3. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2022. 351 с. EDN: MPWWHL.
4. Хиллута В.В. Уголовное право в социальном измерении: контуры перемен и новой стратегии развития: монография. М.: Юрлитинформ, 2023. 440 с. EDN: TXPZGN.
5. Жарова А.К. Правовое регулирование отношений в области предотвращения возможных уязвимостей в информационных технологиях // Безопасность бизнеса. 2022. № 1. С. 19–26. EDN: MNASKI. DOI: 10.18572/2072-3644-2022-1-19-26
6. Криминология кибербезопасности: в 5 т. Т. 2: Уголовно-правовое обеспечение криминологической кибербезопасности / под ред. С. Я. Лебедева. М.: Проспект, 2021. 280 с. EDN: LTKWAE.
7. Ермолович Я.Н., Иванов А.Л. Совершенствование уголовно-правовой охраны информационной безопасности Российской Федерации (научно-практический комментарий к Федеральному закону «О внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2025 года № 282-ФЗ) // Право в Вооруженных Силах. 2025. № 12. С. 50–64. EDN: LZCODN.
8. Дорошков В.В. Актуальные проблемы реализации положений Конвенции ООН против киберпреступности // Мировой судья. 2026. № 2. С. 2–5. EDN: KWMGKK. DOI: 10.18572/2072-4152-2026-2-2-5.

References

1. Dremlyuga R.I. Criminal-legal protection of the digital economy and information society from cybercriminal attacks: doctrine, law, law enforcement: monograph. - M.: Yurlitinform, 2022. 328 p. EDN: HSBXRM
2. Efremova M.A. Criminal-legal protection of information security: monograph. Moscow: Yurlitinform, 2018. 312 p. EDN: ZIHCGI.
3. Ruskevich E.A. Criminal law and "digital crime": problems and solutions: monograph. 2nd ed., revised and enlarged. Moscow: INFRA-M, 2022. 351 p. EDN: MPWWHL.
4. Khilyuta V.V. Criminal law in the social dimension (contours of change and a new development strategy): monograph. – Moscow: Yurlitinform, 2023. 440 p. EDN: TXPZGN.
5. Zharova A.K. Legal regulation of relations in the field of preventing possible vulnerabilities in information technology // Business Security. 2022. № 1. P. 19–26. EDN: MNASKI. DOI: 10.18572/2072-3644-2022-1-19-26
6. Criminology of cybersecurity: in 5 volumes. Vol. 2: Criminal-legal support of criminological cybersecurity / edited by S.Ya. Lebedev. M.: Prospect, 2021. 280 p. EDN: LTKWAE.
7. Ermolovich Ya.N., Ivanov A.L. Improving the Criminal-Legal Protection of Information Security in the Russian Federation (scientific and practical commentary on the Federal Law “On Amendments to Certain Legislative Acts of the Russian Federation” dated July 31, 2025, No. 282-FZ) // Law in the Armed Forces, 2025, no. 12, pp. 50–64. EDN: LZCODN.
8. Doroshkov V.V. Current Issues of Implementing the Provisions of the UN Convention against Cybercrime // Magistrate’s Judge, 2026, no. 2, pp. 2–5. EDN: KWMGKK. DOI: 10.18572/2072-4152-2026-2-2-5.