Северо-Кавказский юридический вестник. 2026. № 2. С. 146–155
North Caucasus Legal Vestnik. 2026;(2):146–155

Научная статья
УДК 343.3+343.7
EDN HKTOFW

Вопросы квалификации и меры противодействия преступлениям, совершаемым с использованием онлайн-платформ

Ирина Анатольевна Семенцова[1, 2, 3]

[1]Филиал Московского университета имени С. Ю. Витте в г. Ростове-на-Дону, Ростов-на-Дону, Россия
[2]Ростовский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), Ростов-на-Дону, Россия
[3]Южный университет (ИУБиП), Ростов-на-Дону, Россия
irina_semen@inbox.ru, https://orcid.org/0000-0003-0888-0877

Аннотация

Введение. Использование социальных сетей для реализации преступных схем создаёт ряд сложностей при уголовно-правовой оценке деяний. Одной из проблем видится в том, что уголовное законодательство не успевает эволюционировать в соответствии с бурным развитием современных информационных технологий. В связи с этим цель статьи – определить конкретные вопросы квалификации указанных деяний и сформулировать действенные меры профилактического значения.

Теоретические основы. Методы. Теоретическую основу исследования составили научные статьи, статистические отчеты государственных ведомственных структур, материалы судебной и следственной практик. Методологическую основу составляют обще используемые методы научного исследования, применение которых обуславливает выбор системного, деятельностного, функционального и междисциплинарного подходов в изучении актуальной проблемы.

Результаты. Социальные сети являются благоприятной средой для преступности, появления новых цифровых форм поведения, часто граничащих на стыке административного и уголовного законодательства. Основная проблема сводится к выявлению субъекта преступления в условиях анонимности и трансграничного характера цифровой преступности. Профилактические меры в первую очередь связаны с реформированием уголовного законодательства, в частности, ужесточение мер ответственности за противоправные деяния, осуществляемые посредством цифровых сервисов, в том числе за привлечение лиц к незаконной деятельности через интернет, установление вредоносного контакта с целью эксплуатации, а также за удаленную реализацию запрещённых психоактивных веществ. Относительно правоохранительных органов необходимо отметить необходимость постоянного повышение цифровой компетенции с целью выявления и пресечения преступности в сети интернет.

Выводы. Для эффективной профилактики правонарушений в социальных сетях необходим многогранный и упорядоченный подход, который будет включать в себя не только уголовно-правовые инструменты, но и организационные механизмы, технологические решения, а также меры, направленные на социально-психологическое воздействие. На государственном уровне необходимо выработать эффективную политику повышения цифровой культуры населения, оперативного реагирования на размещенный противоправный контент. Для правоохранительных органов крайне важно проводить на постоянной основе повышение цифровой квалификации.

Ключевые слова: социальные сети, преступность, цифровое поведение, цифровая культура, кибербуллинг, контент, субъект преступления, профилактика преступлений, электронные доказательства
Для цитирования: Семенцова И. А. Вопросы квалификации и меры противодействия преступлениям, совершаемым с использованием онлайн-платформ // Северо-Кавказский юридический вестник. 2026. № 2. С. 146–155. EDN HKTOFW

Original article

Qualification issues and measures to counter crimes committed using online platforms

Irina A. Sementsova[1, 2, 3]

[1]Branch of the S. Yu. Witte Moscow University in Rostov-on-Don, Rostov-on-Don, Russia
[2]Rostov Institute (Branch) of the Russian Ministry of Justice, Rostov-on-Don, Russia
[3]Southern University, Rostov-on-Don, Russia
irina_semen@inbox.ru, https://orcid.org/0000-0003-0888-0877

Abstract

Introduction. The use of social networks for the implementation of criminal schemes creates a number of difficulties in the criminal legal assessment of acts. One of the problems is that the criminal legislation does not keep up with the rapid development of modern information technologies. In this regard, the purpose of this article is to identify specific issues related to the qualification of these acts and to formulate effective preventive measures.

Theoretical foundations. Methods. The theoretical basis of the study consists of scientific articles, statistical reports of state departmental structures, and materials from judicial and investigative practices. The methodological basis is based on commonly used scientific research methods, which determine the choice of systemic, activity-based, functional, and interdisciplinary approaches to studying this relevant issue.

Results. So, social networks are a favorable environment for crime, the emergence of new digital forms of behavior, often bordering on the intersection of administrative and criminal legislation. The main problem is to identify the perpetrator of a crime in the context of anonymity and the cross-border nature of digital crime. Preventive measures are primarily related to the reform of criminal legislation, in particular, the tightening of liability for illegal acts carried out through digital services, including the involvement of individuals in illegal activities via the Internet, the establishment of malicious contact for the purpose of exploitation, and the remote sale of prohibited psychoactive substances. Regarding law enforcement agencies, it is necessary to note the need for continuous improvement of digital competence in order to detect and prevent crime on the Internet.

Conclusions. To effectively prevent offenses on social networks, a multifaceted and systematic approach is needed, which will include not only criminal law tools, but also organizational mechanisms, technological solutions, and measures aimed at socio-psychological impact. At the state level, it is necessary to develop an effective policy for raising the digital culture of the population and promptly responding to illegal content posted. It is crucial for law enforcement agencies to continuously improve their digital skills.

Keywords: social networks, crime, digital behavior, digital culture, cyberbullying, content, subject of crime, crime prevention, electronic evidence
For citation: Sementsova I.A. Qualification issues and measures to counter crimes committed using online platforms. *North Caucasus Legal Vestnik.* 2026;(2):146–155. (In Russ.). EDN HKTOFW

Введение

Использование социальных сетей в качестве средства совершения преступлений порождает комплекс проблем уголовно-правовой квалификации. Данные трудности обусловлены особенностями цифровой среды, высокой степенью анонимности пользователей, трансграничностью коммуникаций и недостаточной адаптацией уголовного законодательства к современным информационным технологиям.

Одной из наиболее значимых проблем является установление личности лица, совершившего преступление. Использование анонимных аккаунтов, фальшивых профилей, виртуальных номеров, программ анонимизации (VPN, TOR) существенно затрудняет определение фактического автора сообщения, публикации или распространённого контента [1, с. 52].

Теоретические основы. Методы

Теоретическую основу исследования составили научные статьи, статистические отчеты государственных ведомственных структур, материалы судебной и следственной практик. Методологическую основу составляют обще используемые методы научного исследования, применение которых обуславливает выбор системного, деятельностного, функционального и междисциплинарного подходов в изучении обозначенной проблемы.

Результаты и обсуждение

Социальные сети совмещают функции средства массовой информации, платформы коммуникации и цифрового пространства для совершения действий технического характера. В результате возникают сложности в квалификации, поскольку одно и то же деяние может содержать признаки нескольких составов преступлений [2, с. 356].

Рассмотрим проблему, которая выражена в оценке общественной опасности цифрового деяния. Скорость распространения информации и возможный охват аудитории значительно увеличивают потенциальный вред преступления, совершённого посредством социальной сети [3, с. 290]. Однако действующее уголовное законодательство не содержит специальных критериев, учитывающих, количество репостов, сохранений или просмотров, потенциальную «вирусность» контента, массовость вовлекаемого круга лиц.

Отсутствие таких критериев приводит к различиям в судебной практике и усложняет оценку степени общественной опасности деяния.

Для правильной квалификации противоправного деяния необходимо иметь доказательственную базу, что в условиях интернета является проблемой [4, с. 172]. Цифровая форма доказательств требует соблюдения специальных процедур их извлечения, фиксации и исследования. Скриншоты, ссылки и копии переписки сами по себе не всегда являются достаточными доказательствами, что создаёт ряд специфических трудностей.

Так, например, контент в сети может быть быстро отредактирован или удалён, что осложняет его фиксацию в качестве доказательства, а для установления обстоятельств необходимо учитывать метаданные, такие как IP-адрес, время публикации и геолокация. Кроме того, подтверждение принадлежности аккаунта конкретному лицу представляет значительные сложности и требует привлечения специалистов в области компьютерной криминалистики для проведения экспертных исследований.

Трансграничный характер социальных сетей затрудняет определение места совершения преступления, поскольку серверы, на которых размещён контент, могут находиться заграницей или же автор сообщения может находиться в одной юрисдикции, а пострадавший в другой, а также необходимо применять нормы международного сотрудничества и запроса данных у иностранных компаний.

Вследствие этого возникают сложности с применением национального уголовного законодательства и сбором доказательств за рубежом. Н. А. Крайнова [5, с. 43] справедливо отмечает относительно вопроса кибербезопасности, что он давно уже вышел за границы отдельных государств и нуждается в консолидации усилий мирового сообщества. Без построения тесного сотрудничества в этой области между государствами и международными организациями противостоять цифровой преступности будет затруднительно. Крайне необходимо привести к единому стандарту нормы национального законодательства отдельных государств, принимающих участие в разработке инициатив и конструктивных мер в борьбе с преступлениями в сети Интернет.

На сегодняшний день в научных кругах актуальными являются вопросы относительно криминализации ряда негативных действий в цифровой среде, например: создание и

распространение дипфейков, трансляция контента, представляющего угрозу для общества (например, треш-стримы), использование эмодзи в противоправных целях, манипуляции с лайками, блокировка пользователей в информационно-телекоммуникационных сетях, кибербуллинг, онлайн-харассмент, распространение интимных материалов без согласия, онлайн-груминг, подстрекательство к участию в опасных челленджах.

Вопрос касательно отнесения перечисленных деяний к информационным преступлениям, требует определения границ этого понятия, так как следует руководствоваться положениями относительно оснований уголовно-правового запрета и принимать во внимание тенденции, продиктованные цифровой трансформацией общества. В этой связи право является мощным инструментом регулирования социальных процессов. Посредством него представляется возможным определить границы новых социальных реалий. Вместе с тем законодательство не должно быть просто пассивным отражением уже сложившихся общественных отношений [6, с. 146]. Законодатель должен не просто автоматически копировать реальность, а подходить, субъективно формируя правовой образ рассматриваемых отношений, создавая законодательные установления, отвечающие потребностям общества.

На сегодняшний день действующие правовые нормы не содержат чётких мер ответственности за преступления, совершённые посредством дипфейков. Между тем данный вопрос поднимался уже на уровне законодательных органов. Так в Государственной Думе РФ в прошлом году подлежал рассмотрению законопроект № 885494-8 «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации»[1], предлагающий квалифицировать использование дипфейков как обстоятельство, отягчающее наказание. Однако проект не получил одобрения на этапе предварительного рассмотрения и был направлен на доработку. Думается в ближайшем будущем, российский законодатель вернётся к данному вопросу, но пока до этого момента в практической деятельности будут существовать трудности относительно квалификации подобных деяний.

Данный пример дипфейков показывает нам слабые места в сфере информационной безопасности. Быстрый темп развития информационных и цифровых технологий вскрывает дефектность действующих механизмов защиты, а государство пока не успевает адаптировать законодательство и четко определить границы ответственности. Этим пользуются преступники, ощущая правовой вакуум, активно внедряют дипфейки в своих преступных схемах.

Однако можно увидеть попытки законодателя не отставать от процесса цифровизации на примере следующих уголовно-правовых норм: ст. с 272–274 охватывают компьютерные преступления, ст. 159.6 предусматривает ответственность за мошенничество в сфере компьютерной информации, а ст. 238 – за предоставление услуг ненадлежащего качества.

Современные правовые нормы оказались не адаптированы к внедрению компонентов искусственного интеллекта в различные сферы жизни, особенно вызывают некоторые трудности инновационные разработки, как ChatGPT и Midjourney, несущие серьезные риски для социума. Необходимо понимать, что для целей исключения преступных деяний посредством данных компонентов, следует продумать теоретическую основу их правового регулирования. Видится, что законодателю следует пойти по пути закрепления в качестве отягчающего обстоятельства, использование искусственного интеллекта в соответствующих составах.

Находит положительный отклик у автора статьи установление уголовно-правовых запретов на иные виды информационных деяний: оправдание геноцида советского народа, пропаганда противоправного или аморального антиобщественного поведения. Правоведы

[1] Паспорт проекта Федерального закона № 885494-8 «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации» (внесен депутатами Государственной Думы ФС РФ С.М. Мироновым, Я. В. Лантратовой, О. А. Ниловым, Н. В. Новичковым, А. А. Кузнецовым, М. Г. Делягиным, Д. Г. Гусевым, А. С. Аксененко) (снят с рассмотрения) // В данном виде документ опубликован не был.

спорят о целесообразности внесения изменений в УК РФ, путём закрепления квалифицирующего признака использования информационных и коммуникационных технологий, включая технологии искусственного интеллекта.

Усложняет квалификацию процесс разграничения уголовной и административной ответственности. Во многих случаях деяния в социальных сетях находятся на грани между административным и уголовно наказуемым правонарушением. Отсутствие четких критериев порождает неоднозначность в правоприменении и усложняет квалификацию [7, с. 46].

Несмотря на наличие специальных норм УК РФ, учитывающих использование сети Интернет, законодательство остаётся фрагментарным. В ряде случаев отсутствуют специальные квалифицирующие признаки, связанные с использованием социальных сетей, легальные определения современных цифровых терминов, а также единые методические рекомендации по расследованию таких преступлений. Это требует регулярного обновления правовой базы и развития судебной практики.

Наиболее значимыми проблемами квалификации выступают: сложности установления субъекта преступления, необходимость разграничения смежных составов; отсутствие чётких критериев оценки общественной опасности цифрового поведения; проблемы фиксации, сохранения и допустимости электронных доказательств; неопределённость юрисдикции при трансграничном характере коммуникаций; а также нормативные пробелы, связанные с отсутствием специальных юридических конструкций для новых форм цифрового девиантного поведения [8, с. 127].

Анализ показывает, что развитие социальных сетей стремительно опережает обновление уголовного законодательства, что приводит к фрагментарности правового регулирования. В этих условиях ключевую роль начинает играть судебная и экспертная практика, формирующая подходы к применению общих норм Уголовного Кодекса Российской Федерации (далее – УК РФ)[1] в условиях цифровизации.

Чтобы повысить качество квалификации преступных деяний, совершённых посредством социальных сетей надлежит в первую очередь усовершенствовать содержание уголовно-правовых норм, в частности: определиться с трактовками понятий, ввести соответствующие квалифицирующие признаки, установить четкие критерии общественной опасности цифровых деяний, разработать методические рекомендации в части обращения с цифровыми доказательствами.

В настоящее же время процесс квалификация преступных деяний, совершенных посредством социальных сетей, отягощён целым рядом существенных проблем. Так в их число входит неопределенность законодателя относительно выражения вовне цифрового преступления, проблемы, связанные с определением субъекта преступного деяния, особенностей фиксации, хранения и оценки цифровых доказательств.

Установлено, что судебная и следственная практика складывается неоднородно в связи со стремительным развитием информационных технологий и отставанием за ним уголовного законодательства. Это снижает эффективность уголовно-правового реагирования и требует дальнейшего совершенствования правовых механизмов противодействия преступности в сети.

Противодействие преступлениям, совершаемым в социальных сетях, должно носить комплексный характер и сочетать правовые, организационные, технические, образовательные и социально-психологические меры [9, с. 88].

Ключевая задача профилактики – создание условий, при которых вовлеченность граждан в цифровое пространство не повышает вероятность преступных посягательств [10, с. 20]. Это требует модернизации уголовного законодательства, внедрения систем мониторинга

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 20.01.2026) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

и анализа данных, усиления межведомственного сотрудничества, а также формирования цифровой культуры среди пользователей.

Современная практика расследования преступлений в социальных сетях показывает необходимость дальнейшей детализации норм, регулирующих ответственность за преступления в цифровой среде. Важными направлениями являются:

- Уточнение квалифицирующих признаков для мошенничества и незаконного доступа в цифровую инфраструктуру (ст. 159.6, 272–274.1 УК РФ).

- Расширение ответственности за действия, совершённые с использованием цифровых платформ, включая онлайн-вербовку, груминг, дистанционный сбыт наркотиков.

- Введение отдельных составов для цифровой травли и кибersталкинга, учитывая специфику воздействия на жертву.

- Усиление ответственности за распространение экстремистских материалов с использованием алгоритмов автоматического распространения.

Предприняв комплексный подход для упорядочивания цифровых отношений, законодатель в 2025 г. ввёл новые уголовно-правовые нормы (статьи 274.3 и 274.5[1]), направленные на установление ответственности в сфере создания и распространения вредоносного программного обеспечения, а также противоправное вмешательство в работу информационных систем. Указанные выше уголовно-правовые новшества призваны обеспечить профилактику преступных деяний в цифровой среде и дополнить существующие административно-правовые меры, установив повышенную ответственность за кибепреступления.

Помимо рассмотренных изменений, общая часть уголовно-правового законодательства также была изменена, в частности, в статью 63 УК РФ, было введено отягчающее обстоятельство, связанное с использованием VPN, которое усиливает ответственность за преступные деяния в киберпространстве, тем самым создавая препятствия для сокрытия цифровых следов незаконной деятельности.

Политика государства в области обеспечения информационной безопасности преследует цель построения безопасного цифрового пространства, путем принятия совокупности мер относительно социальных платформ [11, с. 239].

Ключевыми элементами политики являются блокировка запрещённой информации, включая материалы экстремистского характера, пропаганду наркотиков и порнографию, а также идентификация пользователей по номеру телефона, что снижает анонимность потенциальных злоумышленников.

Владельцы социальных сетей несут ответственность за несвоевременную реакцию на сообщения о преступном контенте, а интеграция платформ с системами Роскомнадзора позволяет оперативно фильтровать опасные материалы и предотвращать их распространение [12, с. 22].

Деятельность правоохранительных органов необходимо совершенствовать в соответствии с развитием технологий. Для эффективного противодействия преступлениям в социальных сетях необходимо развитие следующих направлений:

- цифровая криминалистика, включающая анализ метаданных, цифровых следов, сетевой активности;

- скрытая работа в сетевых сообществах, позволяющая выявлять преступные группы;

- создание единых межведомственных центров мониторинга социальных сетей, интегрирующих МВД, ФСБ, Роскомнадзор, Следственный комитет;

- использование технологий искусственного интеллекта для обнаружения признаков экстремизма, вербовки, сетевой агрессии и незаконного оборота наркотиков. В эпоху цифровизации особое значение приобретает интеграция современных технологий в повседневную

[1] Федеральный закон от 31.07.2025 № 282-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" // Собрание законодательства РФ. 04.08.2025. № 31. Ст. 4636.

практику. Это открывает новые горизонты для совершенствования способов мониторинга и обработки информации. Так распространенным стало использование специальных алгоритмов в целях осуществления анализа структурированных и неструктурированных массивов данных (Big Data), что может стать полезным и для целей построения цифровой криминологии [13, с. 222].

Возможность посредством специализированных программных средств осуществлять мониторинг сети в целом является актуальным запросом сегодняшнего времени, так как даёт возможность оптимизации ресурсов человека и увеличения количества информации, подлежащей обработке. Внедрение подобных технологий в правоохранительную деятельность, способно улучшить её эффективность.

Нельзя не упомянуть и важность международных каналов взаимодействия, так как внушительная часть цифровых платформ принадлежит иностранным государствам, что подталкивает Россию активно заключать транснациональные соглашения [14, с. 68].

Автор статьи убежден, что на законодательном уровне необходимо внедрить такие меры борьбы с киберпреступностью, как:

- разработка инструментов, дающих возможность оперативно блокировать счета и онлайн-сервисы, которые задействованы в преступных схемах;

- внедрение продуманного механизма обмена данными между органами правопорядка, провайдерами связи, банковскими учреждениями и юридическими лицами, осуществляющими деятельность в области финансовых технологий. Требуется законодательно установить срок равный не более 24 часов для направления ответов на запросы следственных органов, посредством сертифицированных защищенных каналов связи;

- установление чётких правил и порядка для блокировки транзакций и SIM-карт, вызывающих подозрения;

- разработка правовой базы, которая позволит контролировать применение средств анонимизации, включая VPN-сервисы. Полагаем необходимо создать государственный реестр VPN-платформ с чётким определением условий их законного использования, что как представляется должно позитивным образом отразиться, на состоянии преступности в этой сфере.

Конечно, значимым событием следует считать внесенные в 2025 году изменения в уголовный закон, когда в ст. 63 УК РФ[1] был добавлен подп. «ф» п. 1. В соответствии с ним, факт совершения противоправного деяния с применением программно-аппаратных комплексов, обеспечивающих доступ к информационным ресурсам и информационно-телекоммуникационным сетям с ограниченным доступом, теперь рассматривается как отягчающее обстоятельство. Данное законодательное новшество подчёркивает актуальность разработки и внедрения, дополнительных мер, позволяющих контролировать и идентифицировать пользователей, которые применяют технологии маскировки IP-адресов и используют защищённые каналы для передачи данных.

Процесс раскрытия преступлений в цифровой сфере, имеет свои отличительные черты. В качестве характерной особенности следует отметить необходимость фиксировать электронные доказательства в порядке, отражённом в уголовно-процессуальном законодательстве. Ключевую роль в рассматриваемом аспекте играет выстроенное взаимодействие следственных органов с администрациями социальных сетей и интернет-провайдерами, в целях выявление данных о пользователях, преступающих закон [15, с. 159].

В настоящее время специалисты соответствующих подразделений непрерывно повышают свою квалификацию и углубляют профессиональные знания. Так, заметное улучшение результатов работы достигается благодаря, например, внедрению образовательной

[1] Федеральный закон от 31.07.2025 № 282-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" // Собрание законодательства Российской Федерации. 2025. 4 августа (№ 31). Ст. 4636.

программы «Конкурентная разведка в Интернете» для сотрудников, которые ведут борьбу с преступными деяниями в сфере информационно-коммуникационные технологий.

Автоматизированный мониторинг интернет-пространства посредством специализированных программных продуктов в современных реалиях приобретает особую важность. Благодаря обозначенному методу, возможно, провести оптимизацию человеческих ресурсов и существенно расширить объем обрабатываемой информации. Экспертами утверждается, что внедрение подобных технологических инструментов в несколько раз повысит результативность работы правоохранительных органов.

Набирают значимость программы раннего выявления цифровой радикализации и профилактики онлайн-груминга.

Социальные сети несут ответственность за создание безопасного цифрового пространства и обязаны внедрять инструменты, направленные на предотвращение преступной активности. К таким мерам относятся автоматическая фильтрация контента, содержащего признаки агрессии, экстремизма или пропаганды наркотиков, внедрение систем верификации аккаунтов, а также обеспечение эффективных механизмов подачи жалоб и оперативной блокировки нежелательных материалов.

Важным аспектом современной цифровой безопасности является повышение уровня личной защиты в сети. К ключевым мерам относятся использование сложных паролей и двухфакторной аутентификации, ограничение публичности личной информации, а также осторожность при переходе по подозрительным ссылкам и общении с незнакомыми контактами. Не менее важно регулярно обновлять программное обеспечение и использовать антивирусные средства для предотвращения возможных угроз. Чем выше индивидуальная цифровая культура, тем меньше вероятность стать жертвой преступлений [16, с. 145].

Профилактика преступлений, совершаемых через социальные сети, представляет собой многоуровневую систему, включающую законодательные, технические, организационные и образовательные меры. Усиление цифровой грамотности населения, совершенствование уголовного законодательства, развитие оперативно-розыскных возможностей и внедрение автоматизированных технологий мониторинга являются ключевыми факторами в снижении преступной активности в сети [17, с. 156].

Заключение

Таким образом, профилактика преступлений в социальных сетях должна носить комплексный и системный характер, сочетая уголовно-правовые, организационные, технические и социально-психологические меры. Эффективное предупреждение цифровой преступности невозможно без координации деятельности государственных органов, правоохранительных структур, операторов цифровых платформ и общества в целом.

Установлено, что особую роль в системе профилактики играют меры, направленные на повышение уровня цифровой грамотности пользователей, защиту несовершеннолетних, развитие механизмов мониторинга и оперативного реагирования на противоправный контент. Реализация указанных направлений способствует снижению уровня преступности в социальных сетях и укреплению системы уголовно-правовой охраны в цифровой среде.

Список источников

1. Гильмутдинова Ю. Ю. Проблемы уголовно-правовой квалификации киберпреступлений по законодательству Российской Федерации. *Lex criminalis scientiarum*. 2025;1(3):51–55. https://doi.org/10.63118/3034-3259.2025.3.1.008. EDN: ABTRHW

2. Уголовное право. Особенная часть: учебник для вузов / В. Б. Боровиков, А. А. Смердов; 7-е изд., перераб. и доп. М.: Юрайт, 2023. 505 с. ISBN: 978-5-534-17301-7. EDN: CPYAZP

3. Каражеляскоv Б. А., Проблемы уголовной ответственности в сети интернет / Б. А. Каражеляскоv, Л. Н. Карпушева, М. Ф. Юнусов. *Образование и право.* 2022;11:289–292. https://doi.org/10.24412/2076-1503-2022-11-289-292. EDN: BONYBL

4. Анисимова А. М., Кубиевич С.В. Проблемы квалификации общеуголовных киберпреступлений. *Закон и право.* 2023;12:169-174. https://doi.org/10.24412/2073-3313-2023-12-169-174. EDN: GUREHY

5. Крайнова Н. А. "Международная цифровая безопасность": миф или реальность? *Криминология: вчера, сегодня, завтра*. 2019;4(55):42–46. EDN: JFVITS

6. Ключко Р.Н. Информационная безопасность в социально-гуманитарном измерении: дискурс уголовно-правовой институционализации. *Журнал российского права*. 2025;10:140–155. https://doi.org/1010.61205/jrp.2025.10.4. EDN: IFDLSS

7. Евдокимов К. Н. Противодействие компьютерной преступности: теория, законодательство, практика: автореф. дис. док. юрид. наук. М., 2023. 73с.

8. Ефремова И. А. Особенности квалификации преступлений в сфере компьютерной информации и противодействия им. *Правоприменение*. 2025;1:122–131. https://doi.org/10.52468/2542-1514.2025.9(1).122-131. EDN: MQUHVB

9. Чабукиани О. А. Способы противодействия киберпреступности / О. А. Чабукиани, Е. А. Зорина, В. В. Солодовник. *Социология и право.* 2020;3 (49):84–93. https://doi.org/10.35854/2219-6242-2020-3-84-93. EDN: CHKQVI

10. Ванина А. В. Проблемы юридической регламентации уголовно-правового запрета на преступления в сфере компьютерной информации. *Научный компонент.* 2022;2 (14):17–22. https://doi.org/10.51980/2686-939X_2022_2_27. EDN: YZHZSO

11. Клещина Е. Н. Проблемы и основные направления совершенствования правового регулирования противодействия киберпреступности. *Государственная служба и кадры.* 2024;4:237–241. https://doi.org/10.24412/2312-0444-2024-4-237-241. EDN: SELUZW

12. Родина Е. А. Криминологические проблемы противодействия киберпреступности: автореф. дис. … канд. юрид. наук. Саратов, 2022. 27 с. EDN: MYDGRO

13. Пинкевич Т.В. Криминологический мониторинг преступлений, совершаемых с использованием цифровых технологий. *Право и управление*. 2024;10:221–224. https://doi.org/10.24412/2224-9133-2024-10-221-224. EDN: IUVRKJ

14. Петров П. К., Денисович В.В. Преступность в виртуальном пространстве: криминологическая характеристика. *Проблемы права*. 2025;1(97):66–70. https://doi.org/10.14529/pro-prava250111. EDN: FVVUHA

15. Рясов А. А., Багиров З. Р. Возможности использования социальных сетей при расследовании преступлений. *Вестник всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации*. 2025;1. (73):157–162. https://doi.org/10.29039/2312-7937-2025-1-157-162. EDN: JMCQUA

16. Юзиханова Э. Г., Корсикова Н.А. Профилактика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Правопорядок: история, теория, практика. 2025;4:143–146. https://doi.org/10.47475/2311-696X-2025-47-4-143-146. EDN: DPUPTL

17. Берестовой А. Н. Законодательная регламентация вопросов противодействия новым формам девиантного поведения в сети "Интернет". *Вестник Санкт-Петербургского университета МВД России.* 2024;3(103):152–160. https://doi.org/10.35750/2071-8284-2024-3-152-160. EDN: BUJBGR

References

1. Gilmutdinova Yu.Yu. Problems of Criminal Law Qualification of Cybercrimes under the Legislation of the Russian Federation. *Lex criminalis scientiarum.* 2025;1(3):51-55. (In Russ.). https://doi.org/10.63118/3034-3259.2025.3.1.008. EDN: ABTRHW

2. *Criminal Law. Special Part: Textbook for Universities* / V.B. Borovikov, A.A. Smerdov; 7th Edition, Revised and Expanded. Moscow: Yurayt; 2023. 717 p. (In Russ.)

3. Karazhelyaskov B.A., Karpushcheva L.N., and Yunusov M.F. Problems of Criminal Liability on the Internet. *Obrazovanie i pravo*. 2022;11:289-292. (In Russ.). https://doi.org/10.24412/2076-1503-2022-11-289-292. EDN: BONYBL

4. Anisimova A.M., Kubievich S.V. Problems of Qualification of General Criminal Cybercrimes. *Zakon i pravo.* 2023;12:169-174. (In Russ.). https://doi.org/10.24412/2073-3313-2023-12-169-174. EDN: GUREHY

5. Krajnova N.A. "International Digital Security": Myth or Reality? *Kriminologiya: vchera, segodnya, zavtra.* 2019;4(55):42-46. (In Russ.). EDN: JFVITS

6. Klyuchko R.N. Information Security in the Social and Humanitarian Dimension: The Discourse of Criminal Law Institutionalization. *Zhurnal rossijskogo prava.* 2025;10:140–155. (In Russ.). https://doi.org/1010.61205/jrp.2025.10.4. EDN: IFDLSS

7. Evdokimov K. N. *Countering Computer Crime: Theory, Legislation, and Practice.* Doctoral Dissertation in Law. Moscow; 2023. 73 p. (In Russ.)

8. Efremova I. A. Features of Qualifying Crimes in the Field of Computer Information and Countering Them. *Pravoprimenenie.* 2025;1:122–131. (In Russ.). https://doi.org/10.52468/2542-1514.2025.9(1).122-131

9. Chabukiani O. A. Methods of Countering Cybercrime / O. A. Chabukiani, E. A. Zorina, V. V. Solodovnik. *Sociologiya i pravo.* 2020;3 (49):84–93. (In Russ.). https://doi.org/10.35854/2219-6242-2020-3-84-93. EDN: CHKQVI

10.Vanina A. V. Problems of Legal Regulation of the Criminal Law Prohibition of Crimes in the Field of Computer Information. *Nauchnyj komponen*t. 2022;2 (14):17-22. https://doi.org/10.35854/2219-6242-2020-3-84-93. EDN: CHKQVI 10.51980/2686-939X_2022_2_27 (In Russ.)

11.Kleshchina E. N. Problems and Main Directions of Improving the Legal Regulation of Countering Cybercrime. *Gosudarstvennaya sluzhba i kadry.* 2024; 4:237-241. (In Russ.). https://doi.org/10.24412/2312-0444-2024-4-237-241. EDN: SELUZW

12.Rodina E. A. *Criminological problems of countering cybercrime* : abstract of the dissertation. ... kand. jurid. Sciences / E. A. Rodina. Saratov; 2022. 27 c. EDN: MYDGRO. (In Russ.)

13.Pinkevich T.V. Criminological monitoring of crimes committed using digital technologies. *Pravo i upravlenie.* 2024;10:221-224. https://doi.org/10.24412/2224-9133-2024-10-221-224 (In Russ.)

14.Petrov P. K., Denisovich V.V. Crime in the Virtual Space: A Criminological Analysis. *Problemy prava.* 2025;1 (97):66-70. (In Russ.). https://doi.org/10.14529/pro-prava250111. EDN: FVVUHA

15.Ryasov A. A., Bagirov Z. R. Opportunities for Using Social Media in Crime Investigation. *Vestnik vserossijskogo instituta povysheniya kvalifikacii sotrudnikov Ministerstva vnutrennikh del Rossijskoj Federacii.* 2025;1 (73):157-162. (In Russ.). https://doi.org/10.29039/2312-7937-2025-1-157-162. EDN: JMCQUA

16.Yuzikhanova E. G., Korsikova N. A. Prevention of Crimes Committed Using Information and Telecommunication Technologies. *Pravoporyadok: istoriya, teoriya, praktika*. 2025;4:143–146. (In Russ.). https://doi.org/10.47475/2311-696X-2025-47-4-143-146. EDN: DPUPTL

17.Berestovoy A. N. Legislative Regulation of Countering New Forms of Deviant Behavior on the Internet. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii.* 2024; 3 (103):152–160. (In Russ.). https://doi.org/10.35750/2071-8284-2024-3-152-160. EDN: BUJBGR

Информация об авторе

И. А. Семенцова – кандидат юридических наук, доцент.

Information about the author

I. A. Sementsova – Cand. Sci. (Law), Associate Professor.

Автор заявляет об отсутствии конфликта интересов.
The author declares that there is no conflict of interest.

Статья поступила в редакцию 25.04.2026; одобрена после рецензирования 28.05.2026; принята к публикации 03.06.2026.
The article was submitted 25.04.2026; approved after reviewing 28.05.2026; accepted for publication 03.06.2026.