

Научная статья

УДК 343.98

DOI: 10.47475/2411-0590-2025-12-2-250-259

Кибермошенничество: новые методы, старые цели

Наиля Рашидовна Шевко¹, Марина Алексеевна Лукина²

¹ Казанский государственный энергетический университет, г. Казань, Россия

mos_shev@mail.ru

 <https://orcid.org/0000-0003-1092-3389>

² Казанский филиал Российского государственного университета правосудия, г. Казань, Россия

lukina_m@mail.ru

 <https://orcid.org/0000-0002-2792-2190>

Аннотация. Внедрение информационных технологий во все сферы жизни общества во многом упростило процессы обращения граждан в органы государственной власти, получения государственных услуг в электронном виде, обмен данными между ведомствами. Все благодаря тому, что вся необходимая информация хранится в удобном формате — электронном. Однако это потребовало и особого внимания к защите конфиденциальной информации, обеспечению безопасного обращения с персональными данными. Ведь, помещая информацию в виртуальное пространство, возникает возможность доступа к ней и лиц, не уполномоченных для ознакомления с ней и пользования ею. Соответственно, возникают уязвимости защиты персональных данных. Они не всегда связаны с несовершенством программного обеспечения. Зачастую злоумышленники под различными предложениями, используя инструменты социальной инженерии, провоцируют пользователей на предоставление сторонним лицам доступа к личным кабинетам, аккаунтам. Авторами представлены наиболее распространенные схемы мошеннических действий в сфере компьютерной информации, а также их последствия. Теоретический материал подкреплен официальными статистическими данными по данному вопросу, проведен статистический анализ данных по регионам Российской Федерации по числу зарегистрированных преступлений данной категории, а также по количеству лиц, их совершивших.

Ключевые слова: киберпреступность, кибермошенничество, киберугроза, киберзащита, защита данных, фишинг, преступления с использованием информационных технологий, мошенничество в сфере компьютерной информации

Для цитирования: Шевко Н. Р., Лукина М. А. Кибермошенничество: новые методы, старые цели // Викимология. 2025. Т. 12, № 2. С. 250–259. DOI: 10.47475/2411-0590-2025-12-2-250-259

Research article

Cyberfraud: New Methods, Old Target

Nailya R. Shevko¹, Marina A. Lukina²

¹ Kazan State Energy University, Kazan, Russia
mos_shev@mail.ru

 <https://orcid.org/0000-0003-1092-3389>

² Kazan branch of the Russian State University of Justice, Kazan, Russia,
lukina_m@mail.ru

 <https://orcid.org/0000-0002-2792-2190>

Abstract. The introduction of information technologies into all spheres of society has greatly simplified the processes of citizens' appeals to government bodies, receiving government services electronically, and exchanging data between departments. All thanks to the fact that all necessary information is stored in a convenient format — electronically. However, this also required special attention to the protection of confidential information, ensuring safe handling of personal data. After all, by placing information in virtual space, it becomes possible for persons not authorized to read and use it to access it. Accordingly, vulnerabilities in the protection of personal data arise. They are not always related to software imperfections. Often, attackers, under various pretexts, using social engineering tools, provoke users to provide third parties with access to personal accounts. The authors present the most common schemes of fraudulent actions in the field of computer information, as well as their consequences. The theoretical material is supported by official statistical data on this issue, a statistical analysis of data on the regions of the Russian Federation on the number of registered crimes of this category, as well as on the number of people who committed them.

Keywords: cybercrime, cyber fraud, cyber threat, cyber defense, data protection, phishing, information technology crime, computer information fraud

For citation: Shevko NR, Lukina MA. Cyberfraud: new methods, old targets. *Victimology*. 2025;12(1):250-259. (In Russ.). DOI: 10.47475/2411-0590-2025-12-2-250-259

Введение

Новые технологии, уверенно шагнувшие в жизнь современных людей, наряду с достоинствами в виде упрощения, облегчения и оперативности выполнения некоторых операций, оптимизации затрат привнесли в быт и опасность, создали неудобства в использовании обычных гаджетов, подвергли информационной опасности конфиденциальные данные пользователей и их банковские счета. По официальным данным МВД РФ, в 2024 году в России было совершено 765,4 тыс. преступлений, совершенных с использованием информационных технологий. Это на 13 % больше, чем в 2023 году. Причем, доля киберпреступлений в общем числе преступлений выросла до 40 % (ранее

не достигала и 35 %)¹. С расширением покрытия зон интернета и увеличением его скорости выросло и число преступлений, совершенных с его использованием — почти на четверть.

Большую часть киберпреступлений составляет кибермошенничество, с каждым годом приобретающее новый облик — способы и методы обмана пользователей.

Преступления с использованием современных информационных технологий являются одними из новейших направлений исследований ученых. Основные положения квалификации, способы обнаружения,

¹ Состояние преступности // Официальный сайт МВД РФ. URL: <https://мвд.рф/dejatelnost/statistics> (дата обращения: 05.04.2025).

фиксации и изъятие улик, особенности расследования подобного рода преступных деяний в виртуальном пространстве были представлены в трудах таких известных ученых как В. Б. Вехов [1], Т. А. Абрамян [2], М. А. Простосердов [3], Е. А. Лысак [4], М. А. Ефремова [5], Н. С. Зорина [6], Е. А. Кошечкина и С. В. Новиков [7], Д. В. Завьялова [8]. Однако, ввиду стремительного развития научно-технического прогресса многие вопросы остаются дискуссионными.

В современной науке формируются отдельные направления изучения киберпреступности [9; 10]:

- кибербуллинг [11; 12; 13; 14];
- вымогательство в сети [15];
- легализация денежных средств в киберпространстве [16];
- кибермошенничество [17];
- мошенничество с использованием электронных средств платежа [18];
- преступления против собственности с применением информационных технологий [19] и др. [20; 21].

В целях установления динамики распространения мошеннических действий в сфере компьютерной информации на территории Российской Федерации использованы материалы научных исследований по вопросам ответственности за преступления с использованием информационных технологий, в сфере компьютерной информации, специальная литература по предмету исследования, а также официальные статистические данные ГИАЦ МВД России.

Основными задачами проведенного исследования являются:

- проанализировать на основе официальной статистической информации динамику совершения преступлений по ст. 159.6 УК РФ на территории России;
- представить наиболее распространенные методы и способы совершения мошеннических действий с использованием информационных технологий;
- рассмотреть распространенность данного вида преступлений на мировом уровне.

Методологической основой исследования являются общенаучные методы, анализ статистических данных, методы научного познания.

Теоретической базой проведенного исследования выступают труды ведущих специалистов в области противодействия преступлениям, совершенным с использованием информационных технологий [22, с. 84].

Эмпирической базой исследования выступают официальные статистические данные по теме исследования.

Практическая значимость проведенного исследования заключается в обобщении статистических данных по преступлениям, относящимся к мошенничеству в сфере компьютерной информации, на основе которых можно производить среднесрочное криминологические прогнозирование дальнейшего распространения кибермошенничества, а также совершенствование мер профилактики и противодействия преступлениям в киберпространстве.

Процесс и результаты проведенного исследования

В последнее время все большее распространение среди киберпреступлений приобретает кибермошенничество. Фишинг — вид интернет-мошенничества, при котором переход по ссылке осуществляется на подставной сайт, который внешне очень похож на официальный. Как правило, основная цель фишинга — получение доступа к конфиденциальным данным пользователя (логинам, паролям, персональным данным и пр.).

Статистика преступлений, совершенных фишерами, говорит о росте данного вида мошенничества. Законодатель даже выделил этот метод в отдельный квалифицирующий признак, дополнив уголовное законодательство в 2012 году ст. 159.6 УК РФ — мошенничество в сфере компьютерной информации.

Так, по официальным данным ГИАЦ МВД России статистика мошенничества в сфере компьютерной информации характеризуется следующими показателями (табл. 1).

Таблица 1 – Число преступлений по ст. 159.6 УК РФ по округам России за период 2019–2024 г. г. (по данным ГИАЦ МВД РФ)

[Table 1 – Number of crimes under Article 159.6 of the Criminal Code of the Russian Federation by districts of Russia for the period 2019–2024 (according to the State Information and Analytical Center of the Ministry of Internal Affairs of the Russian Federation)]

Территория	2019	2020	2021	2022	2023	6 мес 2024
Центральный ФО	81	63	49	72	207	13
Северо-Западный ФО	77	48	8	0	23	30
Северо-Кавказский ФО	9	7	24	18	4	5
Южный ФО	27	75	37	35	47	37
Приволжский ФО	321	379	195	182	16	13
Уральский ФО	108	114	27	8	33	1
Сибирский ФО	35	23	46	4	23	5
Дальневосточный ФО	22	45	44	6	64	4
Всего по России	687	761	431	334	417	109

При этом наблюдается некоторый разрыв в показателях по различным регионам в разные периоды времени (стабильный рост в последние годы в Центральном ФО до 207 и в то же время снижение в Северо-Кавказском ФО до 4). При этом число лиц, совершивших преступления, стабильно низкое, подтверждающее, что преступники совершают, как правило, несколько преступлений одного вида, преступления многоэпизодные.

Так, число лиц, совершивших преступления по ст. 159.6 УК РФ, характеризуются следующими данными (табл. 2).

Стабильно высокие показатели числа преступников в Приволжском ФО, стабильно низкие — в Северо-Западном, Северо-Кавказском, Дальневосточном и Сибирском ФО.

Мировой опыт подтверждает распространённость данного вида преступности. По данным «Лаборатории Касперского»¹ чаще всего с фишингом сталкивались

пользователи из Перу (19,06 %). Второе место занимает Греция (18,21 %), далее находятся Вьетнам (17,53 %) и Мадагаскар (17,17 %). После них с небольшим отрывом друг от друга идут Эквадор (16,90 %), Лесото (16,87 %) и Сомали (16,70 %).

В большинстве случаев кибермошенники полагаются не только на отсутствие у пользователей информационной грамотности в сфере кибербезопасности, но и на инструменты социальной инженерии, опирающиеся на человеческую доверчивость, чувства сострадания, делая упор на оперативности принимаемых решений.

Фишинговое сообщение обычно отправляется от имени официальных лиц — государственных органов (органов власти, силовых ведомств, социальных служб и т. д.), операторов связи (причем без привязки к используемому жертвой оператору), кредитно-финансовых организаций, а также руководства организаций-партнеров, клиентов или просто сотрудников и знакомых. В содержании таких сообщений содержатся различные данные (от требований органов власти, изменений

¹ Аналитика утечки персональных данных // Официальный сайт Лаборатории Касперского. URL: <https://www.kaspersky.ru/> (дата обращения: 01.03.2025).

Таблица 2 – Выявлено лиц, совершивших преступления по ст. 159.6 УК РФ (по данным ГИАЦ МВД РФ)

[Table 2 – Identified persons who committed crimes under Article 159.6 of the Criminal Code of the Russian Federation (according to the data of the Main Information and Analytical Center of the Ministry of Internal Affairs of the Russian Federation)]

Территория	2019	2020	2021	2022	2023	6 мес 2024
Центральный ФО	29	10	8	14	7	1
Северо-Западный ФО	2	0	1	1	1	0
Северо-Кавказский ФО	2	5	2	0	0	0
Южный ФО	5	11	1	4	1	2
Приволжский ФО	9	6	10	4	6	0
Уральский ФО	9	1	0	1	5	3
Сибирский ФО	8	8	1	0	3	0
Дальневосточный ФО	6	4	4	1	2	1
Всего по России	82	49	34	26	25	7

в законодательстве до необходимости погашения задолженностей по налогам, либо просто просмотр вложенного документа). При этом ссылки могут быть прямыми — на фишинговый сайт. А могут содержать даже pdf-файлы с доступом предварительного просмотра в web-интерфейсе. При «открытии» такого файла происходит автоматический переход по вредоносной ссылке, содержащей отдельные символы, дублирующие посещаемый ресурс, однако ничего общего с ним не имеющий, кроме наличия последовательности этих символов.

Все чаще регистрируются случаи мошенничества с компрометацией корпоративной электронной почты или обмана через известные маркетплейсы и интернет-сервисы размещения бесплатных объявлений.

Учитывая осведомленность пользователей о возможностях фишинговых атак, злоумышленники прибегают к различным уловкам — например, рассылая вирусные сообщения и маскируя их под автоматические уведомления Google-календаря либо обновления уже установленных при-

ложений. Тем самым кибермошенники получают больше возможностей доступа к конфиденциальной информации даже у продвинутых пользователей.

Не получая нужного отклика пользователей через интернет-ресурсы, злоумышленники отправляют подобные сообщения посредством смс-рассылки на телефоны. Такую технику фишинга называют смшингом (smishing). Как правило, этим методом пользуются преступники, маскируясь под банки и направляя пользователей либо на поддельные сайты банков (с авторизацией), либо на сайт для установки приложения в целях обеспечения надежной защиты вкладов (при этом обязательно присутствует «гриф» — срочно).

Мошенники всегда реагируют на актуальные тренды и новости. Не стал исключением и продолжающийся рост мошеннических действий в отношении престарелых людей, участников СВО и их семей по поводу дополнительных выплат и льгот в преддверии 80-летия Победы, в отношении пользующимися популярностью отдельными товарами и услугами (например, «ду-

байский шоколад» или промокоды и сертификаты на крупные суммы на известных маркетплейсах, от имени транспортных компаний и пр.). Фальшивые сайты создают с логотипами известных брендов, через которые злоумышленники распространяют вредоносное ПО или выманивают персональные данные.

Используя поддельные QR-коды, мошенники направляют жертву на мошеннический сайт или на ссылку вредоносной программы. При этом предлогов для перехода по QR-коду достаточно. Это могут быть приглашения для вступления в чат жилого дома (через расклейку объявлений в подъездах, распространения информации через почтовые ящики, даже через поддельные квитанции). Поддельные QR-коды даже встречаются в известных музеях на экспонатах для ознакомления с историей их возникновения — просто настоящий QR-код клеивается подложным. Также коды могут приходиться через взломанные аккаунты знакомых с просьбой проголосовать на конкурсе за сына (дочь, друга, племянницу и т. д.).

Отдельного внимания заслуживают преступные действия для незаконного доступа к личному кабинету на Госуслугах¹. И тут мошенники используют различные предлоги: запись к врачам-специалистам, необходимость обновления данных в электронном журнале школьника (причем, сообщения приходят как родителям, так и самим детям), запись на экзамены (ОГЭ, ЕГЭ) и др. Помимо сообщений и рассылки кодов эти сообщения еще дублируются звонками, в основном, через мессенджеры. Далее следует просьба сообщить код из смс-сообщения, который на самом деле предназначен для доступа к личному кабинету Госуслуг.

Появился и новый вид преступления — криптоджекинг. В этой атаке используются скрипты для майнинга криптовалют в браузерах без согласия пользователя. Атаки криптоджекинга могут включать загрузку

программного обеспечения для майнинга криптовалюты в систему жертвы. Многие атаки зависят от кода JavaScript, который выполняет анализ данных в браузере, если в браузере пользователя открыта вкладка или окно на вредоносном сайте. Никакого вредоносного ПО не требуется устанавливать, поскольку при загрузке затронутой страницы выполняется код майнинга в браузере.

Кибершпионаж предполагает взлом киберпреступниками систем или сетей с целью получения доступа к конфиденциальной информации, хранящейся у правительства или другой организации. Нападения мотивированы прибылью или идеологией. Кибершпионаж включает в себя кибератаки, направленные на сбор, изменение или уничтожение данных, а также использование подключенных к сети устройств, таких как веб-камеры или камеры видеонаблюдения, для слежки за целевым лицом или группами и мониторинга коммуникаций, включая электронную почту, текстовые сообщения и мгновенные сообщения.

Впечатляют и суммы ущерба от таких действий злоумышленников [23, с. 280]. Так, по предварительным данным только за два месяца (в декабре 2024 и январе 2025 года) зафиксировано не менее 400 атак на клиентов ведущих российских банков, средняя сумма списания составила около 100 тыс. рублей².

На ежегодном расширенном заседании коллегии МВД России³ было отмечено об увеличении материального ущерба от кибермошенничества. Только в России в 2024 году ущерб составил более 200 млрд рублей, в 2023 году сумма составляла 156 млрд рублей, а за предыдущие три года (с 2019 по 2022) — около 350 млрд рублей. Причем, более четверти всех обманутых в 2024 году — люди пенсионного возраста.

² Фишинг в России // Официальный сайт TAdviser. URL: <https://www.tadviser.ru/index.php> (дата обращения: 02.04.2025).

³ Состояние преступности // Официальный сайт МВД РФ. URL: <https://мвд.рф/dejatelnost/statistics> (дата обращения: 05.04.2025).

¹ Защита персональных данных // Официальный сайт TAdviser. URL: <https://www.tadviser.ru/index.php> (дата обращения: 02.03.2025).

Злоумышленникам, используя новые схемы совершения преступлений и способы их сокрытия, все чаще удается уходить от правосудия — раскрываемость таких преступлений в 2024 году снизилась до 23 %. Это свидетельствует о наличии определенных трудностей в обнаружении, фиксации и изъятии улик. К сожалению, практика показывает, что противостоять можно только уже налаженным схемам обхода защиты данных. И здесь работать на опережение не всегда представляется возможным. По итогам анализа правоприменительной практики более трети (34,8 %) зарегистрированных в 2023 г. преступлений совершается с использованием информационно-коммуникационных технологий (ИКТ) или в сфере компьютерной информации (всего 677 тысяч), из них 70,2 % совершается путем кражи или мошенничества (475,3 тысячи). При этом за 2023 г. зафиксирован рост на 30 % преступлений, совершаемых с использованием ИКТ, рост продолжился и в 2024 году. При совершении преступлений в рассматриваемой сфере чаще всего злоумышленники использовали сеть Интернет (в 2023 г.: 77,8 %, 526,8 тысяч, рост 38,2 %; 2024 г.: 81,3 %, 472,3 тысячи, рост 25,1 %), мобильную связь (в 2023 г.: 44,7 %, 302,9 тысячи, рост 42,2 %; 2024 г.: 46,7 %, 260,7 тысячи, рост 18,4 %). Также отмечается существенное увеличение количества преступлений, связанных с неправомерным доступом к компьютерной информации — их доля в общем числе преступлений, совершаемых с использованием ИКТ, выросла

в 6,8 раз. При этом раскрываемость таких преступлений остается крайне низкой (5,6 %).

Общие выводы по результатам проведенного исследования

Повсеместное внедрение современных информационных технологий позволило совершать традиционные преступления в виртуальном пространстве.

Мошенничество в новых условиях стало возможным совершать в сфере компьютерной информации [24; 25]. Официальные статистические данные свидетельствуют о широком распространении данного вида преступности не только на территории России, но и в мире. При этом стремительно увеличивается и материальный ущерб от кибермошенничества (только в России в 2024 году ущерб составил более 200 млрд рублей — рост составил более 30 % по сравнению с аналогичным показателем прошлого года). При этом раскрываемость киберпреступлений остается низкой (около 6 %).

Основной задачей на современном этапе является эффективное и оперативное противостояние преступности, к каким бы способам и методам не прибегали злоумышленники. Помимо повышения уровня информационной безопасности пользователей необходимы меры по недопущению несанкционированного доступа к компьютерной информации, введение двухфакторной аутентификации, а также блокировка подозрительных операций.

Список источников

1. Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия. Москва: Право и Закон, 1996. 182 с.
2. Абрамян Т. А. Актуальные проблемы привлечения к ответственности лиц за преступления в сфере информационных технологий // Юрист. 2018. № 5. С. 68–72. DOI: <https://doi.org/10.18572/1812-3929-2018-5-68-72>.
3. Простосердов М. А. Проблемы квалификации компьютерных преступлений // Российское правосудие. 2012. № 6(74). С. 106–108.
4. Лысак Е. А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГА У. 2013. № 90. С. 997–1006.
5. Ефремова М. А. Уголовно-правовая охрана информационной безопасности: монография. Москва, 2018. 306 с.

6. Зорина Н. С. Информационная безопасность подростков в Интернете как средство предупреждения преступности среди несовершеннолетних // Закон и право. 2022. № 2. С. 152–155. DOI: <https://doi.org/10.24412/2073-3313-2022-2-152-155>
7. Кошечкина Е.А., Новиков С. В. К вопросу о проблемах законодательства в сфере кибертерроризма // Омский научный вестник. Серия Общество. История. Современность. 2017. № 4. С. 101–105.
8. Завьялова Д. В. Транснациональная кибербезопасность как объект криминалистического обеспечения // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 3. С. 160–165. DOI: <https://doi.org/10.17803/2311-5998.2019.55.3.160-165>
9. Шевко Н. Р. Кибербезопасность: состояние и перспективы // Державинские чтения: сборник статей XVI Международной научно-практической конференции. Москва, 2021. С. 168–170.
10. Русскевич Е. А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Международное уголовное право и международная юстиция. 2018. № 3. С. 10–13.
11. Zhou Z., Tang H., Tian Y., Wei H., Zhang F., Morrison C. M. Cyberbullying and its risk factors among Chinese high school students // School Psychology International. 2013. Vol. 34, No. 6. P. 630–647. DOI: <https://doi.org/10.1177/0143034313479692>
12. Aricak T., Siahhan S., Uzunhasanoglu A., Saribeyoglu S., Ciplak S., Yilmaz N., Memmedov C. Cyberbullying among Turkish adolescents // Cyberpsychology & behavior. 2008. Vol. 11, No. 3. P. 253–261. DOI: <https://doi.org/10.1089/cpb.2007.0016>.
13. Topçu Ç., Erdur-Baker Ö., Çapa-Aydin Y. Examination of cyberbullying experiences among Turkish students from different school types // Cyber Psychology & Behavior. 2008. Vol. 11, No. 6. P. 643–648. DOI: <https://doi.org/10.1089/cpb.2007.0161>.
14. Шевко Н.Р., Исхаков И. И. Особенности проявления кибербуллинга в социальных сетях // Ученые записки Казанского юридического института МВД России. 2017. Т. 2, № 3. С. 19–22.
15. Простосердов М. А. Вымогательство, совершенное в сети Интернет // Библиотека криминалиста. Научный журнал. 2013. № 6 (11). С. 150–152.
16. Простосердов М. А. Легализация денежных средств в киберпространстве // Российское правосудие. 2014. № 9 (101). С. 75–80.
17. Шевко Н. Р. Кибермошенничество в России: способы совершения и пути решения проблемы // Вестник НЦБЖД. 2021. № 1 (47). С. 125–130.
18. Бриллиантов А.В., Простосердов М. А. Актуальные вопросы квалификации мошенничества с использованием платежных карт и средств компьютерной техники // Библиотека уголовного права и криминологии. 2017. № 5 (23). С. 163–171.
19. Юхименко Д.М.-К. Преступления против собственности с применением информационных технологий // Социальное управление. 2023. Т. 5, № 5. С. 218–229.
20. Иванова Л. В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25–33. DOI: <https://doi.org/10.25136/2409-7136.2019.1.28600>
21. Шевко Н. Р. Киберпреступность: состояние и перспективы // Актуальные проблемы правоохранительной деятельности органов внутренних дел на современном этапе: материалы всероссийской научно-практической конференции. Казань, 2019. С. 221–227.
22. Мордвинов К. В., Удавихина У. А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1 (11). С. 83–88.
23. Шевко Н. Р. Мошенничество в киберпространстве: реальный ущерб в виртуальном мире // Вестник Восточно-Сибирского института МВД России. 2023. № 3 (106). С. 276–284.
24. Кириченко Е.В., Дмитренко А. В. Проблемы квалификации мошенничества в компьютерной информации: уголовно-правовые и криминологические аспекты // Вестник науки. 2025. Т. 3, № 3(84). С. 160–165.
25. Кунц Е. В. Противодействие современным киберпреступлениям // Российско-азиатский правовой журнал. 2025. № 1. С. 97–104. DOI: [https://doi.org/10.14258/ralj\(2025\)1.15](https://doi.org/10.14258/ralj(2025)1.15)

References

1. Vekhov VB *Computer crimes: Methods of commission and detection*. Moscow: Pravo i Zakon, 1996. 182 p. (In Russ.).
2. Abramyan TA Actual problems of bringing to justice persons for crimes in the field of information technology. *Jurist*. 2018;(5):68-72. (In Russ.). DOI: <https://doi.org/10.18572/1812-3929-2018-5-68-72>.
3. Prostoserdov MA Problems of qualification of computer crimes. *Russian justice*. 2012;(6):106-108. (In Russ.).
4. Lysak EA Problems of qualification of crimes in the field of computer information. *Scientific journal of KubSA U*. 2013;(90):997-1006. (In Russ.).
5. Efremova MA. *Criminal-legal protection of information security*: [monograph]. Moscow, 2018. 306 p. (In Russ.).
6. Zorina NS. Information security of adolescents on the Internet as a means of preventing crime among minors. *Law and Right*. 2022;(2):152-155. (In Russ.). DOI: <https://doi.org/10.24412/2073-3313-2022-2-152-155>
7. Koshechkina EA, Novikov SV. On the issue of problems of legislation in the field of cyberterrorism. *Omsk Scientific Bulletin. Series Society. History. Modernity*. 2017;(4):101-105. (In Russ.).
8. Zavyalova DV. Transnational cybersecurity as an object of forensic support. *Bulletin of the O. E. Kutafin Moscow State Law University (MSAL)*. 2019;(3):160-165. (In Russ.). DOI: <https://doi.org/10.17803/2311-5998.2019.55.3.160-165>
9. Shevko NR. Cybersecurity: Status and Prospects. *Derzhavin Readings: Collection of Articles from the XVI International Scientific and Practical Conference*. Moscow, 2021:168-170. (In Russ.).
10. Russkevich EA. International Legal Approaches to Counteracting Crimes Committed Using Information and Communication Technologies. *International Criminal Law and International Justice*. 2018;(3):10-13. (In Russ.).
11. Zhou Z, Tang H, Tian Y, Wei H, Zhang F, Morrison CM. Cyberbullying and its risk factors among Chinese high school students. *School Psychology International*. 2013;34(6):630-647. DOI: <https://doi.org/10.1177/0143034313479692>
12. Aricak T, Siyahhan S, Uzunhasanoglu A, Saribeyoglu S, Ciplak S, Yilmaz N, Memmedov C. Cyberbullying among Turkish adolescents. *Cyberpsychology & behavior*. 2008;11(3):253-261. DOI: <https://doi.org/10.1089/cpb.2007.0016>.
13. Topçu Ç, Erdur-Baker Ö, Çapa-Aydin Y. Examination of cyberbullying experiences among Turkish students from different school types. *Cyber Psychology & Behavior*. 2008;11(6):643-648. DOI: <https://doi.org/10.1089/cpb.2007.0161>.
14. Shevko NR, Iskhakov II. Features of cyberbullying manifestation in social networks. *Scientific notes of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*. 2017;2(3):19-22. (In Russ.).
15. Prostoserdov MA. Extortion committed on the Internet. *Criminologist's Library. Scientific journal*. 2013;(6):150-152. (In Russ.).
16. Prostoserdov MA. Legalization of funds in cyberspace. *Russian justice*. 2014;(9):75-80. (In Russ.).
17. Shevko NR. Cyberfraud in Russia: methods of committing and solutions to the problem. *Bulletin of the National Center for Criminal Justice*. 2021;(1):125-130. (In Russ.).
18. Brilliantov AV, Prostoserdov MA. Actual issues of qualification of fraud using payment cards and computer equipment. *Library of Criminal Law and Criminology*. 2017;(5):163-171. (In Russ.).
19. Yukhimenko DM.-K. Crimes against property using information technologies. *Social management*. 2023;5(5):218-229. (In Russ.).
20. Ivanova LV. Types of cybercrimes under Russian criminal law. *Legal studies*. 2019;(1):25-33. (In Russ.). DOI: <https://doi.org/10.25136/2409-7136.2019.1.28600>
21. Shevko NR. Cybercrime: status and prospects. *Actual problems of law enforcement activities of internal affairs bodies at the present stage: materials of the all-Russian scientific and practical conference*. Kazan, 2019:221-227. (In Russ.).
22. Mordvinov KV, Udavikhina UA. Cybercrime in Russia: Current Challenges and Successful Practices in the Fight against Cybercrime. *Theoretical and Applied Jurisprudence*. 2022;(1):83-88. (In Russ.).

23. Shevko NR. Fraud in Cyberspace: Real Damage in the Virtual World. *Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia*. 2023;(3):276-284. (In Russ.).

24. Kirichenko EV, Dmitrenko AV. Problems of Calibration of Fraud in Computer Information: Criminal Law and Criminological Aspects. *Bulletin of Science*. 2025;3(3):160-165. (In Russ.).

25. Kunts EV. Counteracting modern cybercrimes. *Russian-Asian Legal Journal*. 2025;(1):97-104. (In Russ.). DOI: [https://doi.org/10.14258/ralj\(2025\)1.15](https://doi.org/10.14258/ralj(2025)1.15)

ИНФОРМАЦИЯ ОБ АВТОРАХ

Шевко Наиля Рашидовна

Кандидат экономических наук, доцент, доцент кафедры Информационные технологии и интеллектуальные системы, Казанский государственный энергетический университет.

420066, Россия, г. Казань, Респ. Татарстан, ул. Красносельская, 51.

mos_shev@mail.ru

<https://orcid.org/0000-0003-1092-3389>

Лукина Марина Алексеевна

Старший преподаватель кафедры правовой информатики, информационного права и естественно-научных дисциплин, Казанский филиал Российского государственного университета правосудия.

420088, Россия, г. Казань, Респ. Татарстан, ул. 2-я Азинская, 7А.

lukina_m@mail.ru

<https://orcid.org/0000-0002-2792-2190>

INFORMATION ABOUT THE AUTHORS

Nailya R. Shevko

Candidate of Economic Sciences, Associate Professor, Associate Professor Department of Information Technologies and Intelligent Systems, Kazan State Energy University,

51 Krasnoselskaya st., Kazan, Rep. Tatarstan 420066, Russia.

mos_shev@mail.ru

<https://orcid.org/0000-0003-1092-3389>

Marina A. Lukina

Senior Lecturer, Department of Legal Informatics, Information Law and Natural Sciences, Kazan Branch of the Russian State University of Justice,

7A 2nd Azinskaya st., Kazan, Rep. Tatarstan 420088, Russia.

lukina_m@mail.ru

<https://orcid.org/0000-0002-2792-2190>

ВКЛАД АВТОРОВ

Все авторы сделали эквивалентный вклад в подготовку публикации.

AUTHORS' CONTRIBUTIONS:

All authors made an equivalent contribution to the preparation of the publication.

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 17.04.2025.

Дата рецензирования статьи / Revised: 27.05.2025.

Дата принятия статьи к публикации / Accepted: 10.06.2025.