

Дата поступления рукописи в редакцию: 20.06.2026 г.

DOI: 10.24412/2782-3849-2026-6-227-232

Дата принятия рукописи в печать: 25.06.2026 г.

ГЕНАДЬЕВА Ольга Александровна,

преподаватель кафедры специальных дисциплин Краснодарского университета МВД России, майор полиции,

e-mail: mail@law-books.ru

МАЛЬЦЕВ Сергей Михайлович,

преподаватель кафедры тактико-специальной подготовки Волгоградской академии МВД России, полковник полиции, кандидат юридических наук,

e-mail: mail@law-books.ru

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПЛЕНИЯМ СОВЕРШАЕМЫМ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СРЕДЕ: МОШЕННИЧЕСТВО И ЕГО ВИДЫ

Аннотация. Автор научной статьи проводит комплексное исследование мошенничества в сфере информационных технологий.

В статье анализируются как сами способы совершения преступлений в интернете, так и их причины, а также оцениваются угрозы и масштабы использования цифровой среды в противоправных целях.

Исследуются трудности, возникающие при пресечении таких преступлений, которые ставят перед правоохранительными и законодательными органами серьезные задачи.

В заключение автор предлагает законодательные пути решения проблем и рассматривает особенности раскрытия преступлений в данной области.

Ключевые слова: кибермошенничество, цифровизация, экономика, информационно-телекоммуникационная среда, информация, преступление, противодействие, мошенничество, денежные средства, правоохранительные органы, законодательство, имущество, защита.

GENADIEVA Olga Aleksandrovna,

Lecturer in the Department of Specialized Disciplines Krasnodar University of the Ministry of Internal Affairs of Russia Police Major

MALTSEV Sergey Mikhailovich,

Lecturer, Department of Tactical and Specialized Training Volgograd Academy of the Ministry of Internal Affairs of Russia Police Colonel, PhD in Law

ON COUNTERING CYBERCRIMES COMMITTED IN THE INFORMATION AND TELECOMMUNICATIONS ENVIRONMENT: FRAUD AND ITS TYPES

Annotation. The author of this scientific article conducts a comprehensive study of information technology fraud.

The article analyzes both the methods and causes of online crimes, and assesses the threats and scale of illegal use of the digital environment. The difficulties encountered in preventing such crimes, which pose significant challenges for law enforcement and legislative bodies, are explored.

In conclusion, the author proposes legislative solutions and examines the specifics of solving crimes in this area.

Key words: cyberfraud, digitalization, economics, information and telecommunications environment, information, crime, counteraction, fraud, funds, law enforcement, legislation, property, protection.

С развитием цифровой экономики, когда информация стала дешевле в обработке, а интернет стал доступнее для широкого круга пользователей, преступники получили новые инструменты для своей деятельности.

В результате, мошенничество, особенно с использованием банковских карт, мобильных устройств и компьютерной техники, стало одним из самых частых преступлений. Под компьютерным мошенничеством понимаются любые действия, направленные на изменение компьютерных данных или нарушение работы систем, которые приводят к лишению кого-либо собственности.

Следовательно, главным объектом защиты в данном случае являются общественные отношения, связанные с собственностью, а предметом посягательства может выступать любое имущество, включая электронные и безналичные средства.

В рамках уголовно-правовой науки мошенничество традиционно относится к числу составов преступлений, отличающихся высокой степенью изученности.

Тем не менее, увеличение числа преступлений, совершаемых злоумышленниками посредством информационно-телекоммуникационной среды, порождает необходимость усовершенствования мер по повышению качества по их выявлению, раскрытию и расследованию.

Наряду с этим, наблюдается рост числа зарегистрированных преступлений, при этом методы их совершения в сети Интернет создает все больше затруднений в своевременном их выявлении и пресечении.

Применение информационного пространства в противоправных целях как таковой является и серьезной угрозой современного общества, так и своего рода вызовом обращенным органам государственной власти, а также различным заинтересованным государственным ведомствам и правоохранительным органам, одним из приоритетных направлений которых является реализация установленных в статье 1 ФЗ «О полиции» №3, то есть предназначение полиции, где говорится, что полиция предназначена в том числе и для борьбы с преступностью, обеспечения общественного порядка и безопасности, а также сохранности их имущества.

На сегодняшний день, прогресс цифровых технологий в различных областях, несомненно создает все новые и новые угрозы, в том числе связанные с распространением преступлений совершаемых в интернет пространстве, при этом характеризуется своей специфичностью, международным масштабом,

регулярно проявляющейся в различных формах и способах проявлений, высоким уровнем скрытности, что в последствии подтверждает применение недостаточно действенных способов и профилактических мер по противодействию данному виду преступления, во всех видах ее проявления в социальном обществе.

В целях обеспечения действенных мер, направленных на эффективное противодействие противоправным проявлениям в рассматриваемой сфере, где одним из наиболее распространенных видов латентной преступности является мошенничество, посредством информационно-телекоммуникационной среды, требуется эффективное применение уголовно-правовых норм.

В контексте развития информационных технологий и повсеместной цифровизации, справедливо будет отметить и тот факт, что новейшие достижения науки и технические разработки несомненно упрощают определенные потребности и услуги в сфере информатизации, но именно недостаточная грамотность и защищенность своих информационных ресурсов и чрезмерное проявление доверия в особенности определенного слоя населения и способствует успешному совершению преступления в сети Интернет и распространению такого вида противоправного действия как кибермошенничество.

В качестве примера можно выделить упрощенную систему оплаты жилищно-коммунальных и иных услуг или же совершение покупок различных товаров и вещей через онлайн магазины, которые предполагают оплату через систему электронных платежей, путем транзакции на различные счета и передача определенной информации в при совершении товаров первой необходимости через онлайн-сервисы с последующей доставкой.

Но главная проблема в том, что далеко не все представители нашего общества, при чем в наше время, время постоянного совершенствования и развития информационных технологий и возможностей намерены применять услуги цифровизации благих целях, как качество улучшения качества своих жизненных и иных материальных потребностей, а напротив посредство преступных проявлений в данной сфере, пытаются обеспечить себя и финансово и материально, причиняя в некоторых случаях значительный ущерб своим потенциальным жертвам, тем самым представляют угрозу обществу.

Исходя из этого, можно констатировать факт зарождения преступной деятельности, в данной сфере получившее широкое распространение это есть ничто иное как средство

легкого пути к обогащению, а информационные возможности и навыки злоумышленников, это способы и ресурсы к достижению их противоправных целей, по обогащению за счет государства и определенного слоя населения располагающего значительными и иными материальными средствами и финансовыми возможностями, что требует ужесточение применения санкций за преступления в данной сфере, как один из методов профилактики противодействия этим проявлениям и способом реализации превентивных мер воздействия и на мошеннические действия.

Противодействие преступлениям в цифровой среде и по сей день остается актуальной ввиду его стремительного роста, в сравнении с другими киберпреступлениями, такими как: фишинг, киберджекинг, кибершпионаж.

Основным механизмом противодействия является превенция, предполагающая предъявление требований к поставщикам информационных услуг о предоставлении личной информации о клиентах, в целях последующего использования в преступных целях, что и есть не что иное как кибермошенничество, включающее в себя кибершантаж, утечка информации и получение выгоды.

Кибермошенничество, как вид преступления в информационном пространстве достаточно выявить, поскольку данное противоправное действие реализуется в цифровом пространстве с помощью методов шифрования, используя различные вредоносное обеспечение, что придает ему латентный характер в момент реализации злоумышленником преступных посягательств на цифровую среду потенциальной жертвы, что являет собой противоправную деятельность в информационно-телекоммуникационном пространстве.

Также следует отметить, что такие преступления совершаются с целью – нанесения значительного материального или иного ущерба путем хищения или искажения персональной информации и злоумышленники, действуя в нарушении законодательства, активно применяют компьютерные технологии, периферийные устройства, средства связи и персональные компьютеры

Одним из самых распространенных методов злоумышленников в противоправной деятельности, является заражение устройств вирусами и иными вредоносными программными обеспечениями, скрытыми под видом скачиваемых программ или рекламных баннеров.

После получения доступа, внедренный критическую информационную структуру рабочего компьютера потенциальной жертвы, вредоносное программное обеспечение в виде

вируса, как клавиатурный шпион шифрует все данные пользователя и осуществляет утечку информации или под угрозой искажения или полного уничтожения конфиденциальной информации, начинает шантажировать потенциальную жертву, что называется кибершантажом в среде хакеров.

Масштабное развитие интернета и свободный оборот информации обеспечили благоприятную и доступную почву для появления новых форм кибермошенничества. Эти преступления несут серьезные риски: от потери личных данных обычных граждан до угроз государственной безопасности, включая утечку секретной информации и государственной тайны.

Иначе интерпретируя кибермошенничество, можно охарактеризовать как вид преступной деятельности, реализующейся в информационно-коммуникационном пространстве и суть «предназначения» состоит в причинении значительного материального или иного ущерба посредством утечки информации и неправомерного завладения конфиденциальными сведениями третьего лица с целью получения выгоды или проявления себя, как это делают кибервандалы под угрозой уничтожения информации, а не для целей финансовой выгоды, а показать свои способности в данной сфере.

Преступники, нарушая законодательные нормы, используют персональные компьютеры или иные устройства, подключенные к интернету.

Часто такие преступления совершаются посредством внедрения замаскированных вирусов, которые могут выглядеть как обычные программы, скачанные из сети и заражая персональный компьютер жертвы, начинают манипулировать и требовать плату за сохранение сведений, без искажений.

Стремительный рост популярности интернета привел к тому, что огромные объемы информации стали свободно циркулировать в глобальной сети, что способствовала появлению различных видов преступлений в сети, носящих латентный характер и значительную опасность для пользователей.

Мировое сообщество в ближайшем будущем столкнется с растущей угрозой кибермошенничества, что требует незамедлительных и решительных мер противодействия. Эта проблема находится в центре внимания не только российских правоохранительных органов.

Государство признает особую опасность мошенничества с использованием электронных платежей, считая его более социально значимым, чем традиционные формы. В связи с этим, предпринимаются усилия не только по обеспечению справедливого наказания,

но и по превентивному снижению числа таких преступлений путем совершенствования законодательства.

Интересно, что более высокая общественная опасность не всегда коррелирует с более строгими санкциями: в некоторых случаях наказание за сложные виды мошенничества может быть даже мягче, чем за простые.

Тем не менее, фокусируясь на определенных видах мошенничества, государство направляет ресурсы правоохранительных органов на защиту наиболее критически важных отношений.

Процессуальные аспекты документирования таких преступлений остаются вызовом, поскольку эта категория относительно нова, и единые, отработанные механизмы еще не сформированы.

Стремительное развитие цифровых технологий и появление новых мошеннических схем требуют от правоохранителей постоянного совершенствования методов фиксации преступлений.

Значительная доля киберпреступлений приходится на мошеннические схемы, нацеленные на получение денежных средств от граждан. Преступники мастерски используют убедительные методы, имитируя доверенные роли (например, сотрудников банков), что затрудняет для граждан распознавание обмана.

Российские правоохранительные органы, включая МВД, активно развивают свои возможности в борьбе с киберпреступностью, создавая для этого специализированные структуры.

Одновременно с этим, система подготовки кадров в правоохранительной сфере трансформируется: вводятся новые образовательные программы, нацеленные на формирование специалистов по информационной безопасности и противодействию современным методам несанкционированного доступа к информации.

Проблема киберпреступности носит транснациональный характер и становится все более трудноразрешимой из-за постоянного совершенствования преступных технологий и отставания мер защиты от их темпов развития.

Типичная ситуация заключается в том, что правоохранительные органы получают информацию о преступлении постфактум, что дает киберпреступникам временное преимущество, поскольку защитные меры разрабатываются реактивно, после обнаружения уязвимостей.

Несмотря на положительную динамику в раскрываемости кибермошенничества, значительная доля преступников избегает ответственности.

Это обусловлено их способностью действовать анонимно, используя технические средства, такие как IP-адреса и VPN-серверы, зачастую расположенные за пределами национальной юрисдикции, что существенно затрудняет их идентификацию и привлечение к правосудию.

Среди всего прочего, целесообразно выделить основные направления борьбы с кибермошенничеством и распространенные схемы обмана, для чего государственные органы должны сосредоточить свои усилия на разработке и внедрении мер по пресечению кибермошенничества.

Для эффективной борьбы с подобными преступлениями первостепенное значение имеет усиление мер ответственности.

Параллельно с этим, ключевым направлением станет международное взаимодействие, включающее обмен знаниями с зарубежными правоохранительными структурами и организация и использование общих действенных мер по противодействию преступности в информационной сфере.

Среди наиболее распространенных сегодня видов мошенничества в интернете выделяются телефонные аферы и SMS-мошенничество, когда злоумышленники рассылают сообщения о якобы проблемах с банковскими картами или несанкционированных списаниях средств.

В сообщении указывается номер для связи. Когда гражданин перезванивает, мошенники, выдавая себя за сотрудников банка, выманивают конфиденциальную информацию о банковской карте.

Часто целью является получение доступа к интернет-банкингу через сервисы удаленной регистрации.

Получив доступ к мобильному приложению банка, мошенники могут беспрепятственно похищать средства со всех счетов жертвы.

Телефонные звонки о проблемах с родственниками, очень распространенный метод вхождения в доверие и завязывания диалога с потенциальной жертвой, посредством данного метода преступники звонят на случайные номера, чаще всего пожилым людям, выдавая себя представителей правоохранительных органов и часто по мошеннической схеме сообщают своим потенциальным «клиентам» о якобы каких-либо негативных ситуациях в которые попали их близкие и под предлогом оказания помощи в разрешении проблемных обстоятельств, начинают манипулировать и предлагать платные услуги, на что они соглашаются и в процессе перевода денежных средств для оплаты, не понимая, что это мошенники сообщают свой

персональные данные и сведения о своих реквизитах и злоумышленники совершают незаконные транзакции с их счетов.

Они сообщают о задержании близкого родственника за совершение преступления и предлагают «урегулировать» вопрос за определенную сумму.

В состоянии растерянности жертвы переводят деньги по указанным реквизитам (номер телефона, карты, электронного кошелька) или передают наличные через посредника, в большинстве случаев реализуется осужденными.

Телефонные звонки о социальных выплатах, не менее распространенный вид мошенничества наряду с другими видами киберпреступлений и рассчитаны завести в заблуждение и путем обмана, злоумышленники мошенники под предлогом оказания услуг в получении различных социальных выплат, обманывают наиболее и нуждающийся слой населения.

Представляясь сотрудниками Пенсионного фонда, органов социальной защиты, полиции или банков, они выманивают данные банковских карт под предлогом перечисления средств. Если у получателя социальной помощи нет банковской карты, мошенники могут использовать другие методы для получения информации.

Злоумышленники, также действуют и на бесплатных онлайн-площадках объявлений и для осуществления своих противоправных действий используют следующую тактику: они размещают объявления с очень привлекательными ценами, чтобы заманить покупателей.

Затем, при обращении потенциального клиента, они требуют предоплату или полную оплату переводами, при этом отказываются ознакомить с покупкой, отвлекая внимания покупателя тем, что это ограниченный в количестве товар, а цена ниже рыночной и необходимо произвести быструю транзакцию.

В случае успешного проведения транзакции, соответственно преступники прекращают какую – либо переписку, удаляют или блокируют контакт.

Мошенники создают фальшивые онлайн-магазины, имитирующие известные бренды и предлагающие товары по подозрительно низким ценам.

Это делается для того, чтобы привлечь как можно больше покупателей. Люди, желающие приобрести такие товары, оставляют на сайте свои контактные данные и оформляют заказы.

Затем злоумышленники связываются с ними, подтверждают покупку и требуют предоплату.

После получения денег, они некоторое

время поддерживают связь, обещая доставку и ссылаясь на непредвиденные задержки. Как только им удастся обмануть достаточное количество людей, они исчезают вместе с деньгами, прекращая всякое общение.

В социальных сетях мошенники прибегают к следующей схеме: они пытаются взломать учетные записи пользователей. В случае успешного взлома, они используют аккаунт жертвы для рассылки сообщений.

Эти сообщения обычно содержат информацию о некоей неприятной ситуации, в которой якобы оказался владелец аккаунта, и содержат просьбу о финансовой помощи, например, пополнить банковскую карту или совершить перевод на указанный счет.

Анализ представленной информации позволяет констатировать возрастающую актуальность противодействия мошенничеству в информационно-телекоммуникационной сфере, обусловленную его экспоненциальным ростом.

Для эффективного решения обозначенной проблемы государству необходимо разработать адекватные правовые механизмы для квалификации действий, совершаемых в глобальном цифровом пространстве. Важно также повысить уровень ответственности за распространение запрещенного контента и создать четкие организационно-правовые структуры для борьбы с незаконной деятельностью в данной сфере и именно такой всесторонний, интегрированный подход способен обеспечить полную защиту всех направлений человеческой деятельности от мошеннических посягательств.

Список литературы:

[1] Федеральный закон от 01.04.2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» (ред. от 31.07.2025) // СЗ РФ. 2025. № 14. Ст. 1574; № 31. Ст. 4679.

[2] Федеральный закон от 31.07.2025 г. № 281-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях и Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СЗ РФ. 2025. № 31. Ст. 4635.

[3] Федеральный закон от 28.12.2025 г. № 508-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СЗ РФ. 2025. № 52 (ч. 1). Ст. 8295.

[4] Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

[5] Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. 2). Ст. 5351.

[6] Иванова Л.В., Пережогина Г.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6, № 4 (24).

[7] Лункашу Ю.В., Макаренко И.А. Профилактика в деятельности правоохранительных органов при противодействии правонарушениям, связанным с информационными технологиями // Информационные технологии в деятельности правоохранительных органов: современное состояние, проблемы и перспективы: сб. науч. статей. Орел, 2023.

[8] Механизмы и модели регулирования цифровых технологий: монография / под ред. А.В. Минбалева. М., 2020.

[9] Митряев И.С. Отдельные вопросы расследования правонарушений, совершаемых с использованием современных информационных технологий // Информационные технологии в деятельности правоохранительных органов: современное состояние, проблемы и перспективы: сб. науч. статей. Орел, 2023.

[10] Николахин, А.Ю. Использование технологии VPN для обеспечения информационной безопасности // Экономика и качество связи. 2018. № 3.

[11] Новгородов Д.А. Совершение административного правонарушения в сети Интернет как квалифицирующий признак // Административное право и практика администрирования. 2022. № 2.

References:

[1] Federal Law No. 01.04.2025 of 41-FZ "On the Creation of a State Information System for Combating Offenses Committed Using Information and Communication Technologies and on Amending

Certain Legislative Acts of the Russian Federation" (as amended by 31.07.2025) // RF NW. 2025. № 14. Art. 1574; № 31. Art. 4679.

[2] Federal Law No. 31.07.2025 of 281-FZ "On Amendments to the Code of Administrative Offenses of the Russian Federation and the Federal Law "On Amendments to the Code of Administrative Offenses of the Russian Federation" // of the RF NW. 2025. № 31. Art. 4635.

[3] Federal Law of 28.12.2025 No. 508-FZ "On Amendments to the Code of Administrative Offenses of the Russian Federation" // SZ RF. 2025. No. 52 (part 1). Art. 8295.

[4] Decree of the President of the Russian Federation of 05.12.2016 No. 646 "On Approval of the Information Security Doctrine of the Russian Federation" // SZ RF. 2016. № 50. Art. 7074.

[5] Decree of the President of the Russian Federation of 02.07.2021 No. 400 "On the National Security Strategy of the Russian Federation" // NW RF. 2021. No. 27 (part 2). Art. 5351.

[6] Ivanova L.V., Perezhogina G.V. Digital space as a crime scene under global restrictions // Bulletin of Tyumen State University. Socio-economic and legal studies. 2020. T. 6, NO. 4 (24).

[7] Lunkashu Yu.V., Makarenko I.A. Prevention in the activities of law enforcement agencies in countering offenses related to information technology // Information technology in the activities of law enforcement agencies: current state, problems and prospects: Sat. scientific. articles. Eagle, 2023.

[8] Mechanisms and models of regulation of digital technologies: monograph / ed. A.V. Minbaleeva. M., 2020.

[9] I.S. Mitryaev. Individual issues of investigation of offenses committed using modern information technologies // Information technologies in the activities of law enforcement agencies: current state, problems and prospects: Sat. scientific. articles. Eagle, 2023.

[10] Nikolakhin, A.Yu. Using VPN technology to ensure information security // Economics and quality of communication. 2018. № 3.

[11] Novgorodov D.A. Committing an administrative offense on the Internet as a qualifying feature // Administrative law and administration practice. 2022. № 2.

