МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего профессионального образования
«Уфимский юридический институт МВД Российской Федерации»

Кафедра уголовного права и криминологии

ДИПЛОМНАЯ РАБОТА

на тему **«КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ МОШЕННИЧЕСТВА В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ»**

Выполнил
Пономарев Денис Михайлович,
обучающийся по специальности 40.05.02
Правоохранительная деятельность
2020 года набора, 0201 учебной группы

Руководитель
заместитель начальника кафедры уголовного права и криминологии, к.ю.н.,
полковник полиции,
Нугуманов Азат Римович

К защите рекомендуется
рекомендуется / не рекомендуется
Начальник кафедры _____ И.Р. Диваева
подпись
Дата защиты «___» _____ 2026 г. Оценка _____

ПЛАН

Введение 3
Глава 1. Теоретико-правовые основы интернет-мошенничества 7
§ 1. Понятие и юридическая квалификация мошенничества в сети Интернет 7
§ 2. История развития и современное состояние интернет-мошенничества 16
§ 3. Виды и классификация способов совершения мошеннических действий в глобальной сети 20
Глава 2. Криминологическая характеристика интернет-мошенничества 29
§ 1. Состояние интернет-мошенничества и факторы, способствующие его совершения 29
§ 2. Криминологическая характеристика личности мошенника в сети Интернет 38
§ 3. Предупреждение мошенничества в глобальной сети 47
Заключение 55
Список использованной литературы 59

ВВЕДЕНИЕ

Тема мошенничества в интернете сегодня важна как никогда, потому что наша жизнь всё больше переходит в онлайн. Мы покупаем товары в соцсетях, переводим деньги по номеру телефона, храним сбережения в приложениях банков. Но там же, в цифровом пространстве, активно действуют и мошенники, которые придумывают всё более изощренные способы обмана.

Актуальность темы исследования обусловлена тем, что таких преступлений становится очень много. Статистика показывает, что почти каждое второе преступление в стране так или иначе связано с интернетом или телефонными звонками. Люди теряют огромные суммы – от небольших переводов до миллионов рублей и квартир. И речь не только о деньгах: мошенничество наносит психологический удар, люди чувствуют себя униженными и обманутыми.

Мошенничество в сети быстро меняется. Ещё вчера всех пугали «нигерийскими письмами» и смс «мама, срочно скинь денег», а сегодня преступники используют поддельные голоса и видео, создают сайты-копии банков, взламывают аккаунты в мессенджерах. Они идут в ногу с технологиями, а часто и опережают их. Правоохранителям сложно угнаться за этими схемами, потому что преступник может находиться в другой стране, использовать поддельные сим-карты и анонимные платежные системы.

Криминологическая характеристика личности интернет-мошенника и его жертв имеет свою специфику, отличающуюся от традиционных имущественных преступлений. Анонимность, трансграничный характер сети и техническая опосредованность взаимодействия создают условия, при которых стираются привычные социальные и возрастные границы как преступников, так и потерпевших. Особого внимания требует виктимологический аспект: в условиях тотального проникновения цифровых технологий потенциальной жертвой может стать любой пользователь независимо от уровня образования, социального статуса или возраста.

Существующая система противодействия интернет-мошенничеству сталкивается с рядом объективных трудностей. К ним относятся: межведомственная разобщенность, недостаточная техническая оснащенность правоохранительных органов, сложность получения доказательств в цифровой среде, проблемы международного сотрудничества при расследовании трансграничных преступлений. Кроме того, профилактическая работа зачастую ограничивается информированием населения об уже известных схемах, тогда как мошенники постоянно модифицируют свои методы.

Таким образом, актуальность настоящего исследования определяется необходимостью комплексного криминологического анализа интернет-мошенничества, выявления его детерминант, изучения личностных характеристик участников данного вида противоправной деятельности и разработки на этой основе эффективных мер предупреждения, адекватных современным вызовам и тенденциям развития цифровой среды.

Объектом исследования выступают общественные отношения, складывающиеся в сфере противодействия мошенничеству, совершаемому с использованием глобальной сети Интернет, а также закономерности возникновения и функционирования данного вида преступности как социально-правового явления.

Предметом исследования являются криминологическая характеристика интернет-мошенничества, а также совокупность правовых и организационных мер, направленных на предупреждение данного вида преступлений.

Цель исследования заключается в комплексном криминологическом анализе мошенничества, совершаемого в глобальной сети Интернет.

Поставленная цель определила решение следующих задач:

Для достижения поставленной цели используется совокупность общенаучных и частнонаучных методов познания: диалектический метод, позволяющий рассмотреть явление в развитии; формально-логический метод, применяемый при анализе правовых норм; системно-структурный метод; статистический метод, включающий анализ количественных показателей;

сравнительно-правовой метод, а также метод экспертных оценок.

Степень разработанности темы характеризуется наличием значительного числа исследований, посвященных как общим вопросам мошенничества, так и отдельным аспектам киберпреступности. Теоретические основы изучения мошенничества заложены в трудах Г.Н. Борзенкова, А.И. Бойцова, В.В. Лунеева. Вопросы квалификации мошенничества в сфере компьютерной информации исследовались В.С. Комиссаровым, Ю.В. Гаврилиным, Н.А. Лопашенко. Криминологические аспекты киберпреступности разрабатывались в трудах Ю.М. Батурина, В.В. Крылова, Т.В. Пинкевич, А.Л. Осипенко. Проблемы виктимологического предупреждения поднимались в работах В.И. Полубинского, Д.В. Ривмана. Вместе с тем, стремительное развитие информационных технологий и появление новых способов совершения преступлений требуют дальнейшего научного осмысления данной проблематики, что обусловливает необходимость проведения настоящего исследования.

Теоретическую базу исследования составляют научные труды отечественных и зарубежных ученых в области общей теории права и криминологии, уголовного права и уголовного процесса, криминалистики и оперативно-розыскной деятельности, социологии права, виктимологии, информационной безопасности и психологии.

Нормативную базу исследования образуют Конституция Российской Федерации, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, федеральные законы «Об информации, информационных технологиях и о защите информации», «О национальной платежной системе», «О безопасности критической информационной инфраструктуры Российской Федерации», указы Президента РФ, постановления Правительства РФ, ведомственные нормативные акты, постановления Пленума Верховного Суда РФ в сфере борьбы с киберпреступностью.

Эмпирическую базу исследования составляют официальные данные

ГИАЦ МВД России о состоянии преступности, официальные данные Судебного департамента при Верховном Суде РФ о рассмотрении уголовных дел о мошенничестве, материалы опубликованной судебной практики, включая определения и постановления Верховного Суда РФ и приговоры судов различных инстанций.

Практическая значимость исследования заключается в том, что содержащиеся в нем выводы, предложения и рекомендации могут быть использованы в правоприменительной деятельности сотрудниками правоохранительных органов при выявлении, раскрытии и расследовании данных деяний, а также в профилактической деятельности при разработке программ виктимологического предупреждения и повышения цифровой грамотности населения.

Структура работы определена целью и задачами исследования и состоит из введения, двух глав, включающих в себя шесть параграфов, заключения и списка использованной литературы.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

§ 1. Понятие и юридическая квалификация мошенничества в сети Интернет

Компьютеры (электронные вычислительные машины – ЭВМ) вошли в жизнь человечества сравнительно недавно. Работы по их созданию начались в 1940-х годах практически одновременно в трех странах – СССР, Великобритании и США. В СССР первая ЭВМ была построена в 1950 году. С середины 1990-х годов компьютеры получили повсеместное распространение во всем мире.

Первоначально ЭВМ задумывалась как устройство для математических вычислений. В настоящее же время компьютер превратился в универсальное устройство, используемое практически во всех областях человеческой деятельности для хранения, поиска, получения, передачи, производства и распространения самой различной информации. По прогнозам, в недалеком будущем каждый человек в мире будет иметь доступ к глобальным компьютерным сетям, а компьютерные технологии войдут не только в каждый дом, офис, технологию или производство, но и в большинство используемых человечеством приборов, инструментов, аппаратов и машин[1].

Первая компьютерная сеть появилась в 1960-х годах в министерстве обороны США. К созданной военными исследователями сети присоединились университеты США. Примерно с середины 1980-х годов военные США часть сети стали использовать исключительно в своих целях, а оставшийся сегмент сети постепенно превратился в общедоступный канал связи. Сейчас это Всемирная глобальная компьютерная сеть под названием «Интернет».

Развитие компьютерных технологий привело к тому, что общество

---

[1] Новосельцева А.С. Интернет-мошенничество: ключевые проблемы борьбы и превентивных мер // Актуальные исследования. 2025. № 2. С. 75.

столкнулось с явлениями, представляющими значительную опасность для окружающих, которые ранее не были известны уголовному законодательству (в частности такими, как введение ложной информации в ЭВМ, незаконное использование ЭВМ, нарушение обработки информации, кража информации). Многие государства были вынуждены реагировать на участившиеся случаи использования ЭВМ во вред другим людям и организациям путем принятия специальных уголовных законов. Первым законом в мире, направленным на противодействие компьютерной преступности, стал закон, принятый в США в 1984 году.

Первым официально зарегистрированным компьютерным преступлением, совершенным на территории Советского Союза, было преступление против чужой собственности. В 1979 году в Вильнюсе совершено хищение денежных средств посредством ЭВМ.

Мы живем в информационном обществе, в котором широко представлены информационно-телекоммуникационные (компьютерные) технологии. Количество персональных компьютеров в мире не поддается учету. Растет и количество интернет-пользователей благодаря появлению доступных смартфонов и сравнительно невысоким тарифам на услуги пользования скоростным мобильным Интернетом.

Преступления в сфере компьютерной информации часто называют как «компьютерными преступлениями», так и «киберпреступлениями». Однако единообразия в использовании этих понятий не существует. Например, Т.И. Ястребова и Д.С. Горбунов предпочитают термин «киберпреступность», так как он охватывает более широкий спектр явлений и лучше описывает преступность, связанную с информационным пространством[1].

Э.С. Хмелевский акцентирует внимание на том, что термин «компьютерные преступления» недостаточен для описания всего спектра преступлений, связанных с высокими технологиями. Под киберпреступностью

[1] Ястребова Т.И., Горбунов Д.С. Отдельные проблемы уголовно-правовой характеристики преступлений в сфере компьютерной информации // Научное

она понимает как действия, совершаемые с помощью компьютерной техники и сетей, так и преступления, для которых используются иные способы доступа к киберпространству. Эти деяния могут быть направлены как против самих сетей и данных, так и против систем[1].

О.Е. Атанова предлагает подход, в котором акцент делается на пространстве совершения преступлений – киберпространстве. По ее мнению, оно включает как физические, так и нефизические элементы, создаваемые с помощью компьютеров, сетей и программ. Под киберпреступностью она подразумевает такие действия, как распространение вредоносного программного обеспечения, неправомерный доступ к личным данным, паролям, совершение краж, мошенничество и другие преступления, связанные с использованием современных технологий[2].

В российском законодательстве правонарушения в информационной сфере принято называть «компьютерными преступлениями». Однако это определение носит условный характер, поскольку оно не охватывает все аспекты возможных преступлений, а сам компьютер играет в таких деяниях различные роли. Он может быть как объектом посягательства, так и частью преступления, выполняя функцию технического средства. С.В. Маликов, опираясь на криминалистические исследования, предпочитает использовать термин «киберпреступность». Он определяет киберпреступление как общественно опасное деяние, совершаемое в киберпространстве, которое посягает на общественную безопасность, собственность, права человека и другие охраняемые законом отношения, при этом компьютерная информация становится как предметом преступления, так и средством его подготовки, совершения и скрытия[3].

образование. 2023. № 3. С. 230.

[1] Хмелевский Э.С. Проблемы квалификации преступлений в сфере компьютерной информации / В сб.: Пермский период. Пермь, 2024. С. 451.

[2] Атанова О.Е. Преступления в сфере компьютерной информации как актуальная проблема // Студенческий вестник. 2024. № 37. С. 35.

[3] Маликов С.В. Пробелы уголовного законодательства о преступлениях в сфере компьютерной информации / В сб.: Институциональные основы уголовного права РФ.

Ответственность за компьютерные преступления регулируются главой 28 Уголовного кодекса Российской Федерации (УК РФ). Однако, преступления в сфере компьютерной информации выходят за пределы главы 28 УК РФ. К таким преступления можно отнести специальные виды мошенничества в сфере информационных технологий (ст. 159.3, ст. 159.6 УК РФ).

В настоящее время мошенничество характеризуется тем, что, проникая во все сферы общественной жизни, оно легко приспосабливается к меняющимся рыночным условиям и имеет ярко выраженный интеллектуальный оттенок. Зачастую мошенники действуют под видом организационно-правовых форм, разрешенных законом, используют поддельные банковские и другие финансовые документы и маскируют факт мошенничества в соответствии с гражданско-правовыми сделками, что значительно усложняет расследование этих преступлений.

Понятие мошенничества, совершаемого с использованием всемирной сети, не имеет легального определения, закрепленного в уголовном законе, и представляет собой доктринальную категорию, охватывающую совокупность общественно опасных деяний, объединенных общим признаком использования информационно-телекоммуникационных технологий в качестве инструмента или среды для завладения чужим имуществом[1].

Родовым понятием для данных посягательств выступает хищение чужого имущества или приобретение права на чужое имущество, совершенное путем обмана или злоупотребления доверием. Специфика цифровой среды привносит в классическую конструкцию мошенничества существенные особенности, трансформируя способы воздействия на потерпевшего и создавая новые объекты уголовно-правовой охраны. Отсутствие непосредственного физического контакта между преступником и жертвой, дистанционный характер коммуникации, возможность анонимизации и тиражирования

Краснодар, 2024. С. 505.

[1] Авдеенко В.О. Мошенничество в Интернет // Наука. Промышленность. Оборона: сборник научных статей. Новосибирск, 2025. С. 110.

преступных действий на неограниченный круг лиц, а также активное использование методов социальной инженерии формируют качественно иную картину данного вида преступности, требующую адекватного нормативного регулирования и единообразных подходов к квалификации.

Юридическая оценка подобных деяний базируется на нормах главы 21 УК РФ, где наряду с общей нормой о мошенничестве, закрепленной в статье сто пятьдесят девятой, предусмотрены специальные составы, учитывающие специфику способа совершения преступления. Речь идет о мошенничестве с использованием электронных средств платежа, ответственность за которое установлена ст. 159.3 УК РФ, и о мошенничестве в сфере компьютерной информации, предусмотренном ст. 159.6 УК РФ. Выбор конкретной нормы для квалификации содеянного определяется тем, каким именно образом злоумышленник взаимодействовал с потерпевшим, информационной системой или программным обеспечением в процессе завладения чужим имуществом. Принципиальное значение имеет разграничение ситуаций, когда обман направлен непосредственно на человека, и случаев, когда неправомерное воздействие оказывается на компьютерную информацию или систему, принимающую решение о движении имущества.

Обращаясь к судебной практике, нельзя не отметить положений постановления Пленума Верховного суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (Пленум ВС РФ № 48)[1]. В случае если предметом преступления при мошенничестве являются безналичные денежные средства, то по смыслу положений п. 1 примечаний к ст. 158 УК РФ и ст. 128 ГК РФ содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Исходя из данного

[1] Постановление Пленума Верховного суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» //

положения, можно сделать вывод о том, что в случае с использованием, например, сети Интернет, местом совершения преступления необходимо признавать место совершения общественно-опасного деяния.

Согласно разъяснениям указанного Пленума, если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, например, путем создания поддельных сайтов благотворительных организаций, интернет-магазинов либо использования электронной почты для рассылки дезинформации, то содеянное надлежит квалифицировать по ст. 159 как обычное мошенничество. В подобных случаях сеть выступает лишь каналом коммуникации, средством донесения обманной информации до потерпевшего, который, будучи введенным в заблуждение относительно истинных намерений контрагента или достоверности предоставленных сведений, добровольно передает имущество или право на него. Сама компьютерная система при этом функционирует штатно, без несанкционированного вмешательства в ее работу.

Как считает Н.Ф. Цейтлин, «особого рассмотрения требуют ситуации, когда деяние совершено совместно несколькими лицами из разных государств, однако направлены на достижение единого преступного результата. Наиболее верным является суждение о том, что местом совершения преступления признается территория того государства, где было совершено деяние, вне зависимости от места наступления последствий»[1]. Нам представляется такое решение наиболее удачным и при выборе юрисдикции государства.

В теории уголовного права длительное время велась дискуссия о том, предполагает ли компьютерное мошенничество наличие обмана или злоупотребления доверием как обязательного признака. Пленум ВС РФ № 48 разрешил данный спор, указав, что обман или злоупотребление доверием не

Российская газета. 2017. 11 декабря.

[1] Цейтлин Н.Ф. Преступления, связанные с использованием IT-технологий: проблемы выявления и расследования // Актуальные вопросы охраны общественного

являются способами совершения преступления, предусмотренного ст. 159.6 УК РФ. Тем самым поддержан подход, согласно которому данное деяние характеризуется специфическим способом, не вписывающимся в традиционно выделяемые формы хищения. Само название указанной статьи представляет собой не вполне адаптированный к российской правовой системе термин, тогда как по своей сути данный состав правильнее было бы именовать хищением в сфере компьютерной информации. Однако законодатель сохранил терминологию, и в сложившихся условиях правоприменителю приходится руководствоваться действующей редакцией закона в системном единстве с разъяснениями высшей судебной инстанции[1].

Особую сложность для правоприменения представляют ситуации, когда хищение совершается с использованием электронных средств платежа. В контексте интернет-пространства данный состав приобретает особую актуальность, поскольку значительная часть операций с банковскими картами совершается именно в сети. При квалификации таких деяний необходимо четко отграничивать их от смежных составов. Если злоумышленник получает реквизиты карты путем обмана самого владельца, например, под видом сотрудника банка выведывает у него специальный код и срок действия, и затем использует данные сведения для оплаты покупок в интернете, действия виновного могут быть квалифицированы по ст. 159 УК РФ как обычное мошенничество, поскольку обман был направлен на человека.

В том случае, когда данные карты похищаются путем установки на компьютер жертвы программы-шпиона, перехватывающей вводимые с клавиатуры символы, и затем используются для хищения, содеянное может образовывать состав преступления, предусмотренный ст. 159.6 УК РФ, так как имело место неправомерное вмешательство в функционирование компьютерной системы. Если же преступник завладевает самой картой или ее

порядка и административной деятельности: сборник научных статей. М., 2022. С. 190.

[1] Барабанова Д.А. Интернет мошенничество. Способы борьбы // Тенденции развития науки и образования. 2025. № 2. С. 25.

реквизитами тайно, без использования обмана или компьютерного вмешательства, а затем использует их для списания средств, квалификация может осуществляться по ст. 158 УК РФ как кража.

В разъяснениях Пленума ВСРФ № 48 особо оговорены случаи, когда виновный совершает хищение путем использования учетных данных собственника или иного владельца имущества. Независимо от способа получения доступа к таким данным, будь то тайное ознакомление с ними либо получение путем обмана, когда злоумышленник воспользовался телефоном потерпевшего, подключенным к услуге мобильного банка, или авторизовался в системе интернет-платежей под известными ему данными другого лица, подобные действия подлежат квалификации как кража, если только виновный не оказал незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети[1].

Данное разъяснение имеет важнейшее практическое значение, поскольку позволяет квалифицировать значительный массив хищений, совершаемых с использованием методов социальной инженерии, именно как тайное хищение, а не как мошенничество в сфере компьютерной информации. К числу таких ситуаций относятся случаи, когда потерпевший под влиянием обмана сам сообщает злоумышленнику реквизиты своей карты или коды подтверждения из сообщений, после чего преступник использует эти данные для перевода денежных средств.

Так, суд правильно признал мошенничеством с использованием электронных средств платежа (ст. 159.3 УК РФ) действия женщины, которая размещала в интернете объявления о продаже несуществующих вещей. Покупатели переводили ей предоплату через мобильные приложения банков, но товар так и не получали, поскольку продавщица изначально не собиралась

[1] Бутракова Ю.А., Орлова Л.В. Интерне мошенничество. Способы защиты // Проблемы развития современного общества : сборник научных статей. Курск, 2025. С. 211.

его отправлять[1]. В другом случае суд также квалифицировал деяния по ст. 159.3 УК РФ, где мужчина через чужой аккаунт продавал несуществующие сапоги и получил предоплату на карту, оформленную на постороннего человека[2]. В следующем случае мошенник обещал людям выигранные телефоны, но просил оплатить оформление приза через интернет-банк[3]. Во всех ситуациях потерпевшие добровольно переводили деньги со своих счетов, а преступники забирали их и ничего не отдавали взамен.

Важным обстоятельством, подлежащим установлению при юридической квалификации интернет-мошенничества, выступает субъективная сторона преступления, в частности, направленность умысла виновного лица. Поскольку хищение предполагает корыстную цель и стремление обратить чужое имущество в свою пользу или пользу третьих лиц, доказыванию данных обстоятельств должно уделяться пристальное внимание.

В ситуациях с использованием интернет-технологий установление умысла может быть осложнено отсутствием прямых доказательств, однако анализ способа действий преступника, характера используемых им средств, продолжительности и систематичности противоправной деятельности позволяет сделать обоснованный вывод о наличии корыстной мотивации. Необходимо также учитывать, что для квалификации по статьям о мошенничестве не имеет значения, кто именно – сам виновный или иные лица – получил фактическую возможность распоряжаться похищенным имуществом по своему усмотрению.

Таким образом, несмотря на то, что мошенничество в сети Интернет не имеет отдельного законодательного определения, сложившаяся система

---

[1] Дело № 1-140/2022 Вольский районный суд Саратовской области // Государственная автоматизированная система РФ «Правосудие». Интернет-портал [Электронный ресурс] // URL: https://sudrf.ru/ (дата обращения: 20.12.2025).

[2] Дело № 1-254/2022 Железнодорожный районный суд города Красноярска // Государственная автоматизированная система РФ «Правосудие». Интернет-портал [Электронный ресурс] // URL: https://sudrf.ru/ (дата обращения: 20.12.2025).

[3] Дело № 1-87/2022 (1-554/2021) Куйбышевский районный суд г. Омска // Государственная автоматизированная система РФ «Правосудие». Интернет-портал [Электронный ресурс] // URL: https://sudrf.ru/ (дата обращения: 20.12.2025).

уголовно-правовых норм позволяет достаточно полно охватить различные формы противоправных деяний в цифровой среде. Понятие такого мошенничества формируется доктринально и охватывает широкий спектр общественно опасных действий, объединенных использованием информационно-коммуникационных технологий для завладения чужим имуществом. Юридическая квалификация указанных деяний требует глубокого анализа объективной стороны преступления и установления точного способа завладения имуществом, что нашло свое отражение в разъяснениях высшей судебной инстанции и в специальных составах преступлений, предусмотренных уголовным законом.

§ 2. История развития и современное состояние интернет-мошенничества

История противоправных посягательств, совершаемых с использованием глобальной сети, представляет собой процесс стремительной эволюции, неразрывно связанный с развитием самих информационно-телекоммуникационных технологий. Зародившись как единичные случаи манипуляций в только формирующемся цифровом пространстве, интернет-мошенничество трансформировалось в масштабную индустрию, оказывающую существенное влияние на экономическую безопасность государств и благосостояние миллионов людей[1].

Анализ закономерностей становления данного вида преступности позволяет выделить несколько основных этапов, каждый из которых характеризовался уникальными методами, техническими приемами и субъектным составом, что в конечном итоге привело к формированию современной криминальной среды, требующей адекватного и оперативного реагирования со стороны законодателя и правоприменительных органов.

Первоначальный этап развития интернет-мошенничества, охватывающий

[1] Кильметова Р.Р., Савлохов Р.Р. Современные виды мошенничества в сети Интернет и пути их разрешения // Аграрное и земельное право. 2025. № 7. С. 264.

период примерно с начала девяностых годов прошлого века, был неразрывно связан с коммерциализацией сети и появлением электронной торговли. Ранние схемы отличались примитивностью, но высокой эффективностью из-за отсутствия у пользователей и продавцов опыта работы в новой среде. Одной из первых задокументированных тенденций стало использование похищенных данных кредитных карт совместно с именем какой-либо знаменитости, что позволяло обойти несовершенные на тот момент процедуры верификации. По мере развития электронной коммерции злоумышленники совершенствовали технический арсенал, создавая приложения-генераторы номеров кредитных карт, которые позволяли массово тестировать украденные данные в сети. Логическим продолжением стало создание фиктивных торговых площадок, целью которых был не столько сбыт товара, сколько сбор платежной информации доверчивых покупателей перед быстрым исчезновением с рынка.

В этот период мошенничество носило преимущественно кустарный характер, совершалось узким кругом лиц, а правовые системы многих стран, включая Россию, лишь начинали осознавать необходимость регулирования складывающихся общественных отношений в новой виртуальной среде. Первые попытки криминологического осмысления и уголовно-правового реагирования на подобные деяния относятся еще к советскому периоду, однако активное развитие законодательства началось несколько позже[1].

Следующий этап развития, пришедшийся на конец девяностых – начало двухтысячных годов, ознаменовался усложнением технических средств совершения преступлений и смещением фокуса внимания злоумышленников с единичных атак на создание инфраструктуры для систематического извлечения выгоды. Киберпреступность начала приобретать организованный характер, на смену хакерам-одиночкам пришли преступные группы, нацеленные на кражу виртуальных денег и доступ к банковским счетам. Важнейшим изменением стало использование комбинации различных технологий: массовые рассылки

[1] Кулешова Ю.Г. Современные аспекты интернет-мошенничества: способы совершения и методы противодействия // Криминалистика: актуальные вопросы теории и

вредоносных программ, нацеленных на хищение реквизитов доступа, и создание поддельных сайтов, имитирующих ресурсы известных компаний. Появление и распространение спама превратилось из досадной помехи в серьезную угрозу: через нежелательные письма не только рекламировались сомнительные товары, но и распространялись вирусы, а также осуществлялся фишинг – метод обмана пользователей с целью получения конфиденциальной информации.

На рубеже тысячелетий для рассылки спама и проведения атак злоумышленники начали активно использовать зараженные компьютеры рядовых пользователей, объединяя их в так называемые зомби-сети, которые сдавались в аренду другим преступникам, закладывая основы современного теневого рынка киберуслуг. В это время в России происходило активное проникновение интернета в повседневную жизнь, что, при некотором запоздании по сравнению с Западом, создало благодатную почву для активного развития отечественной школы кибермошенничества, отличающейся, по мнению ряда исследователей, высоким техническим уровнем[1].

Третий, современный этап развития интернет-мошенничества, берущий начало примерно с середины десятых годов двадцать первого века и продолжающийся по сей день, характеризуется переходом к использованию методов социальной инженерии в сочетании с технологиями искусственного интеллекта, а также окончательной криминализацией и профессионализацией данной сферы. Основным драйвером изменений стало повсеместное распространение смартфонов, которые превратились в основное устройство для выхода в сеть и совершения финансовых операций. Злоумышленники сместили акцент со взлома технически защищенных систем на манипулирование человеческой психикой, используя методы спешки, запугивания и создания эффекта неожиданности.

практики: сборник научных статей. Ростов-на-Дону, 2025. С. 129.

[1] Минакова Т.А. Интернет-мошенничество: схемы обмана и способы защиты // Современные вызовы экономики, управления и здоровья: Россия с многополярном мире:

Пандемия коронавируса, вынудившая миллионы людей перейти в удаленный режим работы и активнее использовать цифровые сервисы, придала этому процессу дополнительное ускорение. Одновременно произошел качественный скачок в развитии технологий: искусственный интеллект позволил создавать дипфейки – реалистичные подделки голоса и изображения, которые используются для обмана даже хорошо информированных и подготовленных жертв. Мошенничество превратилось в высокодоходный бизнес с четким разделением труда, где существуют разработчики вредоносного программного обеспечения, операторы сетей зараженных устройств, дропперы, обналичивающие похищенные средства, и непосредственно обзвонщики, применяющие методы социальной инженерии.

Современное состояние интернет-мошенничества в Российской Федерации характеризуется не только ростом количественных показателей, но и изменением качественной структуры угроз, что вызывает необходимость адекватного законодательного противодействия. По официальным данным, фиксируется устойчивый рост числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, что требует от государства принятия системных мер. Важнейшим шагом в этом направлении стало формирование комплексной нормативной базы, направленной на защиту граждан и организаций от противоправных посягательств в цифровой среде[1].

Важным событием стало принятие Федерального закона от 01.04.2025 № 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», которым была создана государственная информационная система противодействия

сборник научных статей. Санкт-Петербург, 2025. С. 308.

[1] Орлова Л.В., Козлов А.М. Интернет-мошенничество: вызов цифровой безопасности и пути его преодоления // Тенденции развития науки и образования. 2025.

правонарушениям, совершаемым с использованием информационно-телекоммуникационных технологий. Данная система призвана обеспечить оперативный обмен данными в режиме реального времени между правоохранительными органами, Банком России, кредитными организациями и операторами сотовой связи для быстрого выявления, пресечения и раскрытия киберпреступлений, а также для защиты финансовых средств граждан[1].

Развитие законодательства направлено на совершенствование системы противодействия и введение дополнительных правовых гарантий для граждан, включая расширение объема информации, хранящейся в государственной информационной системе, усиление идентификации абонентского оборудования, а также введение новых правил для банковского сектора, обязывающих кредитные организации проверять добровольность согласия клиента на совершение операций[2].

Таким образом, киберпреступность в России представляет серьезную угрозу, требующую комплексного подхода и скоординированных усилий на всех уровнях общества для ее эффективного пресечения. Дальнейшее развитие системы противодействия будет неразрывно связано с необходимостью повышения цифровой грамотности населения, так как никакие технологические и законодательные меры не будут полностью эффективны без сознательного и осторожного поведения самих пользователей.

§ 3. Виды и классификация способов совершения мошеннических действий в глобальной сети

Проблема систематизации способов совершения мошеннических действий в глобальной сети представляет собой одно из наиболее сложных направлений современной криминалистики и теории уголовного права.

№ 2. С. 142.

[1] Ройхка А.А. Особенности интернет-мошенничества в современную эпоху: криминологический аспект // Закон. Право. Государство. 2024. № 4. С. 240.

[2] Фомина П.С. Особенности интернет-мошенничества в России // Педагогический конференциум: сборник научных трудов и материалов научно-практических

Многообразие приемов, используемых злоумышленниками, их постоянная трансформация вслед за развитием технологий, а также высокая степень латентности таких деяний обусловливают необходимость построения непротиворечивой классификации, позволяющей не только дифференцировать ответственность, но и выстраивать эффективные системы профилактики и противодействия.

В основе любой классификации лежит понимание мошенничества как хищения чужого имущества или приобретения права на него путем обмана или злоупотребления доверием, что закреплено в ст. 159 УК РФ. Однако применительно к цифровой среде данное определение наполняется специфическим содержанием, поскольку способы обмана реализуются с использованием информационно-телекоммуникационных технологий, а взаимодействие между преступником и жертвой опосредовано электронными устройствами и сетями[1].

Одним из наиболее устоявшихся подходов к классификации интернет-мошенничества выступает разделение по способу взаимодействия с жертвой. Традиционно выделяют мошенничества, совершаемые путем направления электронных сообщений, посредством телефонных звонков, через создание поддельных интернет-ресурсов, а также с использованием вредоносного программного обеспечения. Каждая из указанных групп обладает собственной криминалистической характеристикой и требует особых методов расследования.

Телефонное мошенничество, несмотря на кажущуюся архаичность, продолжает занимать лидирующие позиции по объему причиняемого ущерба: по оценкам экспертов, ежегодный объем таких преступлений в России исчисляется десятками и сотнями миллиардов рублей, причем подавляющее большинство финансовых преступлений совершается с применением методов

конференций. 2024. № 2. С. 214.

[1] Чуб И.С. Мошенничество в сети Интернет: способы совершения и виктимологическая профилактика // Вестник Краснодарского университета МВД России.

социальной инженерии. Злоумышленники используют несколько рабочих номеров, оформленных на подставных лиц, сим-карты уничтожаются после получения денег, а похищенные средства многократно переводятся между различными счетами, что создает высокую степень латентности данных деяний и затрудняет их раскрытие.

Значительное место в системе классификации занимают мошенничества, связанные с использованием банковских карт и электронных средств платежа. С криминалистической точки зрения указанный способ отличается особой технической оснащенностью, поскольку предполагает применение специальных устройств для незаконного получения информации с карт либо непосредственного доступа к денежным средствам. Речь идет о скимминге, то есть установке на банкоматы накладок и видеокамер для считывания данных магнитной полосы и подсмотра пин-кода, о траппинге, когда устройство зажимает карту внутри банкомата, а мошенник извлекает ее после ухода растерянного владельца, а также о более сложных атаках, связанных с подключением к банкомату компьютера и использованием вредоносных программ для принудительной выдачи наличных. Все перечисленные действия квалифицируются по статье 159.3 УК РФ как мошенничество с использованием электронных средств платежа[1].

Дистанционное хищение средств с карты, напротив, может быть совершено любым способом, позволяющим получить реквизиты: номер карты, срок действия и код проверки подлинности. После получения указанных данных злоумышленники осуществляют переводы через интернет-банкинг или системы быстрых платежей, причем нередко такие операции маскируются под легитимные действия самого владельца счета.

Самостоятельную группу образуют мошенничества в сфере компьютерной информации, ответственность за которые предусмотрена

2024. № 1. С. 39.

[1] Авдошкин А.А. О проблемах мошенничества в сети Интернет // Теория и практика кооперации в современном обществе: сборник научных статей. Саранск, 2025.

статьей 159.6 УК РФ. Отличительной чертой данных деяний выступает то, что хищение совершается путем вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей. Спектр таких вмешательств чрезвычайно широк: от несанкционированного доступа к учетным записям в социальных сетях и электронной почте до взлома банковских серверов и использования уязвимостей программного обеспечения.

В юридической литературе неоднократно отмечалась сложность разграничения данного состава со смежными, в частности с кражей с банковского счета и мошенничеством с использованием электронных средств платежа. В соответствии с позицией Пленума ВС РФ № 48, если виновный использует учетные данные собственника, полученные из других источников, и при этом отсутствует незаконное воздействие на информационно-коммуникационные сети, содеянное надлежит квалифицировать как кражу. В случаях же, когда преступник получает доступ к информации непосредственно в момент совершения деяния, но без контакта с потерпевшим, речь идет о мошенничестве в сфере компьютерной информации[1].

Значительную долю в структуре интернет-мошенничества занимают преступления, совершаемые при осуществлении электронной торговли. Создание фиктивных интернет-магазинов и страниц в социальных сетях, предлагающих товары по ценам существенно ниже рыночных, стало массовым явлением. Привлекательные ценовые предложения, качественные изображения товаров и убедительные описания формируют у потенциальных покупателей ложное представление о добросовестности продавца. После получения предоплаты страница удаляется либо доступ покупателя блокируется, а товар, разумеется, не отправляется.

С. 31.

[1] Безбородова Л.С., Девятых А.В. Мошенничество в интернет-пространстве: виды и способы наживы // Юриспруденция: актуальные вопросы теории и практики: сборник научных статей. Пенза, 2024. С. 74.

Статистика свидетельствует, что количество подобных преступлений не снижается, несмотря на активную профилактическую работу правоохранительных органов и регулярные предупреждения в средствах массовой информации. К этой же категории можно отнести мошенничества с билетами на мероприятия, подарочными картами, а также продажу поддельных или некачественных товаров под видом оригинальной продукции.

Особого внимания заслуживает классификация, предложенная исследователями, изучающими организованные формы онлайн-мошенничества. В работе А.А. Давыдова обосновывается положение о том, что современное интернет-мошенничество приобрело признаки высокоорганизованной преступной деятельности с четким разделением функций между участниками. Выделяются разработчики вредоносного программного обеспечения и фишинговых сайтов, операторы, осуществляющие массовые рассылки и телефонные обзвоны, дропперы, на счета которых выводятся похищенные средства, и обнальщики, занимающиеся легализацией денег. Такая структура позволяет преступным группам действовать трансгранично, использовать юрисдикции с несовершенным законодательством и быстро восстанавливаться после ликвидации отдельных звеньев. В рамках организованных форм мошенничества применяются наиболее сложные и технологичные схемы, включая использование нейросетей и технологий дипфейк для имитации голоса и изображения реальных людей[1].

К числу наиболее распространенных и одновременно опасных видов интернет-мошенничества относится фишинг. Сущность данного способа заключается в создании поддельных веб-страниц, имитирующих официальные сайты банков, платежных систем, государственных учреждений или популярных интернет-сервисов. Жертва получает электронное письмо, сообщение в мессенджере или уведомление в социальной сети с предложением перейти по ссылке для подтверждения учетной записи, получения выигрыша,

[1] Давыдов А.А. Интернет-мошенничество как актуальная проблема нового времени // Наука XXI века: актуальные направления развития. 2024. № 1. С. 513-516.

разблокировки карты или иных действий, требующих ввода персональных данных. Переход по ссылке ведет на сайт-двойник, где пользователь вводит логин, пароль, данные карты, после чего информация становится доступной злоумышленникам. В научной литературе фишинг характеризуется как метод кражи идентификационных данных, основанный на создании убедительной имитации легитимных ресурсов. Разновидностью фишинга выступает вишинг, то есть мошенничество с использованием телефонных звонков, и смишинг, осуществляемый посредством смс-сообщений.

Активное развитие получили мошенничества, связанные с использованием социальных сетей и сайтов знакомств. Так называемые брачные мошенничества предполагают длительное общение с жертвой, формирование доверительных отношений, после чего под различными предлогами выманиваются денежные средства. Легенды могут быть самыми разнообразными: необходимость приобретения билетов для встречи, срочное лечение родственника, проблемы с бизнесом, требующие временного займа[1].

Нередко общение заканчивается шантажом, когда полученные в ходе переписки личные фотографии или видео используются для вымогательства. В подобных случаях деяние квалифицируется уже не как мошенничество, а как вымогательство, что предусмотрено статьей 163 УК РФ. Профилактика указанных преступлений заключается прежде всего в повышении цифровой грамотности и осмотрительности граждан при общении с незнакомцами в сети.

Отдельную нишу занимают мошенничества, эксплуатирующие чувство сострадания и желание помочь. Схема, условно обозначаемая правоохранительными органами как крик о помощи, предполагает распространение в социальных сетях историй о тяжелобольных детях, нуждающихся в дорогостоящем лечении, пострадавших от стихийных бедствий семьях, бездомных животных. К публикациям прикрепляются реквизиты для сбора средств, которые на самом деле принадлежат мошенникам.

[1] Кузовлева Н.Ф,, Хусаинов М.К. К вопросу об интерне-мошенничестве в условиях интенсивной цифровизации общества // Светоч науки. 2025. № 2. С. 193.

Убедительность таким историям придают фотографии, часто заимствованные из реальных акций помощи или просто из открытых источников, и эмоциональные тексты. Схожий механизм используется при создании фальшивых благотворительных фондов, собирающих пожертвования на несуществующие цели.

Типологический подход к классификации интернет-мошенничества, предложенный И.А. Лобаченко, основывается на анализе используемых цифровых технологий как инструментов совершения преступлений. В рамках данного подхода выделяются практики, связанные с применением фишинговых сайтов, скам-страниц, файлообменников, дубликатов сим-карт, блютуз-устройств, чат-ботов, QR-кодов и впн-сервисов. Каждый из перечисленных инструментов открывает специфические возможности для обмана: через QR-коды, например, жертва может быть перенаправлена на вредоносный сайт при сканировании обычной на вид метки, размещенной в общественном месте; чат-боты в мессенджерах используются для автоматизированного сбора персональных данных под видом предоставления услуг; дубликаты сим-карт позволяют перехватывать коды подтверждения из смс-сообщений и получать доступ к банковским счетам и аккаунтам. Указанная типология наглядно демонстрирует, насколько тесно современное мошенничество интегрировано с повседневными цифровыми практиками населения[1].

Значительные изменения в классификацию способов совершения мошеннических действий вносит использование технологий искусственного интеллекта. В научных публикациях последних лет все чаще упоминаются дипфейки – синтезированные изображения, видео и аудиозаписи, с высокой степенью достоверности имитирующие реальных людей. С помощью нейросетей злоумышленники создают поддельные видеосообщения от руководителей компаний с распоряжениями о срочных переводах крупных сумм, генерируют голоса родственников, якобы попавших в беду,

[1] Лобаченко И.А. Киберпреступность: анализ и классификация интернет-мошенничества // Актуальные и перспективные научные исследования: сборник научных

изготавливают поддельные документы и удостоверения.

Технологии искусственного интеллекта позволяют автоматизировать создание фишинговых писем, делая их более персонализированными и убедительными, а также анализировать поведение потенциальных жертв для выбора оптимальной стратегии обмана. В юридической литературе ставится вопрос о необходимости выделения мошенничеств с использованием нейросетей в отдельную категорию, поскольку традиционные методы противодействия здесь зачастую оказываются неэффективными[1].

Классификация интернет-мошенничества может быть построена и по предмету посягательства. Наиболее распространенным предметом выступают денежные средства, однако в последнее время участились случаи хищения криптовалюты и иных цифровых активов. Рост популярности криптовалют сопровождается появлением специфических мошеннических схем: создание фальшивых криптобирж, инвестиционных проектов с обещанием сверхдоходности, фишинговых сайтов для кражи ключей от криптокошельков. Мошенничество в сфере криптовалют осложняется анонимностью транзакций и отсутствием единого регулирующего органа, что делает возврат похищенного практически невозможным. Предметом посягательства могут выступать также персональные данные, учетные записи в социальных сетях и игровых сервисах, доступ к платному контенту. Хищение указанных объектов не всегда преследует непосредственную финансовую выгоду, но в дальнейшем используется для шантажа, вымогательства или совершения иных преступлений[2].

Современное российское законодательство учитывает многообразие способов совершения мошеннических действий в глобальной сети и

статей. Пенза, 2025. С. 153.

[1] Михайлов К.В. Развитие интернет-мошенничества в России: анализ основных типов мошенничества // Уголовно-правовые, уголовно-исполнительные и криминологические проблемы обеспечения безопасности человека, общества и государства: сборник научных статей. Санкт-Петербург, 2025. С. 107.

[2] Новрузов И.Н., Новрузов Д.Н. Способы защиты от интернет-мошенничества // Тенденции развития науки и образования. 2025. № 2. С. 134.

предусматривает дифференцированную ответственность в зависимости от способа, размера ущерба, организованной группы и иных обстоятельств. Внесенные в последние годы поправки направлены на усиление защиты граждан и создание механизмов оперативного реагирования на новые угрозы. Федеральным законом № 41-ФЗ от 1 апреля 2025 года создана государственная информационная система противодействия правонарушениям, совершаемым с использованием информационно-телекоммуникационных технологий, которая обеспечивает обмен данными между правоохранительными органами, банками и операторами связи.

Разрабатываемый Министерством цифрового развития пакет законодательных мер, запланированный к вступлению в силу в 2026-2027 годах, предполагает расширение состава информации в государственной системе, усиление идентификации абонентского оборудования, введение самозапретов на выдачу кредитов и получение сим-карт удаленно, а также обязанность операторов связи маркировать вызовы от юридических лиц.

Таким образом, многообразие способов совершения мошеннических действий в глобальной сети обусловливает необходимость построения многомерных классификаций, учитывающих способ взаимодействия с жертвой, используемые технические средства, предмет посягательства, степень организованности преступной группы и иные значимые признаки. Такие классификации имеют не только теоретическое, но и прикладное значение, поскольку позволяют разрабатывать дифференцированные меры профилактики, совершенствовать методики расследования и адаптировать законодательство к быстро меняющимся условиям цифровой среды.

ГЛАВА 2. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ-МОШЕННИЧЕСТВА

§ 1. Состояние интернет-мошенничества в России и факторы, способствующие его совершения

Современное состояние интернет-мошенничества в России представляет собой сложный и динамично развивающийся феномен, требующий постоянного мониторинга и анализа со стороны научного сообщества и правоприменительных органов. Статистические данные последних лет демонстрируют неоднозначную картину: с одной стороны, наблюдается тенденция к сокращению общего количества регистрируемых преступлений в сфере информационно-телекоммуникационных технологий, с другой стороны, сумма причиняемого гражданам ущерба продолжает расти, что свидетельствует о качественной трансформации самих способов совершения противоправных деяний и повышении их общественной опасности.

По итогам 2025 года преступлений, совершенных с использованием информационно-телекоммуникационных технологий, зарегистрировано на 11,8 процента меньше, чем в 2024 году, при этом количество дистанционных мошенничеств снизилось на 9 процентов, дистанционных краж на 23,6 процента, а преступлений в сфере компьютерной информации на 42,2 процента. Аналогичные данные приводят и в Генеральной прокуратуре, отмечая, что по итогам одиннадцати месяцев 2025 года массив IT-преступлений уменьшился на 10,8 процента по сравнению с аналогичным периодом предшествующего года[1].

Однако за внешне благополучной статистикой сокращения числа регистрируемых преступлений скрывается тревожная тенденция роста сумм причиняемого ущерба. По информации заместителя начальника следственного департамента МВД России, за восемь месяцев 2025 года ущерб граждан от

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2025 года [Электронный ресурс]. Режим доступа: https://xn--b1aew.xn--

киберпреступлений составил 134 миллиарда рублей, тогда как в 2024 году аналогичный показатель равнялся 116 миллиардам рублей. Темпы прироста ущерба, хотя и замедлились с 65 процентов в начале года до 26 процентов по итогам восьми месяцев, остаются значительными и вызывают обоснованную тревогу[1]. Еще более показательные данные обнародовал Центральный банк Российской Федерации: в 2025 году мошенникам удалось похитить со счетов клиентов кредитных организаций 29,3 миллиарда рублей, что на 6,4 процента превышает показатель предыдущего года[2].

Парадоксальным образом количество операций без согласия клиента увеличилось на 31,2 процента, что эксперты связывают не столько с возросшей активностью злоумышленников, сколько с расширением инструментов для обращений граждан, включая внедрение с октября 2025 года для системно значимых банков специальной кнопки в мобильных приложениях, позволяющей оперативно сигнализировать о мошеннических действиях. По итогам 2025 года кибермошенники похитили у россиян от 275 до 295 миллиардов рублей.

Столь существенное расхождение с данными Центрального банка объясняется методологией подсчета: регулятор учитывает только переводы из банковских приложений, тогда как оценка Сбербанка включает инциденты, когда клиент снимал деньги со счета и наличными передавал мошенникам, передачу кредитных средств, средств от продажи высоколиквидного имущества, а также сбережений, не хранившихся в финансовых организациях. Более того, по оценкам банка, от 30 до 40 процентов потерь вообще не попадают в какую-либо официальную статистику, поскольку граждане не обращаются ни в правоохранительные органы, ни в Центральный банк.

---

p1ai/reports/item/77848182/ (дата обращения: 30.01.2026).

[1] Ущерб граждан от киберпреступлений за 8 месяцев вырос до 134 млрд рублей [Электронный ресурс]. Режим доступа: nterfax-russia.ru (Дата обрадения: 30.01.2026).

[2] В «Сбере» оценили объем похищенных мошенниками средств в 295 млрд рублей [Электронный ресурс]. Режим доступа: https://expert.ru/news (дата обращения: 30.01.2026).

Средняя сумма ущерба на одного пострадавшего увеличилась на 5 процентов, достигнув 373 тысяч рублей, при этом общее количество пострадавших сократилось до 496,8 тысячи человек, что подтверждает тезис о переходе мошенников к более точечным и дорогостоящим схемам.

Анализ многолетней динамики развития киберпреступности показывает, что за предшествующие двенадцать лет общее число IT-преступлений в России выросло почти в семьдесят раз: с 11 тысяч в 2013 году до 765 тысяч в 2024 году, причем в 2024 году рост составил 13 процентов, а доля IT-преступлений среди всех видов противоправных деяний достигла 40 процентов. В первом полугодии 2025 года удалось впервые за несколько лет замедлить рост числа киберпреступлений: преступления в сфере информационных технологий и телекоммуникаций занимали почти 40 процентов всех зарегистрированных правонарушений, но их количество увеличилось лишь на 0,7 процента, тогда как в первом полугодии 2024 года рост составлял 15,8 процента. Количество мошенничеств в первом полугодии 2025 года снизилось до 221,6 тысячи, причем подавляющее большинство из них – кибермошенничества (185,4 тысячи случаев)[1].

Отечественные исследователи единодушны во мнении, что наиболее распространенными видами киберпреступлений в российском обществе выступают различные формы мошенничества и кражи, совершаемые с использованием информационно-коммуникационных технологий. При этом особую озабоченность научного сообщества вызывает высокая степень общественной опасности указанных деяний и значительные показатели причиняемого ими ущерба, а также существенная латентность, обусловленная как объективными сложностями выявления цифровых следов, так и нежеланием потерпевших обращаться в правоохранительные органы.

Современная криминологическая наука подчеркивает двойственную природу киберпреступности, проявляющуюся в одновременной

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2025 года [Электронный ресурс]. Режим доступа: https://xn--b1aew.xn--

организационной сложности и структурированности преступных сообществ, с одной стороны, и их гибкости и адаптивности к изменяющимся условиям – с другой.

Эмпирические исследования отношения различных групп населения к цифровой преступности, проведенные Ю.Л. Поповым и Д.Р. Шестаковым, позволяют составить достаточно полную картину виктимизации российских граждан. Социологический опрос, проведенный сектором социологии девиантного поведения Института социологии ФНИСЦ РАН среди городского трудоспособного населения в возрасте от восемнадцати до шестидесяти лет, выявил, что многие респонденты оценивают вероятность стать жертвой кибермошенничества как достаточно высокую. Наибольшие опасения у граждан вызывают незаконное использование и хищение персональных данных, а также взлом электронной почты. Установлена отчетливая возрастная дифференциация страхов перед киберугрозами: количество респондентов, опасающихся стать жертвой киберпреступления, увеличивается с возрастом, однако в самых старших возрастных группах данные опасения неожиданно снижаются. Указанный феномен требует дополнительного изучения, поскольку может свидетельствовать либо о недостаточной осведомленности пожилых людей о реальных рисках, либо о своеобразном психологическом механизме защиты, снижающем тревожность перед малопонятными угрозами[1].

Другим важным дифференцирующим фактором в отношении столкновения с киберугрозами выступает уровень образования граждан. Исследование показало, что чем выше образовательный уровень респондентов, тем чаще они имеют опыт столкновения с киберпреступлениями. Данная закономерность объясняется, вероятно, более интенсивным использованием цифровых технологий и финансовых сервисов лицами с высоким образовательным статусом, что объективно повышает вероятность попадания в

---

p1ai/reports/item/77848182/ (дата обращения: 30.01.2026).

[1] Попов Ю.Л., Шестаков Д.Р. Мошенничества в Интернет // Актуальные исследования. 2025. № 1. С. 45.

зону риска. Парадоксальным образом наиболее образованные и социально активные граждане оказываются одновременно и наиболее защищенными в силу лучшего понимания принципов работы цифровых систем, и наиболее уязвимыми в силу большей вовлеченности в онлайн-взаимодействия.

Значительный научный интерес представляют результаты экспертного опроса, проведенного А.А. Сазановой для выявления основных особенностей и тенденций развития киберпреступности в России. К экспертизе были привлечены специалисты различных направлений – от исследователей-девиантологов до практических работников, занимающихся вопросами информационной безопасности и имеющих непосредственный опыт противодействия киберпреступности[1]. Полученные оценки свидетельствуют о неутешительном прогнозе на ближайшие годы: ожидается дальнейший рост киберпреступности, усложнение применяемых преступниками техник, включая активное использование технологий искусственного интеллекта, что обусловливает настоятельную необходимость разработки специализированных защитных решений и совершенствования методов противодействия.

В качестве основных факторов роста киберпреступности в России эксперты выделяют прежде всего ее двойственную природу, сочетающую организационную сложность и структурированность преступных сообществ с их высокой гибкостью и адаптивностью к меняющимся условиям. Современные организованные группы, специализирующиеся на интернет-мошенничестве, представляют собой сложные иерархические структуры с четким разделением функций между участниками.

Существенным фактором, способствующим процветанию интернет-мошенничества, выступает недостаточный уровень цифровой грамотности и технологической осведомленности населения, парадоксальным образом сочетающийся с высоким уровнем доступности интернета в России. Граждане активно пользуются цифровыми сервисами, осуществляют банковские

[1] Сазанова А.А. Современные способы мошенничества в сети Интернет // Актуальные проблемы инновационных систем информатизации и безопасности: сборник

операции онлайн, совершают покупки в интернет-магазинах, но при этом зачастую не обладают необходимыми знаниями о правилах безопасного поведения в сети, не распознают признаки мошеннических схем и становятся легкой добычей злоумышленников, использующих методы социальной инженерии. Указанная проблема усугубляется цифровым неравенством, когда различные социальные группы оказываются в неравном положении с точки зрения доступа к знаниям и навыкам безопасного использования цифровых технологий.

Важным фактором, способствующим росту киберпреступности, является активное использование злоумышленниками достижений научно-технического прогресса, в особенности технологий искусственного интеллекта. В современных исследованиях подчеркивается, что доступность и стремительное развитие технологий глубокого обучения существенно усиливают возможности мошенников по созданию персонализированных атак и автоматизированных схем социальной инженерии. Особую тревогу вызывает использование дипфейков – синтезированных с помощью нейросетей изображений, видео и аудиозаписей, с высокой степенью достоверности имитирующих реальных людей. Преступники создают поддельные видеосообщения от руководителей компаний с распоряжениями о срочных переводах крупных сумм, генерируют голоса родственников, якобы попавших в беду, изготавливают поддельные документы и удостоверения. Технологии искусственного интеллекта позволяют автоматизировать создание фишинговых писем, делая их более персонализированными и убедительными, а также анализировать поведение потенциальных жертв для выбора оптимальной стратегии обмана[1].

Криминологические исследования последних лет обращают особое внимание на проблему вовлечения несовершеннолетних в совершение мошеннических действий с использованием информационно-

---

научных статей. Воронеж, 2025. С. 492.

[1] Черныш М.А., Кумарин А.А. Интернет-мошенничество в современной России // Актуальные проблемы теории и практики уголовного права и процесса: сборник научных

телекоммуникационных технологий. Ученые выделяют специфические криминологические риск-маркеры онлайн-пространства, сигнализирующие о возможном вовлечении подростка в противоправную деятельность. К числу таких маркеров относятся специфичное онлайн-поведение, наличие в речи стилистически маркированных жаргонных слов, имеющих отношение к сфере информационно-телекоммуникационных технологий, подозрительные транзакции, склонность к интеграции в онлайн-сообщества, транслирующие информацию о возможностях неправомерного доступа к компьютерной информации, ее блокировки и модификации, общение с чат-коммуникантами, популяризирующими деструктивную идеологию, обещающую легкий заработок и нивелирующую традиционные духовно-нравственные ценности[1].

Исследователи предлагают комплекс превентивных мер, направленных на обеспечение криминологической безопасности несовершеннолетних, включая реализацию специализированных национальных проектов, ориентированных на привитие навыков безопасного поведения и обеспечения личностной безопасности в сети Интернет, разработку и совершенствование прикладного программного инструментария, позволяющего осуществлять родительский контроль, мониторинг, выявление и блокировку противоправного контента с использованием технологий искусственного интеллекта, а также проведение профилактической разъяснительной работы на уровне семьи и школы по информированию о правилах обеспечения личной безопасности в онлайн-пространстве, возможных мошеннических схемах и неизбежности привлечения к уголовной ответственности за участие в мошенничестве.

Значительное место в научном дискурсе занимают проблемы уголовно-правовой квалификации мошенничества в сфере компьютерной информации, предусмотренного ст. 159.6 УК РФ. Исследователи обращают внимание на противоречивость законодательной конструкции данного состава

статей. Ростов-на-Дону, 2025. С. 234.

[1] Юдина И.А., Орлова Л.В. Интернет мошенничество. Способы защиты // Тенденции развития науки и образования. 2025. № 2. С. 212.

преступления, поскольку в соответствии с частью первой статьи 159 УК РФ способом совершения мошенничества являются обман и злоупотребление доверием, однако применительно к мошенничеству в сфере компьютерной информации потерпевший узнает о совершенном в отношении него общественно опасном деянии лишь с наступлением общественно опасных последствий, то есть никакого воздействия в момент совершения преступления преступник на его сознание не оказывает. Таким образом, в указанной ситуации отсутствует основной признак мошенничества – специфический способ совершения, что создает серьезные проблемы при применении данной нормы на практике.

В рамках совершенствования уголовно-правового регулирования в сфере информационных технологий законодатель дополнил диспозицию статьи специальным способом совершения данного вида мошенничества, а именно: ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[1]. Однако подобное законодательное решение породило проблему дифференциации мошенничества в сфере компьютерной информации и других форм хищений, таких как кража с банковского счета или в отношении электронных денежных средств, предусмотренная пунктом «г» части третьей статьи 158 УК РФ, а также мошенничества с использованием электронных средств платежа, установленного статьей 159.3 УК РФ.

В соответствии с позицией Пленума ВС РФ № 48, хищение, совершенное с использованием учетных данных собственника, независимо от метода их получения, при условии отсутствия незаконного воздействия на информационно-коммуникационные сети, надлежит квалифицировать как кражу. При этом модификация информации о состоянии банковского счета или о движении денежных средств, произошедшая вследствие использования

[1] Ройхка А.А. Особенности интернет-мошенничества в современную эпоху: криминологический аспект // Закон. Право. Государство. 2024. № 4. С. 241.

виновным учетных данных потерпевшего, не должна рассматриваться как незаконное воздействие на информационно-коммуникационные системы . Разграничение составов преступлений основывается на наличии или отсутствии контакта с потерпевшим: при квалификации деяния по статье 159.6 УК РФ виновный получает сведения непосредственно в момент совершения преступления, но без воздействия на сознание потерпевшего.

Одной из характерных особенностей кибермошенничества является необходимость дополнительной квалификации по статьям 272, 273 или 274.1 УК РФ в тех случаях, когда деяние осуществляется посредством несанкционированного доступа к компьютерной информации, а также посредством разработки, использования и распространения вредоносных программ. Указанное обстоятельство существенно усложняет процесс расследования и требует от правоприменителей глубоких знаний не только в области уголовного права, но и в сфере информационных технологий.

В результате проведенного анализа исследователи приходят к выводу о том, что действующая редакция статьи 159.6 УК РФ, определяющая состав преступления, сформулирована недостаточно удачно и в определенной степени противоречит базовому определению мошенничества, что создает серьезные проблемы при применении данной нормы на практике и обусловливает необходимость дальнейшего совершенствования уголовного законодательства в части противодействия киберпреступности[1].

Теоретическое осмысление феномена мошенничества в цифровой среде приводит исследователей к анализу доверия как фундаментального экономического института, обладающего двойственной природой – ресурса развития и источника уязвимости экономической безопасности. В работах, посвященных данной проблематике, раскрывается понятие инфраструктуры доверия как совокупности каналов, норм и технологий, обеспечивающих признание информации и легитимность экономических взаимодействий.

[1] Новрузов И.Н., Новрузов Д.Н. Способы защиты от интернет-мошенничества // Тенденции развития науки и образования. 2025. № 2. С. 135.

Показано, что усложнение указанной инфраструктуры сопровождается ростом системного риска вследствие технологической связанности и возможности эксплуатации каналов верификации злоумышленниками. Предложена концептуальная модель, описывающая трансформацию доверия из ресурса в уязвимость и далее – в источник системных рисков для экономической безопасности государства и общества[1].

Таким образом, современное состояние интернет-мошенничества в России характеризуется сложным комплексом взаимосвязанных факторов, способствующих его распространению и обусловливающих необходимость поиска эффективных мер противодействия. Научное сообщество единодушно во мнении, что только комплексный подход, сочетающий совершенствование законодательной базы, развитие технических средств защиты, повышение цифровой грамотности населения и скоординированные усилия всех заинтересованных субъектов, способен обеспечить долгосрочное и устойчивое снижение уровня киберпреступности и минимизацию ущерба от нее. Дальнейшие научные исследования в данной области должны быть направлены на углубленное изучение региональных особенностей распространения интернет-мошенничества, анализ эффективности применяемых мер противодействия и разработку инновационных методик профилактики, учитывающих стремительное развитие технологий и постоянную трансформацию способов совершения данных преступлений.

§ 2. Криминологическая характеристика личности мошенника в сети Интернет

Личность мошенника, действующего в глобальной сети, представляет собой сложный криминологический феномен, изучение которого имеет первостепенное значение для понимания природы данного вида преступности и

[1] Авдеенко В.О. Мошенничество в Интернет // Наука. Промышленность. Оборона: сборник научных статей. Новосибирск, 2025. С. 113.

разработки эффективных мер противодействия. В современных научных исследованиях подчеркивается, что киберпреступность в целом и интернет-мошенничество в частности обладают двойственной природой, проявляющейся в одновременной организационной сложности и структурированности преступных сообществ, с одной стороны, и их гибкости и адаптивности к изменяющимся условиям – с другой. Указанная особенность находит непосредственное отражение в криминологических характеристиках лиц, совершающих данные деяния, которые существенно дифференцируются в зависимости от роли конкретного субъекта в преступной иерархии, его технической оснащенности, мотивации и психологических особенностей[1].

Традиционный подход к криминологической характеристике личности преступника предполагает анализ социально-демографических, уголовно-правовых и нравственно-психологических признаков, позволяющих составить целостное представление о типичном субъекте противоправного деяния. Применительно к интернет-мошенничеству указанный подход приобретает определенную специфику, обусловленную как технологическим контекстом совершения преступлений, так и высокой степенью организованности данной формы криминальной активности. Исследователи отмечают существенную неоднородность контингента лиц, занимающихся интернет-мошенничеством, что требует типологизации, основанной на различных критериях, включая уровень технической компетентности, характер участия в преступной деятельности, мотивацию и другие значимые признаки[2].

Одной из наиболее распространенных классификаций выступает разделение интернет-мошенников по признаку наличия и глубины специальных технических знаний.

---

[1] Михайлов К.В. Развитие интернет-мошенничества в России: анализ основных типов мошенничества // Уголовно-правовые, уголовно-исполнительные и криминологические проблемы обеспечения безопасности человека, общества и государства: сборник научных статей. Санкт-Петербург, 2025. С. 108.

[2] Черныш М.А., Кумарин А.А. Интернет-мошенничество в современной России // Актуальные проблемы теории и практики уголовного права и процесса: сборник научных статей. Ростов-на-Дону, 2025. С. 235.

Выделяются так называемые хакеры, обладающие высокой квалификацией в сфере информационных технологий, способные самостоятельно разрабатывать вредоносное программное обеспечение, выявлять уязвимости в системах защиты, осуществлять сложные атаки на информационную инфраструктуру.

На противоположном полюсе располагаются лица, не обладающие специальными техническими познаниями, но использующие готовые инструменты и методики, доступные в теневом сегменте сети, либо применяющие методы социальной инженерии, основанные на манипулировании человеческой психикой, а не на взломе технических систем защиты.

Промежуточное положение занимают пользователи, обладающие базовыми навыками работы с компьютерной техникой и сетями, достаточными для реализации несложных мошеннических схем, таких как создание фиктивных страниц в социальных сетях или размещение объявлений о продаже несуществующих товаров[1].

Возрастные характеристики лиц, совершающих интернет-мошенничества, отличаются определенной спецификой по сравнению с общеуголовной преступностью. Исследования свидетельствуют о значительном омоложении данного контингента: значительную долю составляют лица в возрасте от восемнадцати до тридцати лет, что объясняется их высокой вовлеченностью в цифровую среду, свободным владением современными технологиями, а также определенными социально-психологическими особенностями, включая склонность к риску, недостаточно развитое правосознание и ориентацию на быстрое обогащение. Одновременно наблюдается присутствие в преступной деятельности и лиц среднего и старшего возраста, занимающих, как правило, руководящие позиции в организованных группах и выполняющих функции организаторов, координаторов и идеологов преступного бизнеса. Указанная

[1] Юдина И.А., Орлова Л.В. Интернет мошенничество. Способы защиты // Тенденции развития науки и образования. 2025. № 2. С. 213.

возрастная стратификация отражает разделение труда в современной киберпреступности, где молодые исполнители обеспечивают техническую сторону деятельности, а опытные организаторы выстраивают бизнес-процессы и обеспечивают безопасность.

Образовательный уровень интернет-мошенников характеризуется существенной вариативностью. Среди них встречаются лица как с высшим, нередко профильным техническим образованием, так и не имеющие даже среднего специального образования. Высококвалифицированные специалисты в области информационных технологий, занимающиеся разработкой сложного вредоносного программного обеспечения и осуществлением целевых атак на финансовые учреждения, как правило, обладают глубокими познаниями в программировании, сетевых технологиях, криптографии и смежных областях. Напротив, исполнители низового звена, осуществляющие массовые обзвоны потенциальных жертв или выполняющие функции курьеров, забирающих наличные денежные средства, нередко характеризуются невысоким образовательным уровнем и отсутствием специальной подготовки. Промежуточное положение занимают лица, использующие готовые фишинговые комплекты и методики социальной инженерии, для применения которых достаточно базовых пользовательских навыков и определенных психологических способностей[1].

Гендерный состав лиц, совершающих интернет-мошенничества, традиционно характеризуется преобладанием мужчин, однако в последние годы наблюдается тенденция к увеличению доли женщин, особенно в тех сегментах преступной деятельности, которые требуют навыков коммуникации и психологического воздействия. Женщины активно привлекаются к работе в мошеннических кол-центрах в качестве операторов, осуществляющих обзвон потенциальных жертв по легендам, требующим проявления эмпатии и доверия. Кроме того, женщины нередко выступают в роли так называемых дропперов,

[1] Кузовлева Н.Ф,, Хусаинов М.К. К вопросу об интерне-мошенничестве в условиях интенсивной цифровизации общества // Светоч науки. 2025. № 2. С. 196.

предоставляя свои банковские карты и счета для вывода и обналичивания похищенных средств, либо выполняют функции курьеров, получающих наличные деньги от потерпевших. Указанная тенденция отражает общую феминизацию определенных сегментов киберпреступности и требует учета при разработке профилактических мер.

Социальный статус и род занятий интернет-мошенников также отличаются значительным разнообразием. Среди них встречаются как лица, не имеющие постоянного источника дохода и рассматривающие преступную деятельность как основной способ заработка, так и вполне благополучные граждане, имеющие постоянную работу и вовлекающиеся в мошеннические схемы ради дополнительного дохода либо под влиянием иных мотивов. Особую тревогу вызывает вовлечение в данную деятельность несовершеннолетних и студентов, которые зачастую не осознают в полной мере общественной опасности и юридических последствий своих действий и воспринимают участие в мошеннических схемах как своего рода игру или способ легкого заработка, не требующий значительных усилий. Криминологи обращают внимание на наличие специфических риск-маркеров онлайн-поведения несовершеннолетних, сигнализирующих о возможном вовлечении в противоправную деятельность, включая использование специфического жаргона, общение в деструктивных онлайн-сообществах, транслирующих идеологию легкого обогащения и нивелирующих традиционные ценности[1].

Нравственно-психологическая характеристика личности интернет-мошенника представляет собой сложный комплекс качеств, определяющих его поведение и отношение к совершаемым деяниям. Исследователи отмечают, что для значительной части таких лиц характерна деформация ценностно-нормативной сферы, проявляющаяся в ориентации на материальное благополучие любой ценой, пренебрежении интересами других людей, отсутствии эмпатии к жертвам. Специфика интернет-мошенничества,

[1] Барабанова Д.А. Интернет мошенничество. Способы борьбы // Тенденции развития науки и образования. 2025. № 2. С. 26.

предполагающая отсутствие непосредственного контакта с потерпевшим, способствует формированию психологической дистанции, облегчающей совершение преступлений и снижающей чувство вины. Преступник зачастую воспринимает жертву не как живого человека со своими проблемами и переживаниями, а как абстрактный источник дохода, что существенно облегчает процесс дегуманизации и рационализации противоправного поведения.

Важной психологической характеристикой многих интернет-мошенников выступает склонность к риску и авантюризму, сочетающаяся с завышенной самооценкой и уверенностью в собственной неуязвимости. Указанные качества особенно выражены у лиц, занимающихся разработкой сложных мошеннических схем и осуществлением целенаправленных атак на крупные финансовые организации. Ощущение анонимности и безнаказанности, создаваемое использованием современных технологий и трансграничным характером киберпреступности, усиливает данные психологические установки и способствует эскалации преступной деятельности. Вместе с тем, для значительной части исполнителей низового звена характерны иные психологические особенности, включая повышенную внушаемость, зависимость от лидеров преступных групп, недостаточную способность к критическому осмыслению собственных действий[1].

Исследователи обращают особое внимание на проблему вовлечения в интернет-мошенничество лиц, ранее не проявлявших противоправной активности и характеризовавшихся в целом положительно. В научной литературе описываются механизмы криминализации, действующие в отношении таких лиц под влиянием различных факторов, включая материальные трудности, давление со стороны преступных групп, а также идеологическую обработку через деструктивные онлайн-сообщества, популяризирующие противоправные способы обогащения. Особую опасность в

[1] Кузовлева Н.Ф,, Хусаинов М.К. К вопросу об интерне-мошенничестве в условиях интенсивной цифровизации общества // Светоч науки. 2025. № 2. С. 197.

этом контексте представляют Telegram-каналы, форумы и иные интернет-площадки, где в завуалированной или открытой форме предлагаются услуги по участию в мошеннических схемах, размещается информация о вакансиях в кол-центрах и иные материалы, способствующие рекрутированию новых участников преступной деятельности[1].

Организованный характер современного интернет-мошенничества обусловливает необходимость анализа личности преступника в контексте групповой динамики и распределения ролей. В криминологической литературе выделяются несколько типов участников организованных групп, специализирующихся на интернет-мошенничестве.

Организаторы и лидеры преступных сообществ, как правило, обладают высокими интеллектуальными и организаторскими способностями, опытом управления, навыками конспирации и обеспечения безопасности. Разработчики вредоносного программного обеспечения и технические специалисты характеризуются глубокими познаниями в области информационных технологий, программирования, сетевой инфраструктуры. Операторы кол-центров, осуществляющие непосредственное взаимодействие с жертвами, должны обладать развитыми коммуникативными навыками, психологической устойчивостью, способностью к быстрому реагированию на изменяющиеся обстоятельства. Дропперы и курьеры, обеспечивающие вывод и обналичивание похищенных средств, как правило, рекрутируются из числа лиц с невысоким социальным статусом, материальными проблемами и недостаточно развитым правосознанием. Каждый из указанных типов характеризуется специфическими социально-демографическими и психологическими особенностями, что требует дифференцированного подхода при разработке мер профилактики и предупреждения.

Особое место в криминологической характеристике занимают так называемые ситуативные мошенники, совершающие противоправные действия

---

[1] Кильметова Р.Р., Савлохов Р.Р. Современные виды мошенничества в сети Интернет и пути их разрешения // Аграрное и земельное право. 2025. № 7. С. 267.

под влиянием стечения обстоятельств, не имея изначальной установки на систематическую преступную деятельность. Такие лица могут случайно обнаружить уязвимость в системе безопасности какого-либо сервиса и воспользоваться ею для получения выгоды, либо поддаться на предложение легкого заработка, поступившее от знакомых или через интернет-рекламу. Для ситуативных мошенников характерна неустойчивость антиобщественных установок, наличие определенных сдерживающих факторов, способность к осознанию противоправности своих действий и раскаянию. В отношении данной категории преступников наиболее эффективными могут оказаться меры профилактического и воспитательного характера, а также не связанные с лишением свободы меры уголовно-правового воздействия.

Важным направлением криминологического анализа выступает изучение мотивации лиц, совершающих интернет-мошенничества. Традиционно основным мотивом выступает корысть, стремление к незаконному обогащению, получению материальной выгоды. Однако исследования показывают, что мотивационная структура указанных преступлений значительно сложнее и включает помимо корысти также мотивы самоутверждения, стремление к острым ощущениям, желание испытать свои силы и возможности, а в некоторых случаях и идеологические мотивы, связанные с противопоставлением себя обществу, государству, существующей социально-экономической системе. Для отдельных категорий интернет-мошенников, особенно из числа молодых людей с высоким уровнем технической подготовки, важным стимулом выступает признание в соответствующем сообществе, повышение статуса среди единомышленников, подтверждение своей исключительности и превосходства над окружающими[1].

Современные научные исследования уделяют значительное внимание проблеме трансформации личности интернет-мошенника под влиянием развития технологий и изменения социально-экономических условий.

[1] Новосельцева А.С. Интернет-мошенничество: ключевые проблемы борьбы и превентивных мер // Актуальные исследования. 2025. № 2. С. 76.

Отмечается тенденция к профессионализации и специализации преступной деятельности, повышению технической оснащенности злоумышленников, использованию ими сложных многоходовых схем, включающих элементы социальной инженерии, фишинга, вредоносного программного обеспечения и иных инструментов[1]. Указанные изменения предъявляют новые требования к личности преступника, который должен обладать все более широким спектром знаний и навыков, способностью к быстрому обучению и адаптации, готовностью к использованию передовых технологических достижений в противоправных целях. Одновременно наблюдается усиление транснационального характера киберпреступности, что предполагает взаимодействие преступников из различных стран, использование зарубежной инфраструктуры, преодоление языковых и культурных барьеров.

Значительный научный интерес представляет сравнительный криминологический анализ личности традиционного мошенника и мошенника, действующего в сети Интернет. Исследователи отмечают, что при сохранении базовых признаков мошенничества как хищения путем обмана или злоупотребления доверием, интернет-мошенничество приобретает специфические черты, обусловленные опосредованным характером взаимодействия с жертвой, использованием информационно-телекоммуникационных технологий, возможностью анонимизации и сокрытия следов[2]. Указанные особенности накладывают отпечаток на личность преступника, который в меньшей степени нуждается в развитых навыках межличностного общения, но должен обладать определенным уровнем технической компетентности либо иметь доступ к соответствующим ресурсам и услугам, предоставляемым в теневом сегменте сети.

Проблема противодействия интернет-мошенничеству неразрывно связана

---

[1] Авдошкин А.А. О проблемах мошенничества в сети Интернет // Теория и практика кооперации в современном обществе: сборник научных статей. Саранск, 2025. С. 32.

[2] Безбородова Л.С., Девятых А.В. Мошенничество в интернет-пространстве: виды и способы наживы // Юриспруденция: актуальные вопросы теории и практики: сборник научных статей. Пенза, 2024. С. 75.

с задачей изучения личности преступника и разработки на этой основе эффективных мер профилактического воздействия. Криминологические исследования позволяют выделить наиболее уязвимые категории населения с точки зрения риска вовлечения в преступную деятельность и предложить адресные меры предупреждения, включая информационно-просветительскую работу, социальную поддержку, создание альтернативных возможностей для самореализации и законного заработка, особенно для молодежи. Важное значение имеет также работа по разоблачению мифов о легких и быстрых деньгах, популяризация традиционных ценностей и законопослушного поведения, формирование в обществе нетерпимого отношения к любым формам противоправного обогащения[1].

Таким образом, современное состояние интернет-мошенничества характеризуется профессионализацией и специализацией преступной деятельности, усилением ее организованного и транснационального характера, активным использованием злоумышленниками передовых технологий и методов социальной инженерии, что предъявляет новые требования к системе профилактики, которая должна сочетать совершенствование законодательной базы, развитие технических средств защиты, повышение цифровой грамотности населения и адресную работу с группами риска, включая молодежь и лиц, потенциально уязвимых для вовлечения в преступную деятельность.

§ 3. Предупреждение мошенничества в глобальной сети

Предупреждение мошенничества в глобальной сети представляет собой комплексную проблему, требующую системного подхода, объединяющего усилия государства, финансовых институтов, операторов связи и самих

[1] Фомина П.С. Особенности интернет-мошенничества в России // Педагогический конференциум: сборник научных трудов и материалов научно-практических конференций. 2024. № 2. С. 223.

граждан. В основе предупредительной деятельности лежит понимание многообразия способов совершения мошеннических действий, постоянной эволюции преступных схем и высокой адаптивности злоумышленников к изменяющимся условиям, что требует адекватного реагирования со стороны всех субъектов системы противодействия.

Система предупреждения интернет-мошенничества традиционно подразделяется на меры общесоциального, специально-криминологического и индивидуального характера, каждая из которых имеет собственное содержание и направленность.

Общесоциальное предупреждение включает комплекс экономических, социальных, культурных и воспитательных мероприятий, опосредованно влияющих на состояние преступности путем устранения причин и условий, способствующих совершению противоправных деяний. Повышение уровня жизни населения, сокращение имущественного расслоения, развитие системы образования и просвещения создают благоприятный фон для снижения криминогенного потенциала общества и формирования устойчивых антикорыстных установок у граждан. Особое значение в современных условиях приобретает развитие цифровой инфраструктуры и обеспечение равного доступа различных категорий населения к современным технологиям, что позволяет минимизировать цифровое неравенство и связанные с ним риски виктимизации.

Специально-криминологическое предупреждение интернет-мошенничества представляет собой совокупность мер, непосредственно направленных на выявление и устранение обстоятельств, способствующих совершению данных преступлений, а также на предотвращение конкретных противоправных деяний. В указанной сфере можно выделить несколько основных направлений деятельности, включая совершенствование законодательной базы, развитие технических средств защиты, организацию взаимодействия между правоохранительными органами, кредитными организациями и операторами связи, а также проведение профилактической

работы с населением. Каждое из названных направлений требует постоянного развития и адаптации к быстро меняющимся условиям цифровой среды и появлению новых способов совершения мошеннических действий.

Законодательное обеспечение противодействия интернет-мошенничеству в последние годы претерпело существенные изменения, направленные на создание эффективных правовых механизмов защиты граждан и организаций. Принятие Федерального закона № 41-ФЗ от 1 апреля 2025 года ознаменовало создание государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационно-телекоммуникационных технологий, которая призвана обеспечить оперативный обмен данными в режиме реального времени между правоохранительными органами, Банком России, кредитными организациями и операторами сотовой связи.

Разрабатываемый в настоящее время пакет законодательных мер, вступление в силу которого планируется на 2026-2027 годы, предусматривает дальнейшее совершенствование системы противодействия интернет-мошенничеству. Предполагается расширение объема информации, подлежащей включению в государственную информационную систему, включая данные о потерпевших и записи телефонных разговоров, содержащих признаки противоправной деятельности. Особое внимание уделяется вопросам идентификации абонентского оборудования и противодействия использованию подменных номеров, что должно существенно затруднить деятельность мошеннических кол-центров и снизить эффективность методов социальной инженерии[1].

Технические средства защиты играют все более значимую роль в системе предупреждения интернет-мошенничества, поскольку позволяют выявлять и блокировать противоправные действия на ранних стадиях, не дожидаясь

[1] Черныш М.А., Кумарин А.А. Интернет-мошенничество в современной России // Актуальные проблемы теории и практики уголовного права и процесса: сборник научных статей. Ростов-на-Дону, 2025. С. 236.

наступления общественно опасных последствий. Современные антифрод-системы, используемые кредитными организациями, демонстрируют впечатляющую эффективность, предотвращая хищения средств на миллиарды рублей и блокируя миллионы подозрительных операций. В основе работы указанных систем лежат методы машинного обучения и искусственного интеллекта, позволяющие анализировать транзакционные потоки в реальном времени, выявлять аномалии в поведении пользователей и оперативно реагировать на подозрительные операции.

Развитие биометрических технологий и усиление контроля за идентификацией клиентов создают дополнительные барьеры для злоумышленников, существенно усложняя несанкционированный доступ к финансовым средствам граждан.

Значительные перспективы связаны с внедрением систем поведенческого анализа и сетевого мониторинга, позволяющих выявлять сложные многоходовые мошеннические схемы, включающие взаимодействие различных субъектов и использование множества транзакций. Интеграция разнородных источников данных, включая информацию от банков, операторов связи и правоохранительных органов, создает условия для формирования целостной картины криминальной активности и оперативного выявления организованных преступных групп, специализирующихся на интернет-мошенничестве. Дальнейшее развитие указанных технологий должно быть направлено на повышение точности прогнозирования и минимизацию ошибок, что позволит снизить издержки законопослушных пользователей и повысить доверие к системам автоматической защиты.

Организационные меры противодействия интернет-мошенничеству включают совершенствование деятельности правоохранительных органов, развитие межведомственного взаимодействия и координацию усилий различных субъектов системы предупреждения. Создание специализированных подразделений по борьбе с киберпреступностью, повышение квалификации сотрудников, внедрение современных методик расследования и

криминалистического обеспечения позволяют постепенно повышать раскрываемость данных преступлений и привлекать виновных к ответственности.

Важное значение имеет также развитие международного сотрудничества в сфере противодействия транснациональной киберпреступности, поскольку значительная часть мошеннических кол-центров располагается за пределами Российской Федерации, а используемые злоумышленниками технические средства позволяют эффективно маскировать реальное местонахождение преступников.

Взаимодействие правоохранительных органов с кредитными организациями и операторами связи приобретает особое значение в условиях стремительного развития технологий и постоянного усложнения способов совершения мошеннических действий. Создание государственной информационной системы противодействия правонарушениям призвано обеспечить оперативный обмен информацией и координацию усилий всех заинтересованных субъектов, что должно существенно повысить эффективность выявления и пресечения противоправной деятельности. Важным направлением выступает также развитие механизмов частно-государственного партнерства, позволяющих объединять ресурсы и компетенции различных организаций для решения общих задач противодействия киберпреступности.

Профилактика интернет-мошенничества среди населения представляет собой одно из наиболее важных направлений предупредительной деятельности, поскольку значительная часть преступлений совершается с использованием методов социальной инженерии, основанных на манипулировании человеческой психикой, а не на взломе технических систем защиты[1].

Повышение цифровой грамотности граждан, формирование навыков безопасного поведения в сети, информирование о наиболее распространенных

[1] Барабанова Д.А. Интернет мошенничество. Способы борьбы // Тенденции развития науки и образования. 2025. № 2. С. 27.

мошеннических схемах и способах противодействия им позволяют существенно снизить виктимность населения и создать условия для эффективного сопротивления преступным посягательствам. Наблюдается тенденция к росту осведомленности граждан о методах обмана, многие распознают мошенников по типичным легендам, о которых ранее читали или слышали из средств массовой информации и от близких.

Особого внимания требует профилактическая работа с наиболее уязвимыми категориями населения, включая пожилых людей, несовершеннолетних, лиц с низким уровнем образования и ограниченным доступом к информации. Пожилые граждане, несмотря на относительно невысокую интенсивность использования цифровых технологий, часто становятся жертвами мошенников в силу доверчивости, недостаточной осведомленности о современных схемах обмана и трудностей с критическим восприятием информации. Цифровая социализация старшего поколения, включающая обучение правилам безопасного поведения в сети, развитие навыков распознавания мошеннических схем и формирование устойчивых поведенческих реакций, выступает важным направлением профилактической деятельности, способным существенно снизить риски для указанной категории граждан.

Важным направлением профилактики выступает работа с молодежью, направленная на предотвращение вовлечения несовершеннолетних в мошенническую деятельность в качестве соучастников. Распространение в сети предложений легкого заработка, рекрутирование лиц, предоставляющих свои банковские карты для вывода средств, и курьеров через социальные сети и мессенджеры создают серьезные риски криминализации молодого поколения, недостаточно осознающего юридические последствия участия в противоправных схемах.

Профилактическая работа в образовательных учреждениях, разъяснение уголовной ответственности за соучастие в мошенничестве, формирование устойчивых антикорыстных установок и навыков критического мышления

позволяют снизить указанные риски и создать условия для законопослушного поведения молодежи в цифровой среде.

Индивидуальное предупреждение интернет-мошенничества включает меры воздействия на конкретных лиц, склонных к совершению данных преступлений, а также на потенциальных жертв, характеризующихся повышенной виктимностью. Работа с лицами, ранее судимыми за аналогичные преступления, профилактические беседы, социальный контроль и оказание помощи в трудоустройстве и решении социальных проблем позволяют снизить риск рецидива и способствуют ресоциализации осужденных. Виктимологическая профилактика, направленная на выявление граждан с повышенным риском стать жертвой мошенничества и проведение с ними соответствующей работы, также играет важную роль в общей системе предупредительных мер.

Результаты социологических исследований демонстрируют определенный прогресс в сфере противодействия интернет-мошенничеству, связанный с повышением информированности населения и совершенствованием технических средств защиты. Значительная часть граждан, столкнувшихся с попытками мошенничества, сумела избежать потери денежных средств благодаря своевременному распознаванию преступных схем и обращению за помощью к близким или сотрудникам банков. При этом сохраняются серьезные проблемы, связанные с недостаточной осведомленностью части населения, высокой эффективностью методов социальной инженерии, заставляющих жертв в момент общения забывать о мерах предосторожности, и сложностью возврата похищенных средств после их перевода на счета злоумышленников[1].

Совершенствование механизмов противодействия интернет-мошенничеству требует постоянного мониторинга криминогенной ситуации, анализа новых способов совершения преступлений и оперативной разработки

[1] Новосельцева А.С. Интернет-мошенничество: ключевые проблемы борьбы и превентивных мер // Актуальные исследования. 2025. № 2. С. 77.

адекватных мер реагирования. Важное значение имеет также изучение зарубежного опыта и адаптация наиболее успешных практик к российским условиям с учетом особенностей национальной правовой системы и сложившихся социально-экономических отношений. Дальнейшее развитие системы предупреждения должно быть направлено на усиление координации между различными субъектами, повышение эффективности технических средств защиты, совершенствование законодательной базы и активизацию профилактической работы с населением.

Анализ современных тенденций развития интернет-мошенничества позволяет прогнозировать дальнейшее усложнение способов совершения преступлений, активное использование злоумышленниками технологий искусственного интеллекта, включая создание реалистичных подделок голоса и изображения, а также усиление транснационального характера киберпреступности.

Таким образом, система предупреждения мошенничества в глобальной сети представляет собой сложный многоуровневый комплекс, объединяющий правовые, организационные, технические и профилактические меры, реализуемые различными субъектами на общесоциальном, специально-криминологическом и индивидуальном уровнях. Эффективность указанной системы зависит от скоординированности действий всех участников, постоянного совершенствования используемых методов и средств, а также от уровня цифровой грамотности и сознательности самих граждан, выступающих первым и наиболее важным барьером на пути мошеннических посягательств. Только комплексный подход, учитывающий все многообразие факторов, детерминирующих интернет-мошенничество, и опирающийся на передовые технологические достижения и научно обоснованные методики профилактики, способен обеспечить долгосрочное и устойчивое снижение уровня данного вида преступности и минимизацию причиняемого им ущерба.

ЗАКЛЮЧЕНИЕ

Проведенное исследование теоретико-правовых основ, криминологической характеристики и системы предупреждения интернет-мошенничества позволяет сформулировать обобщающие выводы, отражающие современное состояние и перспективы противодействия данному негативному социальному явлению.

1. Интернет-мошенничество представляет собой сложный многоаспектный феномен, не имеющий легального определения, но охватывающий совокупность общественно опасных деяний, совершаемых с использованием информационно-телекоммуникационных технологий путем обмана или злоупотребления доверием. Юридическая квалификация указанных деяний базируется на нормах статей 159, 159.3 и 159.6 Уголовного кодекса Российской Федерации, при этом выбор конкретной нормы определяется способом взаимодействия преступника с жертвой или информационной системой, что требует от правоприменителя глубокого анализа объективной стороны преступления и учета разъяснений высшей судебной инстанции.

2. Историческое развитие интернет-мошенничества прошло путь от единичных примитивных схем до масштабной высокоорганизованной индустрии с четким разделением труда, использованием методов социальной инженерии и технологий искусственного интеллекта, что нашло отражение в многообразии классификаций способов совершения данных преступлений, учитывающих характер взаимодействия с жертвой, используемые технические средства, предмет посягательства и степень организованности преступных групп.

3. Криминологический анализ современного состояния интернет-мошенничества в России выявляет противоречивую динамику: при некотором сокращении количества регистрируемых преступлений сумма причиняемого ущерба продолжает расти, достигая сотен миллиардов рублей ежегодно, что свидетельствует о качественной трансформации преступности в сторону более

точечных и дорогостоящих атак.

4. Факторами, способствующими совершению данных деяний, выступают организованный характер киберпреступности, недостаточный уровень цифровой грамотности населения, активное использование злоумышленниками технологий искусственного интеллекта, высокая латентность преступлений, трансграничный характер противоправной деятельности и вовлечение несовершеннолетних в преступные схемы.

5. Личность интернет-мошенника характеризуется значительной неоднородностью и дифференцируется в зависимости от роли в преступной иерархии: от высококвалифицированных специалистов в области информационных технологий до исполнителей низового звена с невысоким образовательным уровнем, при этом наблюдаются тенденции к омоложению контингента и феминизации отдельных сегментов преступной деятельности, а также деформация ценностно-нормативной сферы, проявляющаяся в ориентации на материальное благополучие любой ценой и отсутствии эмпатии к жертвам.

6. Система предупреждения интернет-мошенничества представляет собой многоуровневый комплекс мер общесоциального, специально-криминологического и индивидуального характера, реализуемых государством, финансовыми институтами, операторами связи и институтами гражданского общества. Особое значение в системе предупреждения приобретает профилактическая работа с населением, направленная на повышение цифровой грамотности, информирование о мошеннических схемах и формирование навыков безопасного поведения в сети, при этом адресные меры должны применяться к наиболее уязвимым категориям граждан, включая пожилых людей, несовершеннолетних и лиц с низким уровнем образования.

Проведенное исследование позволяет выделить ряд существенных проблем, затрудняющих эффективное противодействие интернет-мошенничеству в современных условиях.

1. Прежде всего сохраняется проблема законодательного регулирования,

выражающаяся в противоречивости конструкции ст.и 159.6 УК РФ, которая при формальном отнесении к мошенничеству фактически не предполагает наличия обмана или злоупотребления доверием как обязательных признаков состава преступления, что порождает сложности квалификации и разграничения со смежными составами.

2. Существенной проблемой выступает высокий уровень латентности данных преступлений, обусловленный как объективными трудностями выявления цифровых следов и трансграничным характером противоправной деятельности, так и нежеланием значительной части потерпевших обращаться в правоохранительные органы из-за неверия в возможность раскрытия преступления и возврата похищенного.

3. Серьезным препятствием является недостаточный уровень цифровой грамотности населения, особенно среди старших возрастных групп, при одновременном активном использовании злоумышленниками сложных методов социальной инженерии и технологий искусственного интеллекта, включая создание дипфейков, что делает значительную часть граждан уязвимой перед мошенническими посягательствами.

4. Проблема вовлечения несовершеннолетних и молодежи в преступную деятельность в качестве дропперов и курьеров усугубляется распространением в сети предложений легкого заработка и недостаточной профилактической работой в образовательных учреждениях.

5. Сохраняется проблема трансграничного характера киберпреступности, когда значительная часть кол-центров располагается за пределами Российской Федерации, что затрудняет привлечение организаторов к ответственности и требует развития международного сотрудничества.

В качестве путей решения указанных проблем представляется необходимым дальнейшее совершенствование уголовного законодательства в части уточнения признаков составов преступлений, предусмотренных статьями 159.3 и 159.6 УК РФ, с целью устранения противоречий в квалификации и обеспечения единообразия правоприменительной практики.

Важным направлением выступает развитие государственной информационной системы противодействия правонарушениям, включая расширение объема обрабатываемой информации, совершенствование механизмов межведомственного взаимодействия и обеспечение оперативного обмена данными между всеми субъектами противодействия в режиме реального времени.

Необходима активизация профилактической работы с населением, включая реализацию специализированных программ повышения цифровой грамотности для различных возрастных и социальных групп, широкое информирование о новых мошеннических схемах через средства массовой информации и социальную рекламу, а также проведение разъяснительной работы в образовательных учреждениях с целью предотвращения вовлечения молодежи в преступную деятельность.

Требуется дальнейшее развитие технических средств защиты, включая совершенствование антифрод-систем на базе искусственного интеллекта, внедрение поведенческого анализа и сетевого мониторинга, развитие биометрических технологий и усиление контроля за идентификацией абонентского оборудования.

Важным направлением выступает развитие международного сотрудничества в сфере противодействия транснациональной киберпреступности, включая заключение соответствующих соглашений, гармонизацию законодательства и координацию усилий правоохранительных органов различных государств.

Только комплексная реализация указанных мер в сочетании с повышением цифровой грамотности и сознательности самих граждан способна обеспечить долгосрочное и устойчивое снижение уровня интернет-мошенничества и минимизацию причиняемого им ущерба.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ, от 06.10.2022) // Собр. законодательства Рос. Федерации. 2022. №11, ст.1416.

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собр. законодательства Рос. Федерации. 2001. № 52 (ч. 1), ст. 4921.

3. Уголовный кодекс РФ: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства Рос. Федерации. 1996. № 25. ст. 2954.

4. О полиции: Федеральный закон Рос. Федерации от 07.02.2011 № 3-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 7, ст. 900.

5. О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. Закон Рос. Федерации от 01.04.2025 № 41-ФЗ // СПС КонсультантПлюс.

II. Учебная, научная литература

1. Атанова О.Е. Преступления в сфере компьютерной информации как актуальная проблема // Студенческий вестник. 2024. № 37. С. 33-37.

2. В «Сбере» оценили объем похищенных мошенниками средств в 295 млрд рублей [Электронный ресурс]. Режим доступа: https://expert.ru/news (Дата обращения: 30.01.2026).

3. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2025 года [Электронный ресурс]. Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/77848182/ (Дата обращения:

30.01.2025).

4. Маликов С.В. Пробелы уголовного законодательства о преступлениях в сфере компьютерной информации / В сб.: Институциональные основы уголовного права РФ. Краснодар, 2024. С. 504-513.

5. Ущерб граждан от киберпреступлений за 8 месяцев вырос до 134 млрд рублей [Электронный ресурс]. Режим доступа: nterfax-russia.ru (Дата обращения: 30.01.2026).

6. Хмелевский Э.С. Проблемы квалификации преступлений в сфере компьютерной информации / В сб.: Пермский период. Пермь, 2024. С. 450-452.

7. Цейтлин Н.Ф. Преступления, связанные с использованием IT-технологий: проблемы выявления и расследования // Актуальные вопросы охраны общественного порядка и административной деятельности: сборник научных статей. М., 2022. С. 189-192.

8. Ястребова Т.И., Горбунов Д.С. Отдельные проблемы уголовно-правовой характеристики преступлений в сфере компьютерной информации // Научное образование. 2023. № 3. С. 229-232.

9. Авдеенко В.О. Мошенничество в Интернет // Наука. Промышленность. Оборона: сборник научных статей. Новосибирск, 2025. С. 110-114.

10. Авдошкин А.А. О проблемах мошенничества в сети Интернет // Теория и практика кооперации в современном обществе: сборник научных статей. Саранск, 2025. С. 31-33.

11. Барабанова Д.А. Интернет мошенничество. Способы борьбы // Тенденции развития науки и образования. 2025. № 2. С. 25-28.

12. Безбородова Л.С., Девятых А.В. Мошенничество в интернет-пространстве: виды и способы наживы // Юриспруденция: актуальные вопросы теории и практики: сборник научных статей. Пенза, 2024. С. 73-76.

13. Бутракова Ю.А., Орлова Л.В. Интерне мошенничество. Способы

защиты // Проблемы развития современного общества : сборник научных статей. Курск, 2025. С. 211-213.

14. Давыдов А.А. Интернет-мошенничество как актуальная проблема нового времени // Наука XXI века: актуальные направления развития. 2024. № 1. С. 513-516.

15. Кильметова Р.Р., Савлохов Р.Р. Современные виды мошенничества в сети Интернет и пути их разрешения // Аграрное и земельное право. 2025. № 7. С. 264-268.

16. Кузовлева Н.Ф,, Хусаинов М.К. К вопросу об интерне-мошенничестве в условиях интенсивной цифровизации общества // Светоч науки. 2025. № 2. С. 192-200.

17. Кулешова Ю.Г. Современные аспекты интернет-мошенничества: способы совершения и методы противодействия // Криминалистика: актуальные вопросы теории и практики: сборник научных статей. Ростов-на-Дону, 2025. С. 129-135.

18. Лобаченко И.А. Киберпреступность: анализ и классификация интернет-мошенничества // Актуальные и перспективные научные исследования: сборник научных статей. Пенза, 2025. С. 152-155.

19. Минакова Т.А. Интернет-мошенничество: схемы обмана и способы защиты // Современные вызовы экономики, управления и здоровья: Россия с многополярном мире: сборник научных статей. Санкт-Петербург, 2025. С. 308-313.

20. Михайлов К.В. Развитие интернет-мошенничества в России: анализ основных типов мошенничества // Уголовно-правовые, уголовно-исполнительные и криминологические проблемы обеспечения безопасности человека, общества и государства: сборник научных статей. Санкт-Петербург, 2025. С. 107-109.

21. Новосельцева А.С. Интернет-мошенничество: ключевые проблемы борьбы и превентивных мер // Актуальные исследования. 2025. № 2. С. 75-77.

22. Новрузов И.Н., Новрузов Д.Н. Способы защиты от интернет-мошенничества // Тенденции развития науки и образования. 2025. № 2. С. 133-136.

23. Орлова Л.В., Козлов А.М. Интернет-мошенничество: вызов цифровой безопасности и пути его преодоления // Тенденции развития науки и образования. 2025. № 2. С. 142-145.

24. Попов Ю.Л., Шестаков Д.Р. Мошенничества в Интернет // Актуальные исследования. 2025. № 1. С. 45-47.

25. Ройхка А.А. Особенности интернет-мошенничества в современную эпоху: криминологический аспект // Закон. Право. Государство. 2024. № 4. С. 240-241.

26. Сазанова А.А. Современные способы мошенничества в сети Интернет // Актуальные проблемы инновационных систем информатизации и безопасности: сборник научных статей. Воронеж, 2025. С. 491-493.

27. Фомина П.С. Особенности интернет-мошенничества в России // Педагогический конференциум: сборник научных трудов и материалов научно-практических конференций. 2024. № 2. С. 214-230.

28. Черныш М.А., Кумарин А.А. Интернет-мошенничество в современной России // Актуальные проблемы теории и практики уголовного права и процесса: сборник научных статей. Ростов-на-Дону, 2025. С. 233-237.

29. Чуб И.С. Мошенничество в сети Интернет: способы совершения и виктимологическая профилактика // Вестник Краснодарского университета МВД России. 2024. № 1. С. 39-42.

30. Юдина И.А., Орлова Л.В. Интернет мошенничество. Способы защиты // Тенденции развития науки и образования. 2025. № 2. С. 212-215.

III. Материалы судебной практики

1. Дело № 1-87/2022 (1-554/2021) Куйбышевский районный суд г. Омска // Государственная автоматизированная система РФ «Правосудие». Интернет-портал [Электронный ресурс] // URL: https://sudrf.ru/ (дата обращения:

20.12.2025).

2. Дело № 1-254/2022 Железнодорожный районный суд города Красноярска // Государственная автоматизированная система РФ «Правосудие». Интернет-портал [Электронный ресурс] // URL: https://sudrf.ru/ (дата обращения: 20.12.2025).

3. Дело № 1-140/2022 Вольский районный суд Саратовской области // Государственная автоматизированная система РФ «Правосудие». Интернет-портал [Электронный ресурс] // URL: https://sudrf.ru/ (дата обращения: 20.12.2025).

4. Постановление Пленума Верховного суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. 2017. 11 декабря.

5. Постановление Пленума Верховного суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет» // Российская газета. 2022. 28 декабря.

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну Д.М. Пономарева