

Федеральное государственное казенное образовательное
учреждение высшего образования
«Сибирский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность
(специализация Оперативно – розыскная деятельность,
Профиль образовательной программы – Деятельность подразделений по
Контролю за оборотом наркотиков), заочная форма обучения

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:
**КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА
МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ
СЕТИ ИНТЕРНЕТ**

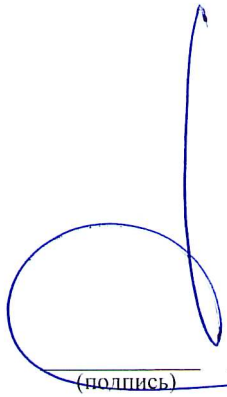
Выполнил:
Слушатель группы П 2012
капитан внутренней службы
Вайсброт Виктор Владимирович

Руководитель:
доцент кафедры криминалистики
кандидат юридических наук
подполковник полиции
Харина Елена Алексеевна

Дата защиты:
«10» апреля 2026 г.

Оценка: хорошо

Председатель ГЭК
Иванович Иван Иванович
(специальное звание)


(подпись) В.В. Вайсброт
(инициалы, фамилия)

Красноярск 2026

Федеральное государственное казенное образовательное
учреждение высшего образования
«Сибирский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность
(специализация Оперативно – розыскная деятельность,
Профиль образовательной программы – Деятельность подразделений по
Контролю за оборотом наркотиков), заочная форма обучения

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:
КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА
МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ
СЕТИ ИНТЕРНЕТ

Выполнил:
Слушатель группы П 2012
капитан внутренней службы
Вайсброт Виктор Владимирович

Руководитель:
доцент кафедры криминалистики
кандидат юридических наук
подполковник полиции
Харина Елена Алексеевна

Дата защиты:
«__» _____ 2026 г.

Оценка: _____

Председатель ГЭК

(специальное звание)

(подпись)

(инициалы, фамилия)

Красноярск 2026

Оглавление

Введение.....	3
Глава 1. ПРАВОВАЯ ХАРАКТЕРИСТИКА ПОЛНОМОЧИЙ ПОЛИЦИИ В ВЫЯВЛЕНИИ И ПРЕСЕЧЕНИИ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ	7
1.1. Понятие и классификация полномочий полиции по выявлению и пресе- чению мошенничества, совершенного с использованием сети Интернет	7
1.2. Отграничение мошенничества, совершенного с использованием сети Интернет от "традиционного" мошенничества.....	15
Глава 2. ИССЛЕДОВАНИЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ИНТЕРНЕТ-МОШЕННИЧЕСТВА	24
2.1. Типичные способы мошенничества, совершенного с использованием сети Интернет	24
2.2. Криминалистическая характеристика личности интернет-мошенника ...	30
2.3. Криминалистическая характеристика жертвы мошенничества, совершенного с использованием сети Интернет	41
2.4. Механизм мошенничества, совершенного с использованием сети Интернет.....	48
2.5. Типичные следы мошенничества, совершенного с использованием сети Интернет.....	55
Заключение	63
Список использованной литературы.....	67

Введение

Актуальность темы исследования. Информационные технологии – это неотъемлемая часть жизни современного человека. В настоящее время человек может получить онлайн практически любую услугу, приобрести вещь и совершить иные действия. Между тем с распространением онлайн-форм взаимодействия, растет и число преступлений, совершенных с использованием информационных технологий.

Например, в 2025 году МВД России зафиксировало 663 тыс. киберпреступлений¹. При этом рост численности совершаемых преступлений требует развития и совершенствования подходов и методик их предотвращения, привлечения к уголовной ответственности преступников. Вместе с тем на данный момент отмечаются определенные трудности в выявлении и расследовании данных преступлений ввиду особенностей способа совершения, а также его высокой адаптивности и новизной. В связи с этим на данный момент исследование тактических особенностей расследования мошенничества, совершаемого с использованием информационных технологий, не теряет своей актуальности. Данная статистика указывает на актуальность исследования аспектов тактических особенностей расследования преступлений, совершенных с использованием информационных технологий.

Таким образом, актуальность темы исследования определена теоретической и практической значимостью исследования данной темы для повышения качества расследования и доказывания преступлений, снижения общей численности преступлений данного вида.

Степень научной разработанности. Следует отметить, что тема мошенничества, совершенного с использованием информационных технологий является достаточно хорошо изученной, что во многом

¹ МВД: число киберпреступлений в России снизилось на 12% в 2025 году. URL: <https://www.kommersant.ru/doc/8442339> (Дата обращения 24.03.2026)

определено их актуальностью в настоящее время. В частности, следует отметить работы Р.С. Антонова, Р.А. Белевского, В.Б. Вехова, Д.А. Ермоленко, В.В. Коломинова, В.В. Крылова, Е.А. Хариной, Е.С. Шевченко и других, которые изучают вопросы криминалистической характеристики преступлений, совершенных с использованием информационных технологий.

Объект исследования – преступная деятельность в форме мошенничества, совершенного с использованием сети Интернет, а также деятельность правоохранительных органов по выявлению, раскрытию и расследованию данных преступных посягательств.

Предмет исследования – закономерности мошенничества, совершенного с использованием сети Интернет, а также связанные с ними закономерности деятельности правоохранительных органов по выявлению, раскрытию, расследованию указанных преступлений.

Цель работы – выявление криминалистически значимых характеристик мошенничества, совершенного с использованием сети Интернет, а также перспектив развития правового регулирования выявления и пресечения мошенничества, совершенного с использованием сети Интернет.

Поставленная цель обусловила выделение следующих задач:

- 1) Определить понятие и классификацию полномочий полиции в сфере предотвращения и выявления мошенничества, совершенного с использованием сети Интернет.
- 2) Выявить особенности отграничения мошенничества, совершенного с использованием сети Интернет, от иных видов мошенничества.
- 3) Охарактеризовать основные схемы и алгоритмы совершения мошенничества, совершенного с использованием сети Интернет.
- 4) Проанализировать криминалистическую характеристику личности мошенника.
- 5) Рассмотреть криминалистическую характеристику жертвы мошенничества, совершенного с использованием сети Интернет.

6) Выделить слепообразование мошенничества, совершенного с использованием сети Интернет.

Теоретическая основа исследования. Теоретической основой для подготовки и написания исследования стали работы отечественных исследователей, посвященных уголовно-правовой и криминологической характеристике кибермошенничества. Так, следует отметить труды таких авторов, как С.С. Алексеев, В.Б. Вехов, Г.Р. Григорян, С.Б. Голятина, А.П. Козлов, В.В. Коломинов, А.Н. Попов, Т.Л. Тропина, Е.А. Харина, А.В. Шеслер, М.Д. Фролов и другие.

Нормативной базой исследования выступили Конституция РФ, федеральные законы РФ, постановления Пленумов Верховного Суда РФ, ведомственные нормативные правовые акты МВД России и другие нормативно-правовые акты.

Эмпирическую базу научного исследования составили соответствующие статистические данные МВД России, Генеральной прокуратуры России, а также соответствующие данные Судебного департамента при Верховном суде РФ, ЦБ РФ, опубликованная судебная практика судов РФ, а также сведения, размещенные в средствах массовой информации.

Поставленные исследовательские задачи решались с использованием как общенаучных методов эмпирического и теоретического познания (анализа, обобщения, классификации), частно-научных методов (статистического, психологического), так и специальных научных методов исследования (в том числе формально-догматического).

Значение разработки проблемы для теории и практики деятельности органов внутренних дел или иных правоохранительных органов. Теоретическая значимость исследования обусловлена возможностью применения сформулированных теоретических выводов для дальнейших научных исследований и совершенствования имеющихся трудов относительно криминалистической характеристики мошенничества,

совершенного с использованием сети Интернет. Практическая значимость исследования обусловлена возможностью использования научных положений и прикладных рекомендаций для повышения эффективности выявления, раскрытия и расследования мошенничества, совершенного с использованием сети Интернет.

Структура работы включает следующие элементы: введение, две главы, семь параграфов, заключение и список использованной литературы.

Глава 1. ПРАВОВАЯ ХАРАКТЕРИСТИКА ПОЛНОМОЧИЙ ПОЛИЦИИ В ВЫЯВЛЕНИИ И ПРЕСЕЧЕНИИ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

1.1. Понятие и классификация полномочий полиции по выявлению и пресечению мошенничества, совершенного с использованием сети Интернет

Информатизация общества несет не только обширные возможности для расширения доступа граждан к услугам, повышения комфорта взаимодействия, но и влечет определенные риски. Одним из таких рисков являются киберпреступлений, включая кибермошенничество. Данной проблеме способствуют упрощение и рост численности безналичных переводов, использования крупных информационных баз данных. Все это предоставляет новые возможности для преступников.

Проведенное исследование позволило заключить, что в практической деятельности мошенничество, совершенное с использованием сети Интернет, квалифицируется как по ст. 159 УК РФ, так и по введенной в действие в 2012 году ст. 159.6 УК РФ.

Современные способы совершения мошенничества с использованием сети Интернет влекут определенные проблемы для сотрудников правоохранительных органов при расследовании и предотвращении преступлений, в первую очередь в связи с трудностями в поиске следов преступления, а также выявлении преступника.

Мошенничество, совершенное с использованием сети Интернет, как уже было отмечено ранее, подразумевает использование интернет-технологий. Соответственно, чаще всего данный вид мошенничества связан с безналичными формами переводов, осуществляемыми с участием банков. Подобная практика определяет необходимость привлечения к профилактической работе не только сотрудников правоохранительных органов, но и кредитных организаций. В связи с этим сотрудники полиции

при расследовании случаев мошенничества, совершенного с использованием сети Интернет, могут привлекать специалистов кредитных организаций в качестве экспертов.

Правоохранительные органы – это основной субъект, уполномоченный на реализацию мер по противодействию мошенничеству, совершенному с использованием сети Интернет. Полномочия по реализации мер по защите правопорядка и обеспечению общественной безопасности возлагаются на органы внутренних дел. В соответствии со статьей 12 закона №58-ФЗ¹, на сотрудников ОВД возлагаются следующие обязанности: знать и обеспечивать соблюдение российского законодательства и должностной регламент, соблюдать права граждан и юридических лиц, соблюдать внутренний служебный распорядок, поддерживать уровень квалификации, беречь государственное имущество, соблюдать правила работы с информацией, предоставлять информацию о доходах и имуществе, сообщать информацию об изменении в вопросах гражданства, происшествиях и временной нетрудоспособности и другие.

По мнению И.С. Назарова, противодействие мошенничеству сочетает предупреждение преступлений, а также привлечение к ответственности². Данная позиция вполне логична, однако, не конкретизирует содержание противодействия мошенничеству, совершаемому с использованием сети Интернет. В соответствии с данной позицией, можно выделить три аспекта деятельности полиции по противодействию мошенничеству, совершенному с использованием сети Интернет: профилактика, выявление и раскрытие преступлений, а также привлечение к ответственности преступника.

Каждая из представленных стадий включает совокупность мероприятий, которые реализуются уполномоченными субъектами. Так, например, на первой стадии достаточно значительная роль отводится

¹ Федеральный закон от 27.05.2003 №58-ФЗ «О системе государственной службы Российской Федерации» // Справочно-правовая система Консультант-Плюс

² Назаров И.С. Проблемы борьбы с мошенничеством в сфере компьютерной информации // Молодой ученый. 2017. N40. С. 40-42

информационно-просветительской работе с населением, а также блокированием подозрительных сайтов, номеров. Эти полномочия возлагаются на полицию, например, в рамках проведения информационно-просветительской работы с населением, в ходе которой сотрудники полиции предоставляют информацию о том, какие способы мошенничества, совершенного с использованием сети Интернет, существуют, как распознать мошенника и не стать его жертвой. Данная обязанность сотрудников полиции определена в соответствии со ст. 2 Федерального закона от 07.02.2011 №3-ФЗ «О полиции»¹.

Выявление и раскрытие случаев мошенничества, совершенного с использованием сети Интернет, связаны с работой правоохранительных органов, органов предварительного следствия и дознания. Например, ст.2 Закона о полиции определяет одно из направлений деятельности полиции – выявление и раскрытие преступлений, производство дознания. В свою очередь, п.10 ст.12 Закона о полиции определяет также обязанность полиции по проведению оперативно-розыскной работы.

Данная работа связана с проверкой факта мошенничества, возбуждением и расследованием уголовного дела. В частности, для возбуждения уголовного дела необходимо проверить достаточность данных о совершении преступления (ст.140 УПК РФ)². С целью проверки получаемых сведений сотрудники осуществляют оперативно-розыскную деятельность, предусмотренную законом 12.08.1995 № 144-ФЗ³, а также ведомственными актами⁴.

¹ Федеральный закон от 07.02.2011 N 3-ФЗ (ред. от 28.11.2025) "О полиции" // Собрание законодательства Российской Федерации. 2011. N 7. Ст. 900

² Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 13.12.2024) // Собрание законодательства Российской Федерации. 2001. N 52. Ст. 4921

³ Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 29.12.2022) "Об оперативно-розыскной деятельности" // Собрание законодательства Российской Федерации. 1995. N 33. Ст. 3349

⁴Приказ МВД России N 776, Минобороны России N 703, ФСБ России N 509, ФСО России N 507, ФТС России N 1820, СВР России N 42, ФСИН России N 535, ФСКН России N 398, СК России N 68 от 27.09.2013 "Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в

Статья 144 УПК РФ устанавливает, что проверка факта мошенничества, по полученному сообщению, может осуществляться дознавателем посредством различных следственных и процессуальных действий. В первую очередь, в ходе получения письменного объяснения, дознаватель выясняет следующие факты:

1) Если мошенничество подразумевало размещение объявления о продаже несуществующего товара или оказании услуг, которые не были оказаны после оплаты, то следует выяснить информацию относительно объявления (ссылка на объявление, характеристика продаваемого товара или услуги, наличие отзывов), условия купли-продажи (стоимость, способов оплаты), информация о продавце (контактные данные, как представился, что сообщил о товаре, описание голоса);

2) Характеристики используемого устройства (технические характеристики устройства, номер, модель телефона, операционная система);

3) Информация о входе в мобильный банк, дата и время входа, информация о переводе (дата, время, сумма, на какой номер или счет);

4) Каким образом известил мошенников о совершении перевода, какова была реакция, что сообщили мошенники о дальнейших действиях;

5) Что жертва сделала после осознания факта мошенничества, обращался ли в банк, имеются ли выписки о переводе и ответы по обращениям;

6) Какой ущерб был причинен преступлениями¹.

Соответственно, фактически, для проверки факта мошенничества с использованием информационных технологий необходимо выявить все условия и сведения относительно произошедшей ситуации, действий

суд" (Зарегистрировано в Минюсте России 05.12.2013 N 30544) // Справочно-правовая система Консультант-Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_155629/ (Дата обращения 24.03.2026)

¹ Методические рекомендации "Расследование мошенничеств, связанных с реализацией товаров и оказанием услуг в сети Интернет". URL: https://49.xn--b1aew.xn--plai/citizen/Razjasnenija_MVD_Rossii (Дата обращения 24.03.2026)

участников, нанесенного ущерба. При этом описание ситуации нужно как можно более подробное. Например, если жертва указывает, что посещала отделение банка, филиалы или банкоматы, то следует выявить подробную информацию о данном факте, а также о лицах, с которым контактировал¹.

При необходимости для проверки факта мошенничества могут также собираться объяснения и у других лиц. Например, о взаимодействии жертвы с близкими лицами – его психологическом состоянии, совершаемых действиях и попытках связаться с преступников повторно. В качестве примера отражения результатов данных следственных действий можно привести апелляционное определение Ульяновского городского суда по делу № 22-937/2018, в котором в качестве доказательств факта совершения мошенничества были приведены результаты допроса близких лиц потерпевших².

Проверка сведений, связанных с совершением мошенничества допускает проведение оперативно-розыскной работы ответственным органом. Главная цель – это поиск и анализ фактов, которые имеют значение для расследования или могут быть использованы в качестве доказательств в процессе судопроизводства.

Большое значение в процессе предупреждения кибермошенничества имеет деятельность кредитных организаций. В связи с этим на всех этапах необходимо обеспечивать сотрудничество правоохранительных органов и кредитных организаций. Например, правоохранительные органы могут направлять запросы в банки для проверки факта мошенничества, принадлежности счета получателя.

Аналогичное можно отметить и в отношении операторов сотовой связи. Взаимодействие субъектов в данном случае может быть связано с

¹Бадзгардзе Г.Б. Особенности возбуждения уголовного дела о мошенничестве, совершенном с использованием информационных технологий // КриминалистЪ. 2023. N3. С.3-10.

²Апелляционное определение Ульяновского городского суда по делу № 22-937/2018. URL: <http://www.ulobsud.ru/index.php?option=3&id=90&idCard=73288> (Дата обращения 24.03.2026)

блокированием номеров, осуществляющих массовые обзвоны, проверкой подозрительных номеров, а также получением информации о номере, по которому осуществлялось взаимодействия мошенника и жертвы¹.

Отдельное направление деятельности по проверки факта мошенничества – это истребование справок и документации от заявителя и учреждений, о движении средств по счету, выписок и справок по операции, разъяснений о совершении отдельных операций. Для сокращения времени проверки могут потребоваться и дополнительные документы – справки, выписки со счета, чеки, если мошенничество совершено с использованием безналичной формы перевода².

В.А. Егоров говорит, что в целом процесс доказывания факта мошенничества включает целую совокупность следственных действий – допрос потерпевшего и свидетелей, проведение обысков, выемки и осмотра технических средств, документов, а также получение разрешений на получение сведений от операторов сотовой связи, осмотр устройств самообслуживания³.

Так, выемка – это одно из наиболее распространенных следственных действий, порядок проведения которой определен нормами ст. 183 УПК РФ. Суть данного следственного действия заключается в изъятии документов и предметов, которые имеют определенное значение для установления ситуации, доказательства виновности мошенника. В частности, дознавателю необходимо совершить выемку информации о вкладах и счетах граждан в

¹Голятина С.М. Методика расследования хищений электронных денежных средств : специальность 12.00.12 «Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность» : автореф. ... дис. канд. юрид. наук / Голятина Светлана Михайловна. Волгоград, 2022. С.17

²Методические рекомендации "Расследование мошенничеств, связанных с реализацией товаров и оказанием услуг в сети Интернет". URL: https://49.xn--b1aew.xn--plai/citizen/Razjasnenija_MVD_Rossii (Дата обращения 24.03.2026)

³Егоров В.А. Криминалистическое обеспечение организации расследования мошенничества, совершенного с использованием средств связи // Юридическая наука и правоохранительная практика. 2017. N 2(40). С. 175 – 176.

банках и иных кредитных организациях согласно порядку норм, ст. 182, 183 и ч.1 ст. 165 УПК РФ.

После получения информации относительно способа перечисления денежных средств, необходимо также установить компанию-провайдер, предоставившую IP-адрес в точное время, в течение которого был совершен факт мошенничества. С этой целью дознаватель направляет поручение для получения информации о провайдерах, MAC-адресе устройства для получения IP-адреса и месте нахождения абонента, информации о нем.

В случае, если перечисление денежных средств мошеннику осуществлялось через мобильный банк, то направляется запрос оператору связи и в кредитную организацию для установления информации об абоненте, а также о соединениях между абонентами.

Если перевод осуществлялся по номеру карты или счета, дознавателю необходимо проверить информацию о месте его открытия, месте обналичивания денежных средств, запросить видеозаписи с камер видеонаблюдения, установленных в банкомате.

После получения ответа от компании-провайдера требуется провести обыск в указанном помещении на основании судебного решения. Порядок проведения обыска определен в ст. 182 УПК РФ¹. Осмотр жилища предназначен для определения обстоятельств, имеющих значение для расследования (ст.176 УПК РФ). Порядок данного следственного действия определен в ст.177 УПК РФ. Так, например, при выявлении имеющего значение предмета осуществляется его выемка.

В качестве предметов, имеющих значение для расследования уголовных дел о мошенничестве, совершенном с использованием сети Интернет, могут являться, например, мобильные средства связи или компьютер, с помощью которого совершалось преступление. В этом случае

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 13.12.2024) // Собрание законодательства Российской Федерации. 2001. N 52. Ст. 4921

необходимо для осмотра изъятого предмета привлекать специалистов по компьютерным технологиям.

Информация, получаемая от оператора мобильной связи, также имеет большое значение для расследования уголовного дела, предупреждения мошенничества, совершенного с использованием сети Интернет. В случае необходимости сотрудники органов дознания могут запрашивать документацию о соединениях абонента, которые затем осматриваются с участием специалиста. Аналогичное можно отметить и в отношении сведений от банков¹. Соответственно, для предупреждения распространения мошенничества в сети Интернет важным условием является развитие взаимодействия между правоохранительными органами, операторами сотовой связи и банками.

Таким образом, выявление и предупреждение мошенничества с использованием сети Интернет осуществляется преимущественно правоохранительными органами, одним из которых является полиция. Задачи и направления работы полиции в рамках выявления и раскрытия мошенничества, совершенного с использованием сети Интернет, определены в Законе о полиции и включают не только проведение оперативно-розыскной работы, но и информационно-профилактической работы с населением для предотвращения роста случаев мошенничества.

При получении сообщения от заявителя о мошенничестве, дознавателем осуществляется проверка информации, доказывающей то, что данный факт действительно был – уточняется информация у заявителя, запрашиваются документы у заявителя, а также у организаций и учреждений. Процесс доказывания факта мошенничества включает разнообразные следственные действия, главная задача которых – это

¹ Методические рекомендации "Расследование мошенничеств, связанных с реализацией товаров и оказанием услуг в сети Интернет". URL: https://49.xn--b1aew.xn--plai/citizen/Razjasnenija_MVD_Rossii (Дата обращения 24.03.2026)

обнаружение предметов и документов, доказывающих факт совершения мошенничества и виновность мошенника.

1.2. Отграничение мошенничества, совершенного с использованием сети Интернет от "традиционного" мошенничества

Нормы, регулирующие уголовную ответственность за совершение мошенничества, расположены в главе 21 УК РФ «Преступления против собственности»¹. Именно данное положение в структуре уголовного закона, по мнению многих авторов, указывает на то, что непосредственным объектом мошенничества являются отношения собственности.

Тем не менее, некоторые авторы говорят о том, что подобный подход к определению объекта мошенничества представляется слишком узким. Например, в соответствии с одной из точек зрения, объектом мошенничества являются имущественные отношения, а также отношения собственности². Основанием для данной точки зрения является тот момент, что в комментариях к статье 158 УК РФ указано, что хищение может причинять вред не только собственнику, но и иным владельцам имущества. В целом, данный подход представляется логичным, однако, любое мошенничество в конечном счете в той или иной мере связано с причинением вреда праву собственности. Кроме того, ст.158 УК РФ и ст.159 УК РФ закрепляют смежные составы преступления, в связи с чем представляется не совсем оправданным применять положения одной статьи для раскрытия состава мошенничества.

В связи с этим, стоит согласиться с мнением авторов, указывающих на четырехступенчатую структуру объектов преступления. Так, в соответствии с данным подходом, следует выделять следующие объект мошенничества:

¹ Уголовный кодекс Российской Федерации (УК РФ) от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. N 25. Ст. 2954.

² Тамазов И.В. Объект и предмет мошенничества // Современное право. 2010. N12. С.129

1) видовым объектом мошенничества является «совокупность общественных отношений собственности, неприкосновенность которых также охраняется уголовным законом»;

2) родовым объектом выступает «экономические отношения, охраняемые уголовным законом, что явствует из названия раздела VIII УК РФ – «Преступления в сфере экономики»»;

3) непосредственным объектом – «общественные отношения конкретно чужой собственности»¹.

Соответственно, учитывая то, что мошеннические действия, направленные против чужой собственности, фактически несут угрозу праву собственности субъекта, подлежащему правовой охране, в качестве непосредственного объекта следует выделить общественные отношения в сфере охраны права собственности.

Отдельно также необходимо рассмотреть предмет мошенничества, поскольку его характеристика позволяет указать, на что именно обращено преступное посягательство виновного лица. Предметом преступного посягательства мошенничества являются, как правило, денежные средства или иное имущество жертвы.

Объект и предмет отличают мошенничество с использованием сети Интернет от традиционного. В обоих случаях объект — отношения собственности. Предмет — чужое имущество или право на него. Однако в интернет-мошенничестве дополнительным объектом могут выступать отношения, обеспечивающие информационную безопасность, а предметом — компьютерная информация, которая используется для хищения.

Характеризуя объективную сторону мошенничества следует указать на то, что оно представляет собой противоправное деяние, заключающееся в

¹ Упоров И.В, Бондарь А.В. Объект и предмет преступного посягательства на собственность в виде мошенничества: теоретические положения и законодательное закрепление // Современная юриспруденция: актуальные вопросы, достижения и инновации: сборник статей V Международной научно-практической конференции. 2018. С.272

изъятии чужого имущества в пользу виновного. Определенную ясность в характеристике объективной стороны преступления вносит Постановление Пленума ВС РФ № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором Суд указал, что мошеннические действия совершаются с «целью безвозмездного обращения в свою пользу или в пользу третьих лиц чужого имущества или приобретения права на него»¹.

По мнению Е.А. Хариной выделяют два вида мошенничества – контактное и бесконтактное². Контактное и бесконтактное мошенничество с использованием интернета — это два разных подхода к обману жертв, которые различаются степенью взаимодействия злоумышленника и жертвы. Контактное мошенничество (ст.159 УК РФ) предполагает непосредственное личное общение злоумышленника с жертвой, хотя часть взаимодействия может происходить через интернет. Например, мошенники могут сначала связаться с жертвой по телефону или в мессенджере, а затем договориться о личной встрече для завершения «сделки» или получения денег. Бесконтактное мошенничество (ст.159.6 УК РФ) происходит полностью удалённо — через интернет, телефонную связь, мессенджеры. Жертва не видит преступника лично.

Статья 159 УК РФ закрепляет две основных формы, в которых может быть совершено мошенничество: хищение и приобретение права на чужое имущество путем обмана или злоупотребления доверием. При этом между собой данные формы являются взаимоисключающими, но независимо от этого преследуют одинаковую цель – передача чужого имущества или прав на него в пользу виновного лица.

При этом некоторые исследователи говорят о том, что злоупотребление доверием как самостоятельный способ совершения мошенничества является

¹ Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате" (Утратил силу) // Справочно-правовая система Консультант-Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_74060/ (Дата обращения 24.03.2026)

²Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации:дисс. ...канд.юрид.наук. Красноярск, 2024. 248 с.

сомнительным, поскольку оно по сути может рассматриваться как один из аспектов обмана¹. При этом большинство исследователей все-таки говорит о необходимости выделения в качестве способа совершения мошенничества не только обман, но и злоупотребление мошенничеством.

Способ совершения мошенничества также является критерием, отграничивающим мошенничество с использованием сети Интернет от традиционного. Традиционное мошенничество предполагает непосредственное взаимодействие с потерпевшим, где злоумышленник использует обман или злоупотребление доверием для того, чтобы жертва добровольно передала имущество или права на него. Например, это может быть личное общение, письменное обращение или телефонный разговор, где потерпевший осознанно совершает действия в пользу мошенника.

Интернет-мошенничество использует компьютерные технологии и информационно-телекоммуникационные сети для достижения цели. Здесь применяются методы, связанные с манипуляциями компьютерной информацией: фишинг (создание поддельных сайтов или писем для кражи данных), использование вредоносного ПО, брутфорс (подбор паролей), социальная инженерия через онлайн-каналы (мессенджеры, соцсети). При этом непосредственного личного контакта с жертвой может не быть.

Соответственно, отграничение может быть проведено и на основании инструментов и технологий совершения преступных действий. Традиционное мошенничество опирается на личные навыки злоумышленника: умение убеждать, манипулировать, использовать поддельные документы или иные способы обмана в офлайн-пространстве.

Интернет-мошенничество задействует цифровые инструменты: электронные письма, поддельные сайты, мессенджеры, социальные сети, онлайн-платформы (например, сайты объявлений), криптовалюты, цифровые кошельки и т. д. Это позволяет масштабировать преступные схемы и действовать на расстоянии.

¹Шиян В.И. Уголовное право (особенная часть). Учебное пособие. М., 2009. 411 с.

Состав мошенничества дифференцирован в зависимости от способа совершения и вида мошенничества. С этой целью законодатель разграничил уголовно-правовые нормы, характеризующие его на несколько статей (ст.159-159.6 УК РФ). Состав мошенничества в целом определен в ст.159 УК РФ, закрепляющей общий состав, а также ряд квалифицирующих признаков.

Мошенничество, совершенное с использованием сети Интернет, также имеет квалифицирующие признаки, которые определены в ст.159.6 УК РФ. Так, в частях 2,3 и 4 определены следующие квалифицирующие признаки: совершенные группой лиц по предварительному сговору или с причинением значительного ущерба, совершенные лицом с использованием служебного положения, совершенные в крупном размере, совершенные в отношении электронных денежных средств или безналично, совершенные организованной группой в крупном размере. Данные признаки не всегда достаточно четко урегулированы в УК РФ. Например, действующая редакция УК РФ не содержит указание на то, какими именно характеристиками обладает группа лиц по предварительному сговору при совершении мошенничества. Опираясь на нормы ст.35 УК РФ, можно выделить следующие черты: наличие двух или более исполнителей преступления, а также наличие предварительного сговора.

Определенную ясность в данный вопрос вносит ВС РФ, определяющий, что на предварительный сговор указывает совместность действий двух и более лиц, а также наличие у всех участников умысла совершения преступления¹. А.В. Шеслер говорит о том, что предварительный сговор влечет возникновение субъективной связи между соучастниками².

Соответственно, главный признак предварительного сговора – это наличие сговора о совершении преступления между преступниками. При

¹ Постановление Пленума Верховного Суда РФ от 27.01.1999 N 1 (ред. от 03.03.2015) "О судебной практике по делам об убийстве (ст. 105 УК РФ)" // Справочно-правовая система Консультант-Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_21893/ (Дата обращения 24.03.2026)

²Шеслер А.В. Соучастие в преступлении: монография. Новокузнецк, 2014. 84 с.

этом на этапе сговора степень согласованности поведения еще очень низка, поскольку они только обсуждают возможность совершения преступления, но отдельные детали – место, время и способ совершения преступления конкретизируют на примитивном уровне¹. Тем не менее сам факт наличия сговора между преступниками уже говорит о повышении общественной опасности преступных действий группы. Повышенная общественная опасность определяет более строгие меры ответственности субъекта.

Понятие «организованная группа» представлено в ст.35 УК РФ, указывающей, что организованная группа характеризуется устойчивостью, а также предварительным объединением группы лиц, а также целью – совместное совершение преступления.

Еще более опасным является мошенничество, квалифицированное по ч.4 ст.159.6 УК РФ, поскольку подразумевает совершение бесконтактного мошенничества организованной группой лиц в крупном размере. Более высокая общественная опасность определена организованностью группы – ее устойчивостью, планированием преступлений, а также более серьезные общественно-опасными последствиями – причинением крупного материального ущерба пострадавшему.

В качестве примера можно привести Приговор Октябрьского районного суда города Новороссийска № 1-159/2019 1-4/2020 от 21 февраля 2020 г. по делу № 1-159/2019, вынесенный в отношении трех обвиняемых. При вынесении решения и определении необходимости применения квалифицирующих признаков ч.4 ст.159 УК РФ суд опирался на факт того, что обвиняемые предварительно распределили между собой в совершении преступления².

¹Козлов А.П. Соучастие: традиции и реальность. СПб., 2001. С.245

² Приговор № 1-159/2019 1-4/2020 от 21 февраля 2020 г. по делу № 1-159/2019. URL: <https://sudact.ru/regular/doc/mzqRYkys7bg8/> (Дата обращения 24.03.2026)

В качестве дополнительных квалифицирующих признаков в ч.4 ст.159 УК РФ определяет: особо крупный ущерб и лишение гражданина право на жилье.

Мошенничество, совершенное с использованием сети Интернет, содержит только один из выделенных признаков – это особо крупный размер. При этом под особо крупным размером понимается ущерб в размере, превышающем - один миллион рублей.

Более высокий уровень общественной опасности влечет более строгую уголовную ответственность. Так за совершение мошенничества с использованием сети Интернет организованной группой в крупном размере предусмотрено лишение свободы со штрафом и ограничением свободы. Вместе с тем, за остальные составы предусмотрены наказания в виде штрафа, исправительных или принудительных работ. Лишение свободы предусмотрено также и за мошенничество, совершенное с использованием служебного помещения (ч.3 ст.159.6 УК РФ), однако, его продолжительность короче.

Необходимость установления более строгого наказания за совершение мошенничества с использованием служебного положения определена тем, что мошенник не просто незаконно получает чужое имущество и права на него, но и использует для этого свое служебное положение – полномочия, предоставленные ему законодательством или иными документами, с целью обеспечения интересов государства или организации¹.

Законодатель в данной норме особо выделил тот момент, что мошенник в данном случае не просо совершает мошеннические действия для завладения чужим имуществом, но и использует для этого свои служебные полномочия.

¹ Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате" // Справочно-правовая система Консультант-Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (Дата обращения 24.03.2026)

Соответственно, должностное лицо характеризуется тем, что оно занимает определенную должность в выделенном законом перечне организаций. Важная особенность в том, что в деятельности данных юридических лиц выражаются интересы государства, субъектов или муниципалитетов. Это означает, что совершение должностного преступления напрямую вредит интересам государства.

При закреплении признаков рассматриваемого преступления, представляется логичным опираться на следующий взгляд в выделении признаков преступления, предусмотренного ч.3 ст.159 УК РФ: существенное условие, делающее совершение преступления возможным – это занимаемое должностное положение лица, действия виновных лиц противоречат интересам службы, наносят ущерб нормальному функционированию государственного или общественного аппарата¹.

Например, в приговоре Ясногорского районного суда Тульской области № 1-11/2020 от 9 октября 2020 г. в отношении ФИО, обвиняемой в совершении мошенничества с использованием служебных полномочий, обвиняемая совершила мошеннические действия с использованием своих служебных полномочий – председателя правления ТСН. Используя свои служебные полномочия председателя и введя в обман ряд лиц нанесла ущерб муниципальному образованию в размере рыночной стоимости земельного участка².

Квалифицирующие признаки, установленные в ч.3 ст.159.6 УК РФ определяет меры уголовной ответственности в отношении лиц, совершивших мошенничество с использованием служебного положения, в особо крупном размере. В качестве характерных признаков данного преступления следует выделить: занимаемое должностное положение лица, действия виновных лиц

¹ Птичкина Т.Д. Основные понятия и сущность должностных преступлений // Вестник экономики, управления и права. 2018. N1. С.70-75

² Приговор № 1-11/2020 от 9 октября 2020 г. по делу № 1-11/2020. URL: <https://sudact.ru/regular/doc/GkTlgDtAqalY/> (Дата обращения 24.03.2026)

противоречат интересам службы, наносят ущерб нормальному функционированию государственного или общественного аппарата.

Наказаниями, предусмотренными за совершение данного преступления, являются: штраф, принудительные работы, ограничение или лишение свободы.

Таким образом, мошенничество, совершенное с использованием сети Интернет, отличается от смежных составов, в первую очередь, по способу совершения преступления, который в обязательном порядке должен быть совершен с применением современных интернет-технологий. При этом данный вид мошенничества, как и остальные его виды, имеет квалифицирующие признаки, закрепленные в УК РФ.

Данные признаки определены более высокой степенью общественной опасностью. В связи с этим в этом случае мошенник привлекается к более строгим мерам уголовной ответственности.

Глава 2. ИССЛЕДОВАНИЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

2.1. Типичные способы мошенничества, совершенного с использованием сети Интернет

Мошенничество, совершенное с использованием сети Интернет, подразумевает совершение мошеннических действий с использованием информационных технологий. Главная общая черта всех способов – это использование современных дистанционных технологий¹. Способ совершения преступления – это один из наиболее значимых аспектов криминалистической характеристики преступления. Мошенничество в целом отличается большим разнообразием способов совершения преступления. Анализ способов совершения мошенничества, совершенного с использованием сети Интернет позволило заключить о существовании двух категорий способов: путем непосредственного контакта преступника с жертвой, а также без такого взаимодействия.

Рассматривая группу способов совершения мошенничества без непосредственного взаимодействия преступника с жертвой, следует отметить, что преимущественно такие преступления квалифицируются по ст. 159.6 УК РФ.

Материалы судебной практики также отражают некоторые существующие, актуальные способы мошенничества, совершенного с использованием информационных технологий. В качестве примера можно привести приговор Минусинского городского суда Красноярского края № 1 - 523/2013, вынесенный гражданам, которые в группе лиц похищали средства со счетов компаний, посредством использования служебного положения – один соучастник предоставлял сведения на предполагаемых абонентов для заключения с ними абонентских договоров. В свою очередь, второй

¹ Яковлева Л. В. Современные способы совершения дистанционного мошенничества // Вестник Краснодарского университета МВД России. 2021. N4 (54). С. 78.

соучастник заключал с клиентами абонентские договоры, осуществлял регистрацию и активацию сим-карт с тарифным планом, предусматривающим кредитный лимит 3 тыс. руб., и передавал активированные сим-карты соучастнику, который осуществлял переводы с номера на номера¹.

Так, К.С. Латыпова выделяет следующие способы мошенничества в сфере компьютерной информации: использование платежных сервисов различных интернет-ресурсов, при осуществлении необходимых платежных операций с последующим обналичиванием денежных средств либо с приобретением различных товаров с использованием денежных средств со счета жертвы; взлом электронных кошельков с последующим хищением денежных средств, переводом на другие счета, оплата услуг либо товаров через электронные платежные системы².

Представляется, что данная классификация является узкой и не охватывает преимущественное большинство способов осуществления рассматриваемой преступной деятельности.

Наиболее полная классификация типичных способов мошенничества в сфере компьютерной информации представлена в диссертационном исследовании Е.А. Хариной³. Автор выделяет следующие способы: посредством осуществления неправомерного доступа к информационной инфраструктуре кредитной организации; посредством воздействия ВПО на компьютерные устройства клиентов кредитных организаций; посредством установления контроля за работой компьютерных устройств юридических лиц через предустановленное ВПО; посредством неправомерного внесения изменений в платежные поручения юридических лиц; посредством

¹ Дело № 1-523/2013, первая инстанция. URL: <https://actofact.ru/case-24RS0035-1-523-2013-2013-08-01-2-0/> (Дата обращения 24.03.2026)

²Латыпова К. С., Дымшеева С.Д. Криминалистическая характеристика мошенничества в сфере компьютерной информации // Молодой ученый. 2021. N45 (387). С. 82-83

³Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дисс. ... канд.юрид.наук. Красноярск, 2024. С. 47-67.

осуществления несанкционированного управления работой банкомата; посредством создания и использования «фишинговых» сайтов.

Рассматривая способы совершения мошенничества с использованием сети Интернет путем непосредственного общения преступника с жертвой стоит отметить, что в настоящее время все большее распространение получает мошенничество, совершаемое через мессенджеры взамен обычных звонков¹. Переход на данный вид взаимодействия с жертвой определен тем, что сотовые операторы обязаны блокировать номера, осуществляющие массовые обзвоны, для пресечения мошенничества. При этом операторы не имеют технической возможности для блокировки звонков, осуществляемых через интернет и мессенджеры.

Одним из направлений такого вида мошенничества является поиск жертвы через лиц, разместивших объявление о продаже на популярных сервисах. Как правило, подобные способы совершения мошенничества подразумевают совершение мошенничества в несколько этапов – общение с жертвой от лица покупателя, формирование и направление ссылки на совершение перевода, как в приговоре Савеловского районного суда города Москва по делу № 1-494/2022².

В 2023 г. появилась новая схема хищения денежных средств. Так, преступники от имени Росфинмониторинга РФ рассылают сообщения о мнимом изъятии средств со счета жертвы, в связи с нарушением законодательства о противодействии легализации преступных доходов в счет государства из-за подозрительной активности, а затем требуют оплатить «комиссию» для отмены операции³.

¹ Сычева А.В., Домовец С.С. О некоторых способах совершения дистанционных мошенничеств в современных условиях и методах их предупреждения // Юрист – Правоведъ. 2023. N2. С.174-181

² Дело № 1-494/2022. URL: <https://savelovskij.mos-gorsud.ru/rs/savelovskij> (Дата обращения 24.03.2026)

³ Сычева А.В., Домовец С.С. О некоторых способах совершения дистанционных мошенничеств в современных условиях и методах их предупреждения // Юрист – Правоведъ. 2023. N2. С.174-181

Одним из распространенных видов мошенничества, совершенного с использованием интернет-технологий является фишинг. Фишинг представляет собой рассылку поддельных писем или создание сайтов официальных государственных органов или учреждений, которые внешне не отличаются от настоящих. При переходе по ссылке из сообщения на фишинговый сайт жертва вводит логин и пароль или данные карты, после чего мошенник получает доступ к личным кабинетам жертвы.

Данный способ мошенничества обеспечивает формирование доверия жертвы за счет использования сайтов и логотипов полностью аналогичных крупным организациям, государственным органам. Например, в качестве примера можно привести Постановление Вахитовского районного суда г. Казани, вынесенного в отношении группы лиц, которые использовали для совершения мошенничества сайт, якобы предоставляющий услуги по покупке авиабилетов¹.

Актуальной схемой совершения мошенничества является также и размещение объявлений на сайтах поиска вакансий. Данная схема подразумевает общую основу – размещение объявления на сайте вакансий, при этом дальнейшие схемы могут отличаться: плата за трудоустройство, например, за обучение, выпуск зарплатной карты, оформление документов; кража персональных данных – мошенники запрашивают у соискателя копии документов, банковские реквизиты, которые затем могут использоваться в преступных целях мошенниками; вредоносные приложения и файлы, которые могут предоставлять удаленный доступ мошенникам или собирать персональные данные².

Схожие цели преследует также мошенничество с технической поддержкой, когда мошенники звонят жертвам, представляясь технической

¹ Постановление № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020. URL: <https://sudact.ru/regular/doc/ftR7s3xLHjHQ/> (Дата обращения 24.03.2026)

² Как не нарваться на мошенников при поиске работы. URL: <https://www.gazprombank.ru/pro-finance/safety/moshenniki-pri-poiske-raboty/> (Дата обращения 24.03.2026)

поддержкой банков, интернет-провайдеров или мобильных операторов. Данная схема также включает убеждение жертвы установить вредоносное программное обеспечение или предоставить удаленный доступ. Данные шаги жертвы приводят к краже личных данных, логинов и паролей жертвы.

Для упрощения формирования доверия и выстраивания отношений с жертвами могут также использоваться схемы, включающие кражу аккаунтов в социальных сетях и рассылку сообщений родственникам и друзьям с просьбой срочно перечислить денежные средства. Данная схема выстраивания контакта также отличается более простым уровнем выстраивания доверительных отношений с жертвой, что повышает вероятность достижения преступной цели мошенников.

Представленные способы совершения мошенничества с использованием сети Интернет позволяют выделить схему, элементы которой имеют свое отражение в преступной деятельности в зависимости от контактных или бесконтактных способов совершения мошенничества:

- подготовка. На данном этапе мошенники готовят соответствующие инструменты совершения преступления – создают поддельные сайты, письма, подбирают жертв, создают профили на сайтах вакансий, сайтах знакомств, сервисах объявлений, крадут аккаунты в социальных сетях, создают, приобретают вредоносное программное обеспечение и т.п.;

- выбор жертвы и возможное установление с ней контакта. Этот этап уже подразумевает взаимодействие мошенника и жертвы письменно или по телефону. Именно на данном этапе мошенники могут использовать разнообразные схемы: отправка письма со ссылкой или приложением, звонок от лица технической поддержки организации, размещение фишингового сайта, размещение объявления о вакансии, звонок с извещением о выигрыше в лотерее. Именно на этом этапе осуществляется формирование доверительных отношений с жертвой;

- создание срочности и эмоционального давления при контактном мошенничестве. Задача данного этапа – это заставить жертву сделать нужное

мошенникам действие прямо сейчас, не допустить обдумывание ситуации. Запрос личных данных, паролей, денег, побуждение установить приложение. Данный момент является конечной целью мошенника – получить деньги или персональные данные, которые затем могут быть использованы мошенниками в преступных целях;

– завершение контактной схемы осуществляется резко путем прерывания контакта. На данном этапе исчезает сайт, прерывается звонок или блокируется жертва.

В целом, все контактные способы совершения мошенничества с использованием сети Интернет предполагают прямое взаимодействие с жертвой, часто с использованием устных или письменных коммуникаций.

Первый вид – это звонки от «банковских сотрудников» или «правоохранительных органов». Мошенники звонят жертве, представляются сотрудниками банка, службы безопасности, полиции или прокуратуры и сообщают о якобы попытке несанкционированного списания средств с карты, оформлении кредита на имя жертвы или других проблемах. Цель — выманить конфиденциальные данные (ПИН-код, CVV-код, одноразовые пароли из SMS) или убедить перевести деньги на «безопасный счёт».

Второй пример – это сообщения в мессенджерах и соцсетях от имени знакомых. Злоумышленники взламывают аккаунт жертвы или её близкого и рассылают сообщения с просьбой срочно перевести деньги, например, «попал в беду», «сломался телефон». Иногда они анализируют переписку, чтобы сделать просьбу более убедительной.

Также в качестве примера можно привести мошенничество с технической поддержкой. Преступники звонят или пишут, представляясь сотрудниками служб технической поддержки (интернет-провайдеров, мобильных операторов или крупных ИТ-компаний), и сообщают о якобы обнаруженной проблеме или вирусе на устройстве жертвы. Они просят установить вредоносное программное обеспечение или предоставить

удалённый доступ к устройству, чтобы получить доступ к личным данным и финансам.

Последний способ – это просьбы о помощи от «родственников». В телефонном разговоре мошенники сообщают, что близкий человек жертвы попал в беду (например, в аварию или в тюрьму), и просят срочно перевести деньги для «выкупа» или «лечения».

Таким образом, мошенничество с использованием сети Интернет характеризуется высокой вариативностью способов совершения преступления. При этом представленный перечень способов совершения нельзя считать исчерпывающим, поскольку с развитием информационных технологий растет и число способов совершения преступления.

Мошенничество, совершенное с использованием сети Интернет – это использование цифровых технологий для обмана людей с целью получения денег, данных или других выгод. Злоумышленники применяют разнообразные схемы, часто сочетая несколько методов для повышения эффективности обмана. С распространением и развитием технологий искусственного интеллекта также распространяются и усложняются и схемы его совершения, при этом основой при контактном мошенничестве все же остается моральное давление и выстраивание доверительных отношений мошенника с жертвой.

2.2. Криминалистическая характеристика личности интернет-мошенника

Криминалистическая характеристика личности интернет-мошенника является одним из характеризующих признаков мошенничества, совершенного с использованием сети Интернет. Криминалистическая характеристика личности преступника представляет собой совокупность социально-демографических, психологических, профессиональных и других

признаков, которые помогают понять механизм преступления, выявить мотивы и особенности поведения злоумышленника¹.

Личностные особенности мошенников отличаются в зависимости от того, является ли мошенничество, совершенное с использованием сети Интернет, контактным или бесконтактным.

Характеристика личности бесконтактных мошенников достаточно подробно представлена в диссертации Е.А. Хариной. Автор делит мошенников данной группы на несколько категорий в зависимости от уровня обладания специальными познаниями:

- специалисты высокого уровня, эксперты в сфере ИТТ, которые характеризуются обширными и глубокими познаниями в данной сфере, разрабатывают программы и генерируют идеи для взлома информационных систем и получения данных. Данная категория мошенников характеризуется уверенностью и самоуверенностью, отсутствием сожалений об общественно-опасных последствиях преступных действий, избирательностью в выборе жертвы, соответственно, преступления в данном случае носят организованный характер;

- опытные преступники в сфере ИТТ – не являются сами разработчиками соответствующих компьютерных программ, однако с большой степенью активности и профессионализма занимаются их использованием, адаптируют программы под дальнейшее использование. При этом данная категория преступников не всецело погружены в данную деятельность и могут иметь основную легальную работу. Главная психологическая характеристика данной группы – это обладание высокой степенью неподдельного интереса к совершению компьютерных преступлений, избирательность жертвы не имеет значения;

- специалисты среднего уровня в сфере ИТТ. Характеризуются обладанием соответствующих познаний на уровне уверенных пользователей,

¹Латыпова К.С., Дымшеева С.Д. Криминалистическая характеристика мошенничества в сфере компьютерной информации. 2021. N45 (387). С. 82-83.

вовлеченность в преступную деятельность данной категории мошенников – бессистемна и носит характер хобби и фрагментарное видение ситуации. Отличительная психологическая особенность – это иллюзорное представление о достижении высоких результатов;

– «бытовые», «случайные» компьютерные преступники характеризуются обывательскими знаниями в сфере ИТТ. Осуществление преступной деятельности может начинаться с внезапно возникшего преступного умысла, совершения преступления, не требующего специальных знаний. Главная психологическая характеристика – это неуверенность в своих действиях и страх быть пойманным¹.

Главная черта контактного мошенничества – это опосредованный контакт мошенника с потерпевшим, который обеспечивается использованием средств связи. Учитывая удаленность и опосредованность взаимодействия мошенника с жертвой, преступники вынуждены использовать все возможные методы воздействия на жертву с учётом имеющейся у него информации о ней, убеждает её, что имеет возможность совершить те действия, которые ждёт от него жертва².

Кроме того, мошенники достаточно активно и оперативно подстраиваются под экономические, политические изменения, значимые события, проходящие в России и в мире. При совершении дистанционного мошенничества с использованием информационных технологий, мошенник не владеет достаточной информацией о личности жертвы, а соответственно ограничен в возможностях использования личного авторитета для воздействия на нее. В этом случае, зачастую, мошенники используют авторитет других лиц и организаций, например, представляясь следователем,

¹ Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дисс.канд.юрид.наук. Красноярск, 2024. – С.89-92.

² Ревенко Н.И. Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий // Вестник Омского университета. Серия «Право». 2024. N2. С.87-90

сотрудниками отдела безопасности банка или государственных учреждений¹.

Учитывая то, что время для взаимодействия мошенника и жертвы при данном виде мошенничества ограничено, достижение преступной цели осуществляется посредством искусственного создания ситуации ограничения по времени у жертвы, создавая эффект неожиданности. В этом случае приоритетное значение приобретают личностные свойства личности.

Криминологическая характеристика лица, совершившего мошенничество, отличается от преступников, совершивших иные тяжкие преступления. Характерная особенность лица, совершающего мошенничество – это умение расположить человека к себе и подстроиться под обстоятельства. Преступность женщин ниже преступности мужчин в 5 - 7 раз. Однако численность преступлений, совершенных женщинами, в последние годы растет. В среднем около 18% рассматриваемых составов совершается женщинами².

Мошенничество – это высокоинтеллектуальное преступление, в связи с чем его осуществление зависит от сноровки и ума преступника, его способности своими действиями (в случае с дистанционным мошенничеством – словами) заставить жертву передать имущество мошеннику. Это означает, что интернет-мошенник отличается аналитическим мышлением, а также способностями усваивать и обрабатывать новую информацию. Именно данные навыки позволяют интернет-мошенникам постоянно развивать и разрабатывать новые способы совершения мошенничества.

Кроме того, мошенничество – это преступление, которое требует планирования. А. В. Швец в своём исследовании утверждает, что в 70%

¹ Ревенко Н.И. Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий // Вестник Омского университета. Серия «Право». 2024. N2. С.87-90

²Чужмарова А.А, Криминологическая характеристика мошенничества // Научный журнал. URL: <https://cyberleninka.ru/article/n/kriminologicheskaya-harakteristika-moshennichestva-1> (Дата обращения 24.03.2026)

случаев у мошенников в течение одного месяца формировался умысел на совершение преступления, у 22% - до полугода¹.

Вместе с тем, следует также отметить, что мошенничество, совершаемое с использованием информационных и компьютерных технологий, зачастую совершается группой лиц. Например, в апелляционном определении по делу № 10-15408/2019 виновными в совершении преступления были признаны сразу 10 человек. Преступная группа совершала мошенничество посредством ввода, блокирования, модификации компьютерной информации в особо крупном размере².

Характеризуя личность мошенников, использующих информационные технологии для совершения преступления, следует отметить достаточно глубокие теоретические или практические познания в области психологии, поскольку только таким образом возможно осуществление влияния на жертву, стимулирование ее к совершению необходимых действий. Учитывая личностные особенности жертв, мошенники используют различные стратегии и приемы в зависимости от индивидуальных особенностей потенциальной жертвы, ее реакции на мошенника и передаваемую информацию.

Значимый вопрос, имеющий значение в уголовно-правовой и криминологической характеристике, связан с личностной характеристикой осужденных мошенников. Личность преступника – это система социально-биологических и психических свойств человека, оказывающих влияние на деятельность по раскрытию и расследованию преступлений³. Соответственно, личность преступника напрямую связана с эффективностью

¹ Швец А. В. Состояние и динамика мошенничеств, совершаемых женщинами // Российский следователь, 2014. № 9.

² Апелляционное определение по делу № 10-15408/2019 (приговор). URL: mos-gorsud.ru (Дата обращения 24.03.2026)

³Криминалистическое изучение личности: науч.-практ. пособие для магистров / А. Г. Бедризов, Т. С. Волчецкая, Н. В. Галяшин [и др.] ; отв. ред. Я. В. Комиссарова. М., 2016. 224 с.

расследования и выявления мошенничества в сфере компьютерной информации.

В качестве основных характеристик личности, осужденных за кибермошенничество следует выделить: пол и возраст, физические и психические характеристики, уровень образования, социальное и семейное положение, профессиональная принадлежность. Вместе с тем, не все из представленных данных могут быть проанализированы и выявлены тенденции на основании анализа материалов судебной практики. Например, в приговорах, размещаемых в свободном доступе, изъяты данные о дате рождения осужденного. Тем не менее, средний возраст осужденных может быть получен из доступных данных официальной статистики, где представлены обобщенные данные. Так, согласно данным официальной статистики органов прокуратуры, наибольшую часть преступлений совершают люди в возрасте от 30 до 49 лет¹.

Данное распределение во многом обусловлено особенностями совершения мошенничества в сфере компьютерной информации. В частности, для совершения данного вида мошенничества необходимы развитые навыки психологического влияния на жертву, а также эрудированности. Вместе с тем, граждане более старшего возраста реже осуждаются за совершение мошенничества с использованием информационных технологий, в связи с более низким уровнем информационной грамотности.

Гендерная принадлежность также является одной из характеристик личности осужденных за мошенничество в сфере компьютерной

¹ Прокуроры выяснили, кто чаще всего нарушает закон. URL: https://rg.ru/2018/02/01/prokurory-vyiasnili-kto-chashche-vsego-narushaetzakon.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (Дата обращения 24.03.2026)

информации. По данным статистики МВД, в 2024 году мужчины совершали преступления в 4 раза чаще, чем женщины¹.

Вместе с тем, проводимые социологические исследования указывают на то, что в настоящее время доля женщин, занятых в сфере компьютерной информации, составляет практически 30%². Это говорит о том, что женщины имеют доступ и возможности для совершения рассматриваемого преступления.

Вместе с тем, представляется, что подобное распределение в большей степени обусловлено отсутствием мотивации у женщин к совершению преступления нежели отсутствием необходимых навыков. В частности, данный вывод подтверждается тем, что в рассмотренных приговорах по ст.159.6 УК РФ, женщины-осужденные часто совершают преступление с использованием служебного положения.

В качестве примера можно привести приговор Анжеро-Судженского городского суда в отношении подозреваемой в мошенничестве в сфере компьютерной информации, совершенном ею с использованием своего служебного положения – на должности сотрудника офиса обслуживания оператора сотовой связи³.

Следующая характеристика – это физические данные. Следует отметить, что не все приговоры содержат указание на физические свойства осужденных. Тем не менее, из двадцати рассмотренных приговоров суда, вынесенных за совершение мошенничества в сфере компьютерной информации, отмечается, что практически в 60% рассмотренных приговоров в качестве смягчающей характеристики при назначении наказания

¹ Мужчины против женщин: кто больше нарушал закон в 2024 году. URL: <https://vc.ru/legal/1896615-statistika-prestupleniy-v-rossii-2024> (Дата обращения 24.03.2026)

²The Gender-Equal Cybercriminal Underground. URL: https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/gender-in-cybercrime?utm_source=Securitylab.ru (Дата обращения 24.03.2026)

³ Приговор № 1-481/2024 1-66/2025 от 22 января 2025 г. по делу № 1-481/2024. URL: <https://sudact.ru/regular/doc/ZpsnpfMDZ4HN/> (Дата обращения 24.03.2026)

выступают проблемы со здоровьем (у 7 человек указано на наличие заболевания).

Так, помимо наличия общих хронических заболеваний, у четырех осужденных отмечается также наличие инвалидности (20%) – по одному осужденному имеют инвалидность первой и второй группы, еще у двоих – инвалидность третьей группы.

Представленные данные статистики указывают на то, что более половины осужденных за мошенничество в сфере компьютерной информации имеют определенные заболевания. Данный вывод основан на результатах анализа судебных приговоров по ст.159.6 УК РФ.

Относительно психического состояния осужденных следует отметить 100% вменяемость, отсутствие каких-либо психических заболеваний. Это подтверждает вывод о том, что мошенники, использующие информационные технологии являются высокоинтеллектуальными личностями.

Характеризуя личность контактных мошенников, использующих информационные технологии для совершения преступления, следует отметить достаточно глубокие теоретические или практические познания в области психологии, поскольку только таким образом возможно осуществление влияния на жертву, стимулирование его к совершению необходимых действий. Учитывая личностные особенности жертв, мошенники используют различные стратегии и приемы в зависимости от индивидуальных особенностей потенциальной жертвы, ее реакции на мошенника и передаваемую информацию.

Относительно уровня образования и профессиональной деятельности, следует отметить, что не всегда данная информация указывается в приговоре. Из двадцати рассмотренных приговоров уровень образования указан только в шести приговорах. На основании анализа приговоров было получено следующее распределение: у двух осужденных – неполное среднее образование, у трех – среднее специальное образование, у одного – неоконченное высшее образование, у трех – высшее образование. Вместе с

тем, анализ профессиональной деятельности по другим делам позволяет предположить также наличие профильного образования у осужденных.

Так, в частности, следует отметить, что практически в 40% случаев кибермошенничество совершалось осужденным с использованием служебного положения (Рисунок 2.1).



Рисунок 2.1. Распределение осужденных по профессиональной принадлежности.

Представленные на диаграмме данные отражают отсутствие четкой тенденции в профессиональной принадлежности осужденных за совершение мошенничества в сфере компьютерной информации. Распределение в данном случае отражает то, что чуть менее половины осужденных имеют профессиональную деятельность. Однако, практически во всех случаях ведения профессиональной деятельности совершение преступления было сопряжено с использованием служебного положения.

Соответственно, статистика указывает на отсутствие прямой взаимосвязи между совершением кибермошенничества и наличием высшего образования в сфере интернет-технологий. Данный вид преступления может совершаться также и людьми, которые имеют определенный доступ к персональным данным, программному обеспечению. Навыки осужденных в сфере ИТ-технологий имеют второстепенное значение.

В связи с этим, всех осужденных за кибермошенничество можно условно разделить на четыре группы: лица, имеющие должность в коммерческой организации (главные бухгалтеры, руководители, директора);

лица, осуществляющие работу с клиентами в отделениях операторов мобильной связи и имеющие доступ к номеру, сим-карте жертв, мобильному банку; лица, занимающиеся иной деятельностью и исполняющие функции обналаживания похищенных средств для остальных соучастников; лица, создающие и распространяющие вредоносные сайты, программы и приложения, которые используются для совершения мошенничества в сфере компьютерной информации.

Чаще всего к ответственности привлекаются первые три группы преступников, последняя же группа выявляется реже всего. Среди рассмотренных примеров судебной практики и приговоров, вынесенных в отношении мошенников, последней группы не было, что говорит о достаточно редких случаях выявления и привлечения к уголовной ответственности создателей вредоносных программ – инструментов совершения кибермошенничества.

Во многом подобная практика обусловлена тем, что в последнем случае преступники практически не взаимодействуют с жертвами напрямую. Соответственно, при поиске и выявлении данных субъектов органы предварительного следствия сталкиваются с проблемами отсутствия информации о преступнике, его портрете и личности.

Также в приговорах не всегда уточняется и мотив преступника. Тем не менее, в рассмотренных приговорах зачастую очевидно прослеживается желание денежного обогащения – болезнь родственников или самого осужденного.

Отдельный интерес представляют также и взгляды исследователей на наличие или отсутствие взаимосвязи между мошенниками и пострадавшими. На основании данного критерия выделяют следующие группы интернет-

мошенников: лица, находящиеся с потерпевшим в деловых или трудовых отношениях; лица, не имеющие деловых связей с потерпевшим¹.

Таким образом, на основании проведенного анализа можно сделать вывод о том, что личность осужденного за мошенничество в сфере компьютерной информации достаточно сложно охарактеризовать собирательным образом. Во многом это обусловлено отсутствием ряда значимых социальных, физических и психических характеристик, осужденных в приговоре.

На основании анализа приговоров суда были выделены следующие характеристики личности осужденного за контактное мошенничество в сфере компьютерной информации:

- наиболее распространены преступления в среднем возрасте 30-49 лет;
- среди осужденных отсутствует привязка к уровню образования, наличию компьютерных навыков;
- среди осужденных высока доля лиц, имеющих различные заболевания;
- за мошенничество в сфере компьютерной информации чаще всего привлекаются лица, которые используют служебное положение для совершения преступления. Лица, создающие и распространяющие вредоносные программы, на данный момент практически не привлекаются к уголовной ответственности.

Бесконтактные мошенники отличаются следующими характеристиками:

- наличие определенных знаний в области ИТТ – наличие профильного образования, практических навыков, опыта работы с компьютерными технологиями. При слабом развитии данных навыков на первых этапах совершения преступления может возникать потребность и готовность развивать свои навыки в сфере ИТТ.

¹ Русаков И.М. Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг // Вестник Краснодарского университета МВД России. 2015. N4. С.206-208.

– мотивация чаще всего включает азарт и желание доказать свое превосходство, что определяет избирательность в выборе жертвы и организованный характер преступной деятельности (за исключением бытовых бесконтактных мошенников).

2.3. Криминалистическая характеристика жертвы мошенничества, совершенного с использованием сети Интернет

Жертвы мошенников, использующих информационные технологии, в настоящее время не ограничиваются пожилыми людьми, включает молодых людей и юридических лиц. По большей части, жертвами мошенников становятся также и экономически активные граждане всех возрастных групп. В общей сложности выделяют следующие категории жертв мошенников, использующих информационные технологии:

1) Доверчивые, характеризующиеся низкой критичностью к информации, обладающие повышенной тревожностью. В отношении данной категории жертв, как отмечает Р.А. Макаров мошенники осуществляют определенный процесс подготовки, на первом этапе которого мошенник входит в доверие, проявляя сочувствие, а затем предлагает решение проблемы, предполагающее срочное совершение определенных действий¹.

2) Жертвы, характеризующиеся склонностью к риску, необдуманном действиям, импульсивностью. В отношении данной категории жертв мошенники могут действовать несколькими способами: выигрыш в крупной лотерее, предложение вернуть деньги за некачественно оказанную услугу, защитить права, нарушенные действиями остальных участников гражданского оборота.

¹ Макаров Р. А. Личность пострадавшего как элемент криминалистической характеристики хищений, совершённых дистанционно с использованием информационно-телекоммуникационных технологий // Закон и право. 2021. N 11. С. 233.

Социально-демографические характеристики жертв мошенничества, совершенного с использованием сети Интернет, также являются достаточно показательными. Но данные характеристики в некоторой степени дифференцированы в зависимости от того, контактное или бесконтактное мошенничество были совершены.

В первую очередь, нужно отметить, что чаще всего жертвами контактных мошенников становятся женщины. Так, согласно портрету жертвы интернет-мошенника, доля женщин (55,5%) значительно превысила долю мужчин (44,4%)¹.

Подобное распределение обусловлено более высоким уровнем эмоциональности и чувства эмпатии, соответственно, являются более уязвимыми к манипуляциям мошенников.

В качестве дополнительных рисков, определяющих более частые случаи мошенничества, совершенного с использованием сети Интернет, в отношении женщин, можно выделить:

- использование мошенниками схем, рассчитанных на чувство страха женщин за близких (например, звонки «от родственников» с просьбой срочно помочь в опасной ситуации);
- финансовая самостоятельность современных женщин;
- стремление женщин отвечать на звонки с неизвестных номеров, чтобы быть на связи;
- повышенная уязвимость отдельных категорий женщин – матери-одиночки и бабушки, которые обладают повышенной тревожностью, одинокие женщины, которые могут стать жертвой схемы онлайн-знакомств, женщины пожилого возраста, которые менее уверены в цифровом пространстве и доверчивы.

¹ Банк России составил портрет пострадавшего от кибермошенников. URL: <https://cbr.ru/press/event/?id=18398> (Дата обращения 24.03.2026)

В свою очередь, мошенники используют ряд схем, которые ориентированы на женщин. Так, можно выделить следующие схемы, к которым восприимчивы женщины:

- звонки и сообщения, связанные с детьми;
- сообщения о срочной оплате доставки.

Возрастные особенности жертв контактного мошенника также достаточно часто становятся объектом статистических наблюдений. При этом статистика распределения жертв интернет-мошенников показывает, что чаще всего жертвами становятся люди старше 66 лет (Рисунок 2.2).

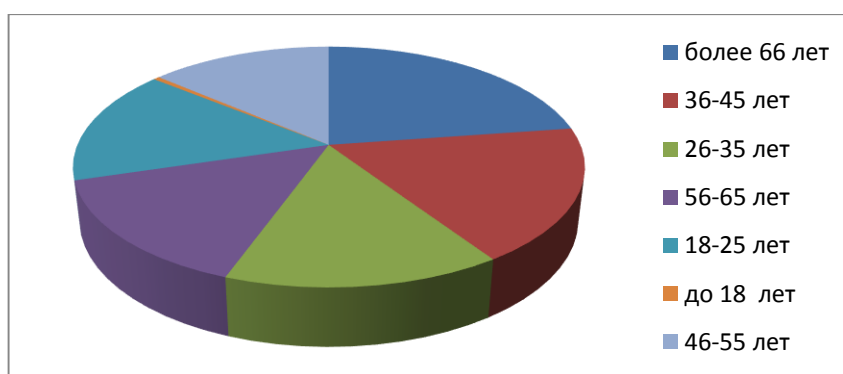


Рисунок 2.2. Распределение жертв интернет-мошенников по возрасту¹.

Представленная статистика представлена в разрезе города Москвы, тем не менее, ее данные, представляется, могут отражать общее распределение жертв интернет-мошенников по возрасту. Вполне логично, что люди в возрасте становятся жертвами мошенников чаще всего, что обусловлено следующими факторами: психологические и нейрофизиологические особенности (снижение когнитивных функций и способностей к критической оценке затрудняют распознавание обмана), высокий уровень доверчивости, социальная изоляция пожилых граждан и ограниченный круг общения, недостаток знаний и навыков в области работы с современными технологиями, физические ограничения (снижение слуха и проблемы со зрением) усложняют восприятие деталей в разговоре или сообщении,

¹ Женщины чаще мужчин становятся жертвами телефонных мошенников в Москве. URL: <http://ntv.ru/novosti/2868712/> (Дата обращения 24.03.2026)

эмоциональные и финансовые факторы, например, страх потерять имущество, потребность в медицинской помощи.

В свою очередь, мошенники используют схемы, которые в наибольшей степени соответствуют особенностям пожилых граждан – создание иллюзии срочности, угрозы негативными последствиями. Для создания ложной экспертности и формирования доверия мошенники могут представляться медиками, сотрудниками государственных органов.

Вместе с тем, работающие люди также зачастую становятся жертвами работающих людей. Выбор мошенниками данной категории обусловлен их финансовой независимостью, наличием платежных карт. В отношении данных возрастных категорий интернет-мошенники также используют схемы, направленные на создание иллюзии срочности, воздействие на эмоциональность.

Наименьшее же количество случаев мошенничества в представленной статистике зафиксировано в отношении несовершеннолетних лиц. Данная ситуация обусловлена финансовой зависимостью несовершеннолетних от законных представителей и отсутствием собственных доходов.

Портрет жертвы интернет-мошенника, составленный Банком России, в качестве социальной характеристики жертвы выделяет также и проживание в городе. Данная характеристика жертв мошенничества, совершенного с использованием сети Интернет, обусловлена следующими факторами:

- высокая плотность населения и экономическая активность, что определяет высокое число потенциальных жертв;
- активное использование цифровых сервисов жителями города, что упрощает возможность реализации схем интернет-мошенников;
- наличие технологических возможностей для массовых атак.

Например, существуют возможности для массовых обзвонов с использованием автоматизированных систем, программ для массовой рассылки сообщений. Более высокий охват населения увеличивает также и шансы успешного применения схем мошенников.

– психологические особенности жителей города: повышенный уровень стресса и эмоционального напряжения, доверчивость и склонность к импульсивным действиям, желание быстро решить проблемы, включая и дистанционными способами.

– социально-экономические факторы, включающие более высокий уровень доходов населения.

– более высокая активность населения в использовании онлайн-сервисов, большой цифровой след и повышенный риск утечки данных.

Также следует выделить и ряд психологических характеристик, определяющих повышенный риск стать жертвой мошенника. В качестве таких характеристик можно выделить: доверчивость и наивность, склонность верить другим людям без должной проверки и критической оценки ситуации, эмоциональная уязвимость – повышенные стресс и тревожность, финансовые трудности, которые снижают критичность восприятия, желание быстрого успеха или легкого заработка, определяющие более высокую привлекательность предложений с быстрым обогащением, страх упустить возможность, низкая самооценка, недостаток критического мышления, желание помочь другим¹.

При этом следует также выделить и некоторые поведенческие особенности. Так, например, стремление помочь другим может использоваться мошенниками путем убеждения отправить деньги или предоставить личные данные для помощи нуждающимся – детям, пожилым гражданам, бездомным животным.

Другой пример – это отсутствие осведомленности о киберугрозах, низкий уровень информирования о способах мошенничества, способах защиты в онлайн-среде. Подобная практика упрощает применение схем мошенничества, совершенного с использованием сети Интернет.

¹ Белодед Д.Р. Некоторые психологические особенности жертв преступлений, совершаемых с использованием цифровых технологий // Виктимология. 2023. N3. С.320-334

Кроме того, можно также отметить импульсивность и толерантность к риску. Так, склонность людей к принятию поспешных и необдуманных решений без предварительного обдумывания последствий также упрощает применение схем мошенничества.

Также в качестве поведенческой особенности жертв мошенничества, совершенного с использованием сети Интернет, выделяются также эвристическое мышление. Данное мышление характеризуется тем, что жертвы склонны принимать решения на основании жизненного опыта, эмоций, а не с позиций рационального анализа. Следует отметить, что определенным образом интернет-мошенники искусственно создают ситуацию стресса, ограниченности времени с целью лишить жертву возможности рационально осмыслить ситуацию и принять верное решение. Подобные действия мошенников приводят также и к тому, что жертва использует непродуктивные копинг-стратегии.

Рассматривая характеристику жертвы бесконтактного мошенничества, следует указать несколько основных черт, выделенных Е.А. Хариной. Во-первых, учитывая то, что бесконтактное мошенничество чаще всего является спланированным (за исключением бытовых преступлений) и выбор жертвы тщательно проводится преступником, жертвы характеризуются обладанием определенным имуществом, представляющим интерес для преступника.

Вторая черта – это обладание необходимыми средствами компьютерной информации, которые позволяют использовать бесконтактные способы совершения преступления – поддерживающие загрузку и установку вредоносного программного обеспечения.

Третья черта – это определенная степень самонадеянности, приводящая к небрежному отношению защиты информации, обеспечения надежности паролей, использования мер безопасности¹.

¹Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дисс.канд.юрид.наук. Красноярск, 2024. С.107-108.

Также, представляется логичным выделить следующие черты и характеристики, которые позволяют совершить бесконтактное мошенничество:

- Отсутствие специальных знаний в области IT или недостаточный уровень цифровой грамотности. Многие жертвы не обладают достаточными знаниями для распознавания фишинговых сайтов, вредоносных программ или мошеннических схем, связанных с компьютерными технологиями. Это делает их более уязвимыми для обмана.

- Использование цифровых сервисов и онлайн-транзакций. Потерпевшие часто являются пользователями интернет-банкинга, электронных кошельков, онлайн-магазинов, социальных сетей или других цифровых платформ. Это расширяет возможности злоумышленников для вмешательства в их финансовые операции или получения доступа к личным данным.

- Возрастные особенности. В группу риска могут входить как пожилые люди, которые менее знакомы с цифровыми технологиями, так и дети/подростки. Последние часто становятся жертвами из-за недостаточно развитого критического мышления, особенно в контексте онлайн-игр, где распространены схемы с предложением бесплатной валюты или бонусов в обмен на личные данные.

- Недостаточный уровень защиты информации. Если потерпевший не использует надёжные пароли, не обновляет антивирусное ПО, не проверяет подлинность сайтов или источников информации, это повышает вероятность стать жертвой мошенничества.

- Ситуация, требующая быстрого решения. Например, срочная необходимость перевести деньги, подтвердить доступ к аккаунту, «спасти» близкого человека (в случае взлома аккаунта знакомого в мессенджере). В таких случаях человек может действовать необдуманно, не проверяя информацию.

Таким образом, на основании исследования статистических данных можно сделать вывод о том, что типичные характеристики жертвы контактного мошенничества, совершенного с использованием сети Интернет, включают: финансовую самостоятельность, наличие источников постоянного дохода; наличие психологических и поведенческих особенностей, например, склонность к альтруизму, эмоциональная уязвимость, желание быстрого успеха, высокий уровень доверчивости, наиболее часто жертвами мошенников становятся городские жители, ввиду наличия инфраструктурных возможностей для большего охвата населения и более высокой плотности населения.

Жертвы бесконтактного мошенничества характеризуются несколькими основными чертами – обладание необходимым имуществом, наличие и активное использование необходимых средств связи, компьютерных и мобильных устройств, пренебрежение использованием средств защиты информации.

Криминалистическая характеристика жертвы помогает в расследовании преступлений, разработке профилактических мер и понимании механизмов вовлечения в мошеннические схемы. Учёт этих особенностей позволяет создавать целевые программы повышения цифровой грамотности и психологической устойчивости к манипуляциям.

2.4. Механизм мошенничества, совершенного с использованием сети Интернет

Представленные особенности жертв активно используются интернет-мошенниками для разработки схем. Так, в частности, мошенники используют психологические и поведенческие особенности при разработке схем мошенничества. При этом механизмы совершения мошенничества, совершенного с использованием сети Интернет, включают несколько

основных компонентов и отличаются для контактных и бесконтактных способов совершения мошенничества с использованием сети Интернет.

Первый обязательный компонент – это выбор жертвы и подбор вида мошенничества. Учитывая то, что мошенничество, совершенное с использованием сети Интернет, не подразумевает личного контакта мошенника и жертвы, преступники достаточно щепетильно относятся к подбору жертв, осуществляя целенаправленный поиск уязвимых людей. Для этих целей используются данные утечек, социальные сети, онлайн-площадки. Зачастую также мошенники предварительно осуществляют оценку уязвимости жертвы, например, направляют сообщения с предложениями поучаствовать в акции, с информацией о выигрыше.

Второй компонент механизма совершения контактного мошенничества, совершенного с использованием сети Интернет, – это искусственное создание доверия и паники, срочности решения вопроса. Для осуществления данных задач используются различные инструменты манипуляции, чтобы жертва утратила критическое мышление и действовала исходя из эмоционального состояния, а не рационального выбора.

Для создания доверия мошенники используют такие инструменты, как: использование авторитета государственных органов, использование персонализации и ложных знаний о личности жертвы, манипуляции недостатками знаний жертвы в правовой сфере, социальную инженерию, включающую манипулирование эмоциями, например, чувство вины, страх, использование взломанных аккаунтов.

Активно также интернет-мошенники используют и инструменты создания давления, ограничения принятия решения. Основные последствия подобных действий мошенников, на которые рассчитывают интернет-мошенники, включают следующие:

- возникновение психофизиологических реакций у жертвы – стресс, тревожность, паника;

- когнитивные изменения – снижение способности к принятию рациональных решений, критическому осмыслению ситуации;

- страх финансовых потерь, кражи личных данных, ущерба репутации.

Следующий компонент механизма совершения мошенничества, совершенного с использованием сети Интернет, – это технические инструменты. Данные инструменты готовятся мошенниками заранее. В качестве наиболее часто используемых можно выделить:

- фишинг – создание поддельных сайтов, массовой рассылки писем и сообщений якобы от официальных источников. После введения данных жертвой они попадают к мошенникам и используются в преступных целях;

- брутфорс также применяется интернет-мошенниками и представляет собой подбор паролей методом перебора символов. Данный метод может применяться для взлома аккаунтов, с которых затем осуществляются рассылки по списку контактов;

- создание и использование вредоносных программ, рассылка которых осуществляется посредством использования электронных писем, сообщений. Основная задача данных программ заключается в краже личных данных, блокировке системы и рассылке спама;

- зеркальные сайты реальных интернет-площадок также создаются и используются мошенниками для обмена жертв при покупке и продаже товаров;

- для контактного мошенничества также характерно получение доступа мошенников к данным путем запроса информации от жертвы под воздействием обмана. В данном случае жертва сама сообщает логины, пароли и данные карт, находясь под воздействием обмана. В некоторых случаях жертва также сама самостоятельно перечисляет деньги на указанные мошенниками реквизиты, находясь под воздействием обмана.

При этом в научной литературе встречаются различные взгляды на наиболее распространенные инструменты мошенничества.

Ярким примером способа совершения бесконтактного мошенничества с использованием сети Интернет является фишинг, который направлен не на получение денежных средств от жертвы напрямую, а на получение ее персональных данных, таких как пароля, логина, номера карт оплаты, ПИН-кода и др. Мошенники рассылают электронные письма от имени банков или платежных систем. Жертве предлагается зайти на сайт — копию настоящего, где под различным предлогом жертве предлагается ввести свои данные, которые затем используются для изготовления поддельной пластиковой карты и обналичивания денежных средств.

В качестве примера можно привести создание мошенниками более 700 поддельных доменов, предоставляющих услуги по покупке билетов на Олимпийские игры онлайн. Обслуживание осуществлялось на 12 языках, что увеличило охват жертв¹;

Так, например, в соответствии с одним из взглядов наиболее распространенными являются следующие способы контактного мошенничества, совершенного с использованием сети Интернет:

– нигерийские письма, суть которых в том, что житель развивающейся страны предлагает жителю более обеспеченной страны помочь ему вывести значительную сумму с территории своего государства под благовидным предлогом и обещает в случае успеха поделить полученные деньги. Данные финансы якобы некогда принадлежали высокопоставленным чиновникам, родственникам мошенника. Если получатель письма соглашается в участии, у него начинают вымогать сначала небольшие, но со временем все более возрастающие суммы, необходимые якобы для оформления документов, оплаты пошлин, сборов, взяток и т.п. После чего, естественно, мошенники исчезают;

– «казино». Жертве приходит письмо о наличии в коде конкретного Интернет казино ошибки или существовании беспроигрышной комбинации.

¹ Самые дерзкие фишинговые схемы 2024 года, которые сработали. URL: <https://habr.com/ru/companies/selectel/articles/867228/> (Дата обращения 24.03.2026)

Зачастую сами казино являются отправителями данных писем — таким образом они привлекают клиентов.

– просьбы о помощи и использование информации о различных бедствиях. Злоумышленники создают сайт-копию страницы благотворительной организации или детского дома, рассылают жертвам электронные письма, размещают просьбу о помощи в социальных сетях. Всем желающим помочь предлагается перечислить деньги на банковский счет или произвести оплату через систему «Веб-мани».

Ярким примером является случай мошенничества с просьбой перечисления средств на лечение ребенка от редкого заболевания, жертвой которого стал футболист ФК «Текстильщик». Началом мошеннической схемы стало личное сообщение жертве в социальных сетях с просьбой помочь собрать средства на лечение ребенка¹;

– построение бизнеса, связанное с предложением по созданию в сети Интернет собственного «бизнеса». Жертве предлагают купить описание секретной методики построения бизнеса, 100 % приносящей. Полученные от злоумышленника «чудо-методики», как правило, содержат информацию об организации бизнеса по той же схеме, которую реализуют преступники;

– интернет-магазины. Заказав и оплатив товар в данном магазине, пользователь либо его не получает вовсе, либо получает и оплачивает на почте пустую коробку;

– мошенничество, связанное с мобильной сотовой связью. Жертве предлагают отправить сообщение на короткий SMS-номер, либо ввести код, присланный на телефон жертвы мошенником. Как правило, стоимость отправки SMS-сообщения на номер мошенников намного выше той, которую они указывают. А в случае введения присланного мошенником кода происходит подписка телефона жертвы к платной рассылке;

¹ Новая схема. Как распознать аферу за сбором денег для больных детей. URL: <https://ria.ru/20220209/deti-1771694699.html> (Дата обращения 24.03.2026)

– «волшебные кошельки». Суть данного мошенничества заключается в том, что злоумышленники уверяют, что обнаружен «волшебный кошелек», после перечисления денег на который, они вернутся обратно жертве в увеличенном размере.

Несколько схожая схема подразумевает также звонки с информированием о выигрыше в лотерее, получении дивидендов. В качестве примера можно привести случаи использования злоумышленниками схемы с данными Росбанка. Злоумышленники представлялись сотрудниками Росбанка и сообщали о праве жертвы получить дивиденды от продажи природных ресурсов. Для получения данной выплаты необходимо открыть счет и внести на него определенную сумму¹;

– Free GSM. Мошенники предлагают жертве за небольшую сумму скачать на телефон программу, которая позволяет совершать бесплатные звонки, писать бесплатные СМС другим абонентам. На своем сайте мошенники подробно описывают приложение: с какими операторами оно работает, какие требования к системе телефона предъявляются, что вводит жертву в заблуждение о достоверности предлагаемого продукта. Однако после оплаты жертве приходит программа-пустышка².

Распространенной в настоящее время схемой контактного мошенничества, совершенного с использованием сети Интернет, также можно считать и шантаж с угрозами рассылки интимных фото, личных переписок. Для усиления угрозы мошенники также могут в переписке указывать персональные данные жертвы, усиливая тем самым чувством паники и тревожности жертвы³.

¹ Инвесторы обмана — 2. URL: <https://www.kommersant.ru/doc/8008859> (Дата обращения 24.03.2026)

² Михайленко И.А. К вопросу о способах мошенничества в сети Интернет // Сибирские уголовно-процессуальные и криминалистические чтения. URL: <https://cyberleninka.ru/article/n/k-voprosu-o-sposobah-moshennichestva-v-seti-internet> (Дата обращения 24.03.2026)

³ Хакеры освоили шантаж рассылкой интимных фото по списку контактов. URL: <https://www.vedomosti.ru/technology/articles/2023/12/28/1013347-hakeri-osvoili-shantazh-rassilkoj-intimnih-foto> (Дата обращения 24.03.2026)

Следующий компонент механизма совершения мошенничества, совершенного с использованием сети Интернет – это сокрытие следов. Данный этап является заключительным и реализуется для уклонения от уголовной ответственности и сохранения анонимности. С этой целью мошенники используют такие схемы, как: использование анонимных платежных систем, использование подставных лиц, включение в схему зарубежных сервисов, осложняющих запрос данных правоохранными органами, создание ложных следов, например, поддержание контакта с жертвой в течение некоторого времени после получения денег, использование чужих аккаунтов или аккаунтов-двойников, уничтожение материальных следов – удаление аккаунтов, использование криптовалют.

Также одним из элементов механизма совершения мошенничества является обман или злоупотребление доверием. Статья 159 УК РФ закрепляет две основные формы, в которых может быть совершено мошенничество: хищение и приобретение права на чужое имущество путем обмана или злоупотребления доверием. При этом между собой данные формы являются взаимоисключающими, но независимо от этого преследуют одинаковую цель – передача чужого имущества или прав на него в пользу виновного лица.

При этом некоторые исследователи говорят о том, что злоупотребление доверием как самостоятельный способ совершения мошенничества является сомнительным, поскольку оно по сути может рассматриваться как один из аспектов обмана¹. При этом большинство исследователей все-таки говорит о необходимости выделения в качестве способа совершения мошенничества не только обман, но и злоупотребление мошенничеством.

Таким образом, механизм совершения мошенничества, совершенного с использованием сети Интернет, представляет собой совокупность действий, которые используются мошенниками для обмана и злоупотребления

¹Шиян В.И. Уголовное право (особенная часть). Учебное пособие. М., 2009. 411 с.

доверием жертвы и подразумевают использование цифровых технологий. Основная цель механизма совершения мошенничества, совершенного с использованием сети Интернет – это хищение денежных средств или личных данных жертв. Ключевая особенность данного механизма мошенничества – это отсутствие прямого контакта мошенника и жертвы, повышающее анонимность злоумышленника.

Структурно механизм мошенничества, совершенного с использованием сети Интернет, включает: подготовку инструментов мошенничества: разработку фишинговых сайтов, взлом аккаунтов, создание аккаунтов-двойников, подготовку текстов сообщений; разработку способов обмана и злоупотребления доверием; установление контакта и доверительных отношений с жертвой: использование авторитета государственных органов и крупных организаций, создание интернет-магазинов, просьбы о помощи и благотворительности, фишинг, рассылка сообщений о выигрыше в лотерею; сокрытие следов преступления: использование анонимных аккаунтов и аккаунтов двойников, включение в схему зарубежных сервисов.

2.5. Типичные следы мошенничества, совершенного с использованием сети Интернет

Еще одна характеристика мошенничества, совершенного с использованием сети Интернет – это следообразование. Следообразование можно определить, как процесс возникновения следов – криминалистически значимой информации, которая может быть использована для раскрытия преступления и установления личности преступника.

При этом следообразование в случае мошенничества, совершенного с использованием сети Интернет, имеет ряд особенностей, которые обусловлены содержанием и особенностями механизмов и схем совершения мошенничества, совершенного с использованием сети Интернет. Так, следует учитывать следующие особенности:

- отсутствие физического контакта преступника и жертвы, а также осуществление взаимодействия с применением цифровых каналов общения – электронной почты, мессенджеров, телефонных звонков и сайтов;

- преобладание информационных следов, что определяет меньшую роль материальных следов, а также приоритетное значение цифровых следов. Соответственно, при расследовании случаев мошенничества, совершенного с использованием сети Интернет, особое значение имеют такие следы, как сетевые данные, метаданные;

- распределение следов по множеству объектов. Данная особенность следообразования мошенничества, совершенного с использованием сети Интернет, отличается особенностями сущности и характеристик цифровой информации – сохранение следов на системах компьютерного устройства, у интернет-провайдеров, в сетевых узлах, на серверах, в базах данных;

- цифровые следы требуют специальных технических средств фиксации. Это определяет, что поиск и разработка цифровых следов мошенничества, совершенного с использованием сети Интернет, требуют специальных технических средств, а также знаний для их обнаружения и изъятия.

Представленные особенности определяют, что цифровые следы мошенничества, совершенного с использованием сети Интернет, отличаются сложностью в выявлении и обработке, а также применении. Все это повышает значимость технических специалистов, компетентных в сфере информационных технологий. Кроме того, растет значимость взаимодействия правоохранительных органов и сотрудников банков, ИТ-специалистов.

Одной из классификаций является деление цифровых следов на виды в зависимости от их значения в расследовании. Например, на основании данного критерия выделяется три основных вида: следы, способствующие установлению личности преступника; следы, способствующие определению

местоположения преступника; следы, которые содержат информацию о свойствах личности преступника.

Также цифровые следы мошенничества, совершенного с использованием сети Интернет, можно разделить на два основных вида:

– активные следы, которые являются результатом сознательной деятельности мошенников в информационно-телекоммуникационном пространстве. В качестве примера данного вида можно выделить переписку мошенника с жертвой, комментарии, тексты рассылок.

– пассивные следы являются данными, которые были оставлены без участия мошенника, сохраняясь автоматически. Например, здесь можно выделить историю посещения сайтов, IP-адреса, данные о подключениях к сети.

Наиболее распространенные следы мошенничества, совершенного с использованием сети Интернет, представлены в Таблице 2.1..

Таблица 2.1. Криминалистически значимые следы мошенничества, совершенного с использованием сети Интернет.

Следы	Содержание
Данные о взаимодействии с интернет-провайдером	Информация о регистрации доменов, IP_адреса
Следы в системах банковского обслуживания	Сведения о переводах, электронных кошельках, привязке номеров телефонов к счетам и операциях по картам.
Метаданные	Информация о файлах и сообщениях – дата создания, автор, местоположение
Логи сетевых соединений	Данные о подключениях, доступе в интернет
Следы вредоносного программного обеспечения	Остатки кодов вирусов, отчеты антивирусных программ, зашифрованные файлы
Данные, сохраняющиеся в социальных сетях и мессенджерах	Привязки к электронной почте или номеру телефона, история переписок
Информация об использовании сим-карт	Данные об абонентах, соединениях по

	номеру, IMEI и IMSI
--	---------------------

Оба вида следов имеют криминалистическое значение, в связи с чем преступники стремятся к устранению и сокрытию данной информации. В случае с явными следами мошенники применяют автоудаляемые сообщения, удаляют переписку или же используют взломанные аккаунты для сохранения своей анонимности.

Соккрытие пассивных следов является более сложным, поскольку требует использования специальных программ, анонимных сетей. Например, для сокрытия IP-адресов злоумышленники могут использовать следующие способы:

- использование виртуальных частных сетей, создающих зашифрованное соединение между устройством пользователя и удаленным сервером, скрывающие реальный адрес и местоположение мошенника и сохраняющие лишь IP-адрес удаленного сервера;

- использование прокси-серверов в качестве посредников, перенаправляющих трафик через себя, в результате чего сайт видит только IP-адрес прокси-сервера, а не реального пользователя. Несмотря на то, то данный способ не шифрует трафик, местоположение мошенников все равно остается скрытым;

- использование анонимных сетей, маршрутизирующих интернет-трафик через сеть узлов для последовательного шифрования и перенаправления данных. Данная многоуровневость также осложняет отслеживание источника трафика;

- IP-спуфинг является технологий подмены IP-адреса, который также используется мошенниками для сокрытия своего местоположения и считывания системой безопасности источника трафика как надежного источника;

- антидетект-браузеры также позволяют создавать несколько виртуальных профилей, симулирующих уникальное устройство, тем самым

скрывая IP-адрес и изменяя цифровой отпечаток браузера, затрудняющие идентификацию устройства и отслеживание пользователя;

- динамические IP-адреса подразумевают автоматическое его изменение при каждом подключении к сети. Данная технология затрудняет отслеживание поскольку каждого перезапуска роутера или смены сессии;

- подключение к публичным сетям Wi-Fi также позволяет скрыть реальный IP-адрес мошенников, поскольку в качестве источника трафика демонстрирует адрес точки доступа¹.

Представленные способы указывают на то, что интернет-мошенники используют различные схемы сокрытия цифровых следов, в связи с чем необходимо совершенствовать оперативно-розыскную работу сотрудников полиции. Осмотр места происшествия осуществляется в соответствии со ст.176 УПК РФ, если были обнаружены следы преступления, выяснена обстановка происшествия и иные обстоятельства, имеющие значение для уголовного дела.

Следует отметить, что всего можно выделить два основных вида осмотра: осмотр места происшествия, то есть участка или помещения, в котором обнаружены следы совершенного преступления, а также осмотр места преступления, под которым понимается место непосредственного совершения преступления или наступления преступного результата².

Осмотр места нахождения следов или совершения преступления является неотложным следственным действием, которое проводится с целью установления, фиксации и изучения ситуации на месте происшествия, выявления следов преступления и виновных лиц, а также других фактических данных, позволяющих вкупе с доказательствами сделать

¹ Как хакеры остаются анонимными: обзор методов сокрытия личности в сети. URL: <https://www.securitylab.ru/blog/personal/Neurosinaps/354324.php?ref=123> (Дата обращения 24.03.2026)

²Казиахмедов М.Н. Роль осмотра места происшествия в раскрытии и расследовании преступлений // Проблемы совершенствования законодательства. 2019. С.48-50

выводы о ходе совершения преступления и других обстоятельствах события¹.

Так, в случае взаимодействия потерпевшего с мошенником (просмотра объявления, ответа на телефонный звонок) в занимаемом жилом помещении, следует произвести осмотр места происшествия: жилища, в котором располагаются компьютерные устройства, содержащие компьютерную информацию. Результаты осмотра должны быть отражены в протоколе осмотра. В частности, обязательно нужно отразить данные относительно расположения устройства, средств телекоммуникации, их соединения между собой, серийной информации, содержания рабочего стола.

В случае, если интернет-ресурс, с использованием которого совершены противоправные действия, продолжает функционировать на момент осмотра места происшествия, необходимо в протоколе указать представленную на сайте контактную информацию, род деятельности ресурса, наличие отзывов, приложить распечатки с интернет-сайта, экранную копию (снимок экрана) ресурса сети Интернет, на которой должны быть видны реквизиты - адресная строка страницы, идентификатор страницы и т.д.

В рамках осмотра места происшествия дознавателем с письменного согласия заявителя может быть произведен осмотр его мобильного телефона с целью закрепления следующей информации: IMEI телефонного аппарата, наличия SIM-карт с абонентскими номерами; информации, содержащейся в журнале вызовов мобильного устройства, в банке -сообщений, в записной книжке внутренней памяти мобильного устройства или SIM-карты; сохраненных текстов переписки между соответствующими абонентскими устройствами посредством SMS -сообщений или мессенджеров; истории посещения интернет-сайтов и др. Такой осмотр целесообразно производить с участием специалиста.

¹Россинская Е.Р. Криминалистика: Вопросы и ответы. URL: <https://www.konspekt.biz/index.php?text=40749> (Дата обращения 24.03.2026)

В рамках осмотра необходимо детально исследовать соответствующие разделы приложения "Мобильный банк" ("История платежей", "Последние операции" и пр.), в которых зафиксировано движение денежных средств по счету (банковской карте), сделать снимки экрана мобильного устройства, запечатлевающие данную информацию.

При осмотре жилого помещения заявителя возможно изъятие полученных им самостоятельно документов и сведений, относящихся к событию хищения: детализации входящих и исходящих соединений абонентского номера, по которому заявитель общался с подозреваемым лицом; выписки движения денежных средств по банковской карте (счету), с которого были переведены денежные средства; договор банковского счета (банковского обслуживания) и документов об оформлении банковской карты и др¹.

Эффективность работы правоохранительных органов по поиску и выявлению цифровых следов имеет большое значение, поскольку они позволяют решить целый ряд задач, а именно: идентификация личности преступника, восстановление хронологии событий, доказательство факта совершения мошенничества, доказательство виновности подозреваемого лица, выявление схемы совершения мошенничества, установление связи между различными элементами преступления, выявление соучастников и посредников.

При этом на следообразование влияют различные аспекты и факторы, которые включают, например, используемые технические средства, действия потерпевшего или способы совершения мошенничества, а также меры, которые предпринимал преступник для сокрытия следов преступления. Соответственно, эффективность поиска и выявления данных следов при расследовании зависит от опытности и профессионализма сотрудников правоохранительных органов, привлечении технических специалистов. Так,

¹ Методические рекомендации "Расследование мошенничеств, связанных с реализацией товаров и оказанием услуг в сети Интернет". URL: https://49.xn--b1aew.xn--plai/citizen/Razjasnenija_MVD_Rossii (Дата обращения 24.03.2026)

в частности, для работы с цифровыми следами зачастую необходима компьютерно-техническая экспертиза, позволяющая не только найти, но и расшифровать цифровые следы. Вместе с тем, даже несмотря на разработку и внедрение аналитических систем и специальных платформ, автоматизирующих анализ цифровых следов мошенничества, совершенного с использованием сети Интернет, сохраняется проблема быстрого устаревания технологий, использование мошенниками современных цифровых технологий – децентрализованных площадок, криптовалют, шифрования данных и международных транзакций.

Таким образом, следы мошенничества, совершенного с использованием сети Интернет, носят преимущественно цифровой характер, что отличает процессы их поиска и анализа. Наиболее яркими и значимыми следами мошенничества, совершенного с использованием сети Интернет, можно признать данные о взаимодействии с интернет-провайдером, об использовании сим-карт, сведения, сохраняющиеся в социальных сетях.

В связи с этим при расследовании случаев мошенничества, совершенного с использованием сети Интернет, необходимо проведение компьютерно-технической экспертизы, привлечение экспертов – ИТ-специалистов, сотрудников банков и мобильных операторов, интернет-провайдеров. Для повышения эффективности анализа цифровых следов государством разрабатываются специальные программы, однако, постоянно существует проблема устаревания используемых технологий и обновление схем и технологий, используемых мошенниками.

Заключение

В ходе проведенного исследования было установлено, что выявление и предупреждение мошенничества с использованием сети Интернет осуществляется преимущественно правоохранительными органами, одним из которых является полиция. Задачи и направления работы полиции в рамках выявления и раскрытия мошенничества, совершенного с использованием сети Интернет, определены в Законе о полиции и включают не только проведение оперативно-розыскной работы, но и информационно-профилактической работы с населением для предотвращения роста случаев мошенничества.

Мошенничество с использованием сети Интернет делится на два основных вида – контактное (ст.159 УК РФ) и бесконтактное (ст.159.6 УК РФ).

Мошенничество, совершенное с использованием сети Интернет, отличается от смежных составов, в первую очередь, по способу совершения преступления, который в обязательном порядке должен быть совершен с применением современных интернет-технологий. При этом данный вид мошенничества, как и остальные его виды, имеет квалифицирующие признаки, закрепленные в УК РФ. Данные признаки определены более высокой степенью общественной опасности. В связи с этим в этом случае мошенник привлекается к более строгим мерам уголовной ответственности.

Также было установлено, что мошенничество с использованием информационных и коммуникационных технологий характеризуется высокой вариативностью способов совершения преступления. При этом представленный перечень способов совершения нельзя считать исчерпывающим, поскольку с развитием информационных технологий растет и число способов совершения преступления.

Мошенничество, совершенное с использованием сети Интернет — это использование цифровых технологий для обмана людей с целью получения

денег, данных или других выгод. Злоумышленники применяют разнообразные схемы, часто сочетая несколько методов для повышения эффективности обмана. С распространением и развитием технологий искусственного интеллекта также распространяются и усложняются и схемы его совершения, но при этом основой все же остается моральное давление и выстраивание доверительных отношений мошенника с жертвой.

На основании проведенного анализа материалов судебной практики был сделан вывод о том, что личность осужденного за контактное мошенничество в сфере компьютерной информации достаточно сложно охарактеризовать собирательным образом. Во многом это обусловлено отсутствием ряда значимых социальных, физических и психических характеристик, осужденных в приговоре.

На основании анализа приговоров суда были выделены следующие характеристики личности осужденного за мошенничество в сфере компьютерной информации: наиболее распространены случаи совершения преступлений в среднем возрасте 30-49 лет; среди осужденных отсутствует привязка к уровню образования, наличию компьютерных навыков; среди осужденных высока доля лиц, имеющих различные заболевания; за мошенничество в сфере компьютерной информации чаще всего привлекаются лица, которые используют служебное положение для совершения преступления.

Бесконтактные мошенники отличаются следующими характеристиками: наличие определенных знаний в области ИТТ – наличие профильного образования, практических навыков, опыта работы с компьютерными технологиями. При слабом развитии данных навыков на первых этапах совершения преступления может возникать потребность и готовность развивать свои навыки в сфере ИТТ, а также мотивация чаще всего включает азарт и желание доказать свое превосходство, что определяет избирательность в выборе жертвы и организованный характер преступной деятельности.

Криминалистическая характеристика жертв мошенничества, совершенного с использованием сети Интернет, обусловлена необходимостью выявления особенностей жертв для повышения эффективности профилактической работы. На основании исследования статистических данных можно сделать вывод о том, что типичные характеристики жертвы мошенничества, совершенного с использованием сети Интернет, включают: финансовая самостоятельность, наличие источников постоянного дохода; наличие психологических и поведенческих особенностей, например, склонность к альтруизму, эмоциональная уязвимость, желание быстрого успеха, высокий уровень доверчивости; наиболее часто жертвами мошенников становятся городские жители, ввиду наличия инфраструктурных возможностей для большего охвата населения и более высокой плотности населения.

Жертвы бесконтактного мошенничества характеризуются несколькими основными чертами – обладание необходимым имуществом, наличие и активное использование необходимых средств связи, компьютерных и мобильных устройств, пренебрежение использованием средств защиты информации.

Криминалистическая характеристика жертвы помогает в расследовании преступлений, разработке профилактических мер и понимании механизмов вовлечения в мошеннические схемы. Учёт этих особенностей позволяет создавать целевые программы повышения цифровой грамотности и психологической устойчивости к манипуляциям.

Механизм совершения мошенничества, совершенного с использованием сети Интернет, представляет собой совокупность действий, которые используются мошенниками для обмана и злоупотребления доверием жертвы и подразумевают использование цифровых технологий.

Ключевая особенность данного механизма мошенничества – это отсутствие прямого контакта мошенника и жертвы, повышающее анонимность злоумышленника. Структурно механизм совершения

мошенничества, совершенного с использованием сети Интернет, включает: подготовку инструментов мошенничества: разработку фишинговых сайтов, взлом аккаунтов, создание аккаунтов-двойников, подготовку текстов сообщений; разработку способов обмана и злоупотребления доверием; установление контакта и доверительных отношений с жертвой; использование авторитета государственных органов и крупных организаций, создание интернет-магазинов, просьбы о помощи и благотворительности, фишинг, рассылка сообщений о выигрыше в лотерею; сокрытие следов преступления: использование анонимных аккаунтов и аккаунтов двойников, включение в схему зарубежных сервисов.

Следы мошенничества, совершенного с использованием сети Интернет, носят преимущественно цифровой характер, что отличает процессы их поиска и анализа. Наиболее яркими и значимыми следами мошенничества, совершенного с использованием сети Интернет, можно признать данные о взаимодействии с интернет-провайдером, об использовании сим-карт, сведения, сохраняющиеся в социальных сетях.

В связи с этим при расследовании случаев мошенничества, совершенного с использованием сети Интернет, необходимо проведение компьютерно-технической экспертизы, привлечение экспертов – ИТ-специалистов, сотрудников банков и мобильных операторов, интернет-провайдеров. Для повышения эффективности анализа цифровых следов государством разрабатываются специальные программы, однако, постоянно существует проблема устаревания используемых технологий и обновление схем и технологий, используемых мошенниками.

Список использованной литературы

Нормативные правовые акты и иные официальные документы

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 13.12.2024) // Собрание законодательства РФ. 1996. N 25. Ст. 2954
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 13.12.2024) // Собрание законодательства Российской Федерации. 2001. N 52. Ст. 4921.
3. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 29.12.2022) "Об оперативно-розыскной деятельности" // Собрание законодательства Российской Федерации. 1995. N 33. Ст. 3349.
4. Федеральный закон от 27.05.2003 №58-ФЗ «О системе государственной службы Российской Федерации» // Собрание законодательства Российской Федерации. 2003. N 22. Ст. 2063.
5. Федеральный закон от 07.02.2011 N 3-ФЗ (ред. от 28.11.2025) "О полиции" // Собрание законодательства Российской Федерации. 2011. N 7. Ст. 900.
6. Приказ МВД России N 776, Минобороны России N 703, ФСБ России N 509, ФСО России N 507, ФТС России N 1820, СВР России N 42, ФСИН России N 535, ФСКН России N 398, СК России N 68 от 27.09.2013 "Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд" (Зарегистрировано в Минюсте России 05.12.2013 N 30544) // Справочно-правовая система Консультант-Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_155629/ (Дата обращения 24.03.2026).
7. Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате"

(Утратил силу) // Справочно-правовая система Консультант-Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_74060/

8. Постановление Пленума Верховного Суда РФ от 27.01.1999 N 1 (ред. от 03.03.2015) "О судебной практике по делам об убийстве (ст. 105 УК РФ)" // Справочно-правовая система Консультант-Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_21893/.

9. Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате" // Справочно-правовая система Консультант-Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_283918/.

Монографии, учебники, учебные пособия

10. Валькова, Т. В. Расследование преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий [Электронный ресурс] : учебное пособие / Т В. Валькова, В.В. Долгаев, С.В. Смелова. – СПб : Санкт-Петербургский университет МВД России (СПб), 2021. – 131 с.

11. Дерюгин Р.А. Организация расследования хищений денежных средств, совершенных с применением ИТ-технологий [Электронный ресурс] : учебное пособие / Роман Александрович Дерюгин, Владислав Юрьевич Иванов, Иван Вадимович Мосин. – Екатеринбург : Уральский юридический институт МВД России (УрЮИ МВД России), 2025. – 71 с.

12. Деятельность органов внутренних дел по с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие : в 2 ч. Ч. 1 / Ю.В. Гаврилин [и др.]. М. : Академия управления МВД России, 2019. – 208 с.

13. Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учебное пособие / А.

А. Балашова [и др.] ; под редакцией Ю. В. Гаврилина, А. В. Победкина. – Москва : Академия управления МВД России, 2021. – 138 с.

14. Криминалистическое изучение личности : науч.-практ. пособие для магистров / А. Г. Бедризов, Т. С. Волчецкая, Н. В. Галяшин [и др.] ; отв. ред. Я. В. Комиссарова. М., 2016. – 224 с.

15. Козлов А.П. Соучастие: традиции и реальность. СПб., 2001. – 359 с.

16. Методические рекомендации "Расследование мошенничеств, связанных с реализацией товаров и оказанием услуг в сети Интернет".

17. Пидусов, Е.А. Особенности обнаружения и изъятия виртуальных следов при расследовании преступлений против собственности в сфере информационных технологий [Электронный ресурс] :методические рекомендации / Е.А. Пидусов [и др.] . – Воронеж : Воронежский институт МВД России (ВИ МВД России), 2022 . – 35 с.

18. Противодействие преступлениям в сфере информационных технологий : учебник / В.В. Гончар [и др.] . – 2-е изд., перераб. и доп . – М. : Главное управление по работе с личным составом МВД России(ГУРЛС МВД России), 2022 . – 232 с.

19. Процессуально-правовые основы расследования мошенничества (с применением информационно-телекоммуникационных технологий) [Электронный ресурс] : учебно-методическая рекомендация / Жыргалбек Токтоназарович Айдарбеков [и др.]. – Бишкек : Академия МВД Кыргызской Республики им. генерал-майора милиции Э.А. Алиева, 2025. – 14 с.

20. Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений [Электронный ресурс] : сборник статей. Вып. 11 / редкол. Сергей Владимирович Родин [и др.]. – Воронеж : Воронежский институт МВД России (ВИ МВД России), 2025. – 153 с.

21. Расследование преступлений в сфере компьютерной информации, совершаемых против собственности: учебное пособие / А.В.

Андреев [и др.]. – М. : Московский университет МВД России им. В.Я Кикотя (МосУ МВД России), 2020. – 185 с.

22. Старичков М.В. Тактика производства следственных действий при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий [Электронный ресурс] : учебное пособие / Максим Владимирович Старичков, Елена Игоревна Третьякова, Сергей Игоревич Усачев. – Москва : ГУРЛС МВД России, 2025. – 128 с.

23. Шеслер А.В. Соучастие в преступлении: монография. Новокузнецк, 2014. – 84 с

24. Шиян В.И. Уголовное право (особенная часть). Учебное пособие. Москва, 2009. – 411 с.

25. Южанинов, В.С. Противодействие преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий [Электронный ресурс] : учебное пособие / В.С. Южанинов, А.С. Студнев, М.С. Савченко . – Краснодар : Краснодарский университет МВД России(КрУ МВД России), 2024 . – 89 с.

Научные публикации и статьи в иных периодических изданиях

26. Бадзгарадзе Г.Б. Особенности возбуждения уголовного дела о мошенничестве, совершенном с использованием информационных технологий // КриминалистЪ. 2023. N3. С.3-10.

27. Белодед Д.Р. Некоторые психологические особенности жертв преступлений, совершаемых с использованием цифровых технологий // Викимнология. 2023. N3. С.320-334.

28. Голятина С. М. Методика расследования хищений электронных денежных средств: специальность 12.00.12 «Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность» : автореф. ...

дис. канд. юрид. наук / Голятина Светлана Михайловна. Волгоград, 2022. С.17.

29. Егоров В.А. Криминалистическое обеспечение организации расследования мошенничества, совершенного с использованием средств связи // Юридическая наука и правоохранительная практика. 2017. N2(40). С. 175 – 176.

30. Казиахмедов М.Н. Роль осмотра места происшествия в раскрытии и расследовании преступлений // Проблемы совершенствования законодательства. 2019. С.48-50.

31. Коломинов В.В. О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. URL: <https://cyberleninka.ru/article/n/o-sposobe-soversheniya-moshennichestva-v-sfere-kompyuternoy-informatsii/viewer>

32. Латыпова К.С., Дымшеева С.Д. Криминалистическая характеристика мошенничества в сфере компьютерной информации // Молодой ученый. 2021. N45 (387). С. 82-83.

33. Майкайлова Е.В. Кибермошенничество: виды, схемы, способы противодействия. URL: <https://school-science.ru/22/14/59552>.

34. Майтесян А.М. Мошенничество в сети интернет и способы защиты от него // Международный журнал гуманитарных и естественных наук. 2020. N5-4. С.69-72.

35. Макаров Р. А. Личность пострадавшего как элемент криминалистической характеристики хищений, совершённых дистанционно с использованием информационно-телекоммуникационных технологий // Закон и право. 2021. N11. С. 233.

36. Михайленко И.А. К вопросу о способах мошенничества в сети Интернет // Сибирские уголовно-процессуальные и криминалистические чтения. URL: <https://cyberleninka.ru/article/n/k-voprosu-o-sposobah-moshennichestva-v-seti-internet/viewer>

37. Назаров И. С. Проблемы борьбы с мошенничеством в сфере компьютерной информации // Молодой ученый. 2017. №40. С. 40-42.
38. Птичкина Т.Д. Основные понятия и сущность должностных преступлений // Вестник экономики, управления и права. 2018. №1. С. 70-75.
39. Ревенко Н.И. Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий // Вестник Омского университета. Серия «Право». 2024. N2. С. 87-90.
40. Русаков И.М. Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг // Вестник Краснодарского университета МВД России. 2015. N4. С. 206-208.
41. Сычева А.В., Домовец С.С. О некоторых способах совершения дистанционных мошенничеств в современных условиях и методах их предупреждения // Юристъ – Правоведъ. 2023. N2. С. 174-181.
42. Тамазов И.В. Объект и предмет мошенничества // Современное право. 2010. N12. С. 129.
43. Упоров И.В., Бондарь А.В. Объект и предмет преступного посягательства на собственность в виде мошенничества: теоретические положения и законодательное закрепление // Современная юриспруденция: актуальные вопросы, достижения и инновации: сборник статей V Международной научно-практической конференции. 2018. С. 272.
44. Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации : дис. ... канд. юрид. наук. Красноярск, 2024. 248 с.
45. Чужмарова А.А. Криминологическая характеристика мошенничества // Научный журнал. URL: <https://cyberleninka.ru/article/n/kriminologicheskaya-harakteristika-moshennichestva-1/viewer>

46. Швец А. В. Состояние и динамика мошенничеств, совершаемых женщинами // Российский следователь, 2014. N9. С. 40-45.

47. Яковлева Л. В. Современные способы совершения дистанционного мошенничества // Вестник Краснодарского университета МВД России. 2021. N4 (54). С. 78.

Интернет-ресурсы

48. Банк России составил портрет пострадавшего от кибермошенников. URL: <https://cbr.ru/press/event/?id=18398>.

49. Женщины чаще мужчин становятся жертвами телефонных мошенников в Москве. URL: <http://ntv.ru/novosti/2868712/>.

50. Инвесторы обмана — 2. URL: <https://www.kommersant.ru/doc/8008859>.

51. Как хакеры остаются анонимными: обзор методов скрытия личности в сети. URL: <https://www.securitylab.ru/blog/personal/Neurosinaps/354324.php?ref=123>.

52. Как не нарваться на мошенников при поиске работы. URL: <https://www.gazprombank.ru/pro-finance/safety/moshenniki-pri-poiske-raboty/>.

53. МВД: число киберпреступлений в России снизилось на 12% в 2025 году. URL: <https://www.kommersant.ru/doc/8442339>.

54. Новая схема. Как распознать аферу за сбором денег для больных детей. URL: <https://ria.ru/20220209/deti-1771694699.html>.

55. Прокуроры выяснили, кто чаще всего нарушает закон. URL: https://rg.ru/2018/02/01/prokurory-vyiasnili-kto-chashche-vsego-narushaet-zakon.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F.

56. Россинская Е.Р. Криминалистика: Вопросы и ответы. URL: <https://www.konspekt.biz/index.php?text=40749>.

57. Самые дерзкие фишинговые схемы 2024 года, которые сработали. URL: <https://habr.com/ru/companies/selectel/articles/867228/>.

58. Хакеры освоили шантаж рассылкой интимных фото по списку контактов. URL:

<https://www.vedomosti.ru/technology/articles/2023/12/28/1013347-hakeri-osvoili-shantazh-rassilkoi-intimnih-foto>.

59. The Gender-Equal Cybercriminal Underground. URL: https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/gender-in-cybercrime?utm_source=Securitylab.ru.

Эмпирические материалы

60. Апелляционное определение Ульяновского городского суда по делу № 22-937/2018. URL: <http://www.ulobsud.ru/index.php?option=3&id=90&idCard=73288>.

61. Апелляционное определение по делу № 10-15408/2019. URL: mos-gorsud.ru.

62. Дело № 1-494/2022. URL: <https://savelovskij.mos-gorsud.ru/rs/savelovskij>.

63. Дело № 1-523/2013, первая инстанция. URL: <https://actofact.ru/case-24RS0035-1-523-2013-2013-08-01-2-0/>.

64. Приговор № 1-159/2019 1-4/2020 от 21 февраля 2020 г. по делу № 1-159/2019. URL: <https://sudact.ru/regular/doc/mzqRYkys7bg8/>.

65. Приговор № 1-11/2020 от 9 октября 2020 г. по делу № 1-11/2020. URL: <https://sudact.ru/regular/doc/GkTlgDtAqalY/>.

66. Приговор № 1-481/2024 1-66/2025 от 22 января 2025 г. по делу № 1-481/2024. URL: <https://sudact.ru/regular/doc/ZpsnpfMDZ4HN/>.

67. Постановление № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020. URL: <https://sudact.ru/regular/doc/ftR7s3xLHjHQ/>.