

УДК 343.72:343.985.7

DOI: 10.24412/2713-1033-2025-4-70-84

**А. А. Пестрякова**

Академия управления и производства,  
Москва, Россия, e-mail: Alena\_krivova@mail.ru

## **СОДЕРЖАНИЕ И ЗНАЧЕНИЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ**

Криминалистическая характеристика мошенничества, совершенного с использованием электронных средств (онлайн-мошенничества), является обязательным элементом методики расследования данного вида преступлений. Образующие ее сведения успешно используются при раскрытии и расследовании различных видов киберпреступлений. Однако, это не означает отсутствия в теории и на практике ряда спорных вопросов, имеющих отношение к рассматриваемой характеристике. В частности, до настоящего времени не решен однозначно вопрос о круге сведений, которые целесообразно освещать в рамках криминалистической характеристики онлайн-мошенничества. К такого рода сведениям должны предъявляться определенные требования – теоретическая доказанность, распространенность, значимость для решения криминалистическими средствами и методами задач выявления, раскрытия преступлений, изобличения виновных и т.д.

Изучение предлагаемых в научных и практических работах по проблемам раскрытия и расследования киберпреступлений вариантов криминалистической характеристики онлайн-мошенничества показало, что многие из этих характеристик являются неполными, противоречивыми, отдельные сведения не всегда правильно интерпретируются, недостаточно увязываются с насущными потребностями следственной практики. Отмеченные моменты актуализируют важность специального исследования структуры и содержания криминалистической характеристики мошенничества, совершенного с использованием электронных средств.

**Ключевые слова:** мошенничество, совершенное с использованием электронных средств, онлайн-мошенничество, киберпреступления, криминалистическая характеристика, криминалистически значимые признаки, методика расследования, компьютерная информация, способ, обстановка, цифровые следы.

**Ссылка для цитирования:** Пестрякова А.А. Содержание и значение криминалистической характеристики мошенничества, совершенного с использованием электронных средств // Социальные нормы и практики. 2025. № 4. С. 70-84. DOI: 10.24412/2713-1033-2025-4-70-84.

**A. A. Pestryakova**

Academy of Management and Production,  
Moscow, Russia, e-mail: Alena\_krivova@mail.ru

## **THE CONTENT AND SIGNIFICANCE OF CRIMINALISTIC CHARACTERISTICS OF FRAUD COMMITTED BY ELECTRONIC MEANS**

In contemporary investigative practice, the criminalistic characteristics of fraud committed by electronic means (online fraud) constitutes a key element of the methodology for investigating this category of crimes. The information it comprises is successfully used in the detection and investigation of various types of cybercrime. However, numerous controversial issues remain in both theory and practice. In particular, the scope of information appropriate for inclusion in a forensic characterization of online fraud has not yet been clearly defined. Such information must meet certain requirements, including theoretical substantiation, prevalence, and relevance for solving the problems of identifying and investigating crimes, establishing the persons involved, and ensuring effective criminal prosecution through forensic tools and methods.

A study of criminalistic characteristics of online fraud presented in academic and practical research on cybercrime detection and investigation reveals that many of these characteristics are incomplete and contradictory. Certain pieces of information are not always correctly interpreted and insufficiently aligned with the pressing needs of investigative practice. These findings highlight the importance of a specialized study of the structure and content of criminalistic characteristics of fraud committed by electronic means.

**Keywords:** fraud committed by electronic means, online fraud, cybercrime, criminalistic characteristics, forensically significant features, investigative methodology, computer information, method, context, digital traces.

**For citation:** Pestryakova A.A. (2025) The Content and Significance of Criminalistic Characteristics of Fraud Committed by Electronic Means. *Social norms and practices*. No. 4. P. 70-84. DOI: 10.24412/2713-1033-2025-4-70-84.

### **Введение**

Обеспечение государственной защиты интересов российских граждан в информационной сфере является одним из основных принципов Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. № 203 (п. «е» ст. 3)<sup>1</sup>. Как отмечалось в нашей более ранней работе, «в данном направлении наше государство предпринимает комплекс мер, в числе которых особое место

---

<sup>1</sup> О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

занимает введение уголовной ответственности за посягательства в сфере информационной безопасности граждан. Подтверждением этого служит криминализация ряда противоправных действий, связанных с использованием современных информационных технологий (так называемых киберпреступлений)» [Пестрякова, 2025: 84]. Так, в УК РФ были включены статьи 159.3 «Мошенничество с использованием электронных средств платежа» и 159.6 «Мошенничество в сфере компьютерной информации».

Складывающиеся тенденции в сфере борьбы с киберпреступлениями вызывают определенные опасения. По данным официальной статистики МВД России, доля данных деяний растет. Например, «...в 2022 г. зарегистрировано 522065 таких преступлений, что составляет 26,5 % от общего числа всех зарегистрированных преступных посягательств, тогда как... в 2017 г. этот показатель был почти в шесть раз ниже и составлял всего 4,4 %» [Харина, 2024: 3-4]. В 2024 году в МВД зарегистрировали 765 тыс. киберпреступлений, среди которых 486 тыс. приходилось на онлайн-мошенничество, что составило 40 % от общего числа всех правонарушений. В результате действий кибермошенников в 2024 году пострадали 448,9 тыс. человек, немного больше, чем в 2023 году, когда этот показатель составил 448,5 тыс. В 2024 году ущерб от онлайн-мошенничества увеличился на 36 % и составил 200 миллиардов рублей. В статистике МВД РФ за 2023 год аналогичный ущерб был зафиксирован на уровне 147 миллиардов рублей.

Данные показатели свидетельствуют о том, что на текущий момент борьба с онлайн-мошенничествами недостаточно эффективна по ряду причин: «...во-первых, особенности противоправной деятельности, связанной с компьютерной информацией, изучение которой всегда требует применения специальных знаний, высокой квалификации, высокотехнологичных средств, специализированных информационных ресурсов; во-вторых, сложности в обнаружении следов преступной деятельности, существующих в форме компьютерной информации; в-третьих, постоянно совершенствующиеся способы совершения преступлений, связанные с новыми программными продуктами и компьютерными устройствами; в-четвертых, использование различных средств коммуникации, затрудняющих идентификацию пользователей (анонимные мессенджеры и др.)» [Пестрякова, 2025: 84].

Для повышения эффективности борьбы с онлайн-мошенничествами необходимо переосмыслить подходы к разработке криминалистической характеристики киберпреступлений и ее практическому применению.

### **Материалы и методы**

Теоретической основой исследования послужили труды С.Ю. Балмочных, Ю.М. Батурина, В.Ю. Белицкого, Л.В. Бертовского, А.А. Васильева, В.Ф. Васюкова, В.Б. Вехова, Ю.В. Гаврилина, Г.Р. Григоряна, М.А. Ефремовой, Л.В. Ивановой, Е.П. Ищенко, Р.Г. Камнева, А.Н. Колычевой, К.С. Латыповой, В.А. Мещерякова, В.А. Милашева, В.А. Образцова, Г.В. Пережогойной, В.В. Полякова, И.М. Рассолова, Е.Р. Россинской, Е.А. Рускевича,

М.Д. Фролова, Е.А. Хариной и других ученых.

В целом, исследования указанных авторов позволили создать оптимальную, цельную, законченную систему описания криминалистически значимых признаков онлайн-мошенничества, показать их значение для эффективного осуществления практической криминалистической деятельности. Однако отдельные аспекты требуют более глубокого изучения, становятся актуальными новые вопросы, связанные с современным состоянием и динамикой киберпреступности и борьбы с нею.

Методологическую основу исследования составили диалектический, сравнительный, статистический, логические, психологические методы, а также группа методов криминалистического анализа и изучения следственной практики.

### **Изучение проблемы**

Любая криминалистическая характеристика представляет собой описание характерных, отличительных качеств, черт какого-либо преступления, значимых для его раскрытия и расследования, и отражает самые существенные и устойчивые признаки и закономерности определенного вида преступлений. Чтобы получить криминалистическую характеристику, необходимо обобщить данные о соответствующем виде преступлений и выявить закономерности между элементами таких преступлений.

Криминалистическая характеристика имеет практическую ценность, когда представляет собой не просто комплекс сведений, но при условии, что «... между его составляющими установлены корреляционные связи и зависимости, носящие закономерный характер» [Белкин, 2001: 222].

Учитывая вышесказанное, криминалистическую характеристику мошенничества, совершенного с использованием электронных средств, можно определить как систему сведений, основанную на обобщенных данных следственной и судебной практики и отражающую совокупность криминалистически значимых признаков данного вида преступлений, знание которых необходимо для разработки научно обоснованных рекомендаций по выявлению, раскрытию и расследованию преступлений.

Мошенничество, совершаемое с использованием электронных средств, представляет собой двойственную по своей природе форму преступного поведения, которая одновременно охватывает признаки преступления против собственности и относится к числу высокотехнологичных (компьютерных) уголовно-правовых деликтов. С одной стороны, данное деяние сохраняет классическую структуру имущественного преступления и направлено на незаконное изъятие имущества или приобретение прав на него. С другой стороны, особенности способа совершения, основанного на информационных технологиях, выводят это преступление за пределы обычной криминальной практики.

В структуру криминалистической характеристики мошенничества, совершенного с использованием электронных средств, обычно включаются

данные о способах реализации преступного замысла, об обстановке, в которой совершается преступление, о следовой картине, а также сведения о типичных личностных свойствах преступника и потерпевшего.

Под способом реализации преступного замысла понимается совокупность методов, применяемых субъектом преступной деятельности для достижения противоправного результата. Следует отметить, что способ совершения преступления – это не просто технический прием, а системное отражение внутренней мотивации и целенаправленности личности правонарушителя, реализующееся во внешне наблюдаемой форме. Он охватывает действия по подготовке преступления, его непосредственному осуществлению, а также укрывательству следов и представляет собой динамическую совокупность внешних проявлений внутреннего состояния субъекта, направленных на достижение противоправного результата [Харина, 2023а: 12].

Анализ правоприменительной практики и научной литературы позволяет выделить и систематизировать наиболее характерные способы совершения рассматриваемых деяний. В рамках предложенной классификации выделяются несколько моделей онлайн-мошенничества: организованное (предполагающее участие устойчивой группы лиц, действующих по предварительному плану); несложное (характеризующееся применением ограниченного набора технических средств и низкой степенью сокрытия следов); простое (при котором используется минимальный уровень информационно-технологической подготовки).

В структуре способа совершения преступления важное место занимают действия, предшествующие непосредственному осуществлению противоправного деяния, то есть подготовительный этап, на котором закладываются основные условия для успешной реализации преступного замысла. Анализ материалов, полученных в ходе исследования, свидетельствует о том, что мошенничество, совершаемое с использованием электронных средств, практически никогда не осуществляется спонтанно, напротив, оно предполагает предварительную проработку схемы действий, адаптацию инструментов и анализ цифровой среды. Подготовительные мероприятия могут варьироваться по глубине, сложности и длительности в зависимости от выбранной модели совершения преступления.

Типовыми подготовительными мероприятиями являются, в частности: «...разработка плана и механизма преступной деятельности; получение специальных познаний, навыков и умений в сфере ИТТ либо приискание лиц, ими обладающих; создание преступного формирования; приобретение соответствующих компьютерных устройств, технических средств, средств связи, средств платежа (банковских, иных платежных карт и т.д.); регистрация электронной почты, установка мессенджеров, программ, сервисов, затрудняющих идентификацию; регистрация юридических лиц, открытие банковских счетов для перенаправления похищенных денежных средств; приобретение в собственность и/или аренда жилых, нежилых помещений; получение конфиденциальной информации, необходимой для совершения

хищений; приискание, создание ВПО (*вредоносного программного обеспечения* – курсив мой. – А.П.); поиск, аренда управляющих серверов; создание сайтов, имитирующих официальные сайты; использование в противоправных целях компьютерных сетей, позволяющих организовать доступ к информации, распространение которой в России запрещено; использование различных программ, направленных на сокрытие следов преступной деятельности; изучение деятельности объекта преступного посягательства» [Харина, 2024: 21-22].

В настоящее время, с учетом проведенных исследований, можно выделить следующие наиболее распространенные способы онлайн-мошенничества:

«1) посредством осуществления неправомерного доступа к информационной инфраструктуре кредитной организации;

2) посредством воздействия вредоносного программного обеспечения... на компьютерные устройства клиентов кредитных организаций;

3) посредством установления контроля за работой компьютерных устройств юридических лиц через предустановленное ВПО;

4) посредством неправомерного внесения изменений в платежные поручения юридических лиц;

5) посредством осуществления несанкционированного управления работой банкомата;

6) посредством задержки шторки купюроприемника банкомата либо с использованием приспособлений, позволяющих вернуть вложенные купюры;

7) посредством создания и использования «фишинговых» сайтов» [Харина, 2024: 13-14].

«Анализ следственной практики свидетельствует о высокой степени активности субъектов преступной деятельности, направленной на противодействие выявлению, раскрытию и расследованию онлайн-мошенничеств. Указанное поведение приобретает особенно выраженный характер при участии организованных преступных групп, в составе которых нередко действуют специализированные лица, основной задачей которых является сокрытие цифровых следов, образующихся в результате реализации преступного замысла» [Пестрякова, 2025: 87].

В целях противодействия расследованию преступники активно используют специализированные программные решения, предназначенные для маскировки источников и маршрутов цифровой активности. Среди них: «ремейлеры», осуществляющие переадресацию писем и подмену адреса отправителя, затрудняющие отслеживание исходного узла отправки; анонимайзеры, обеспечивающие подмену IP-адреса, используемого устройством; VPN-сервисы, создающие зашифрованный туннель между пользователем и удаленным сервером, скрывающим истинный источник интернет-соединения; прокси-серверы, играющие роль посредников в передаче данных между клиентом и интернетом, в том числе открытые и анонимные, через которые может проходить трафик от сотен пользователей, имеющих один и тот же внешний IP-адрес.

Выявление способа реализации преступного замысла, как правило, тесно коррелирует с другим важным элементом криминалистической характеристики – системой следов, возникающих в результате противоправной деятельности.

Последствиями преступлений в сфере информационных технологий могут быть как вещественные следы (например, следы электронных носителей, модификации программных кодов), так и цифровые следы (журналы активности, сетевые лог-файлы, данные о подключениях и др.). Анализ следовой информации позволяет реконструировать не только непосредственный способ совершения преступления, но и детали, касающиеся подготовки, примененных технических средств, сценариев сокрытия, а также числа и характеристик лиц, принимавших участие в совершении деяния.

Особенности следовой картины при расследовании онлайн-мошенничеств во многом определяются преобладанием цифровых следов, составляющих основную доказательственную базу [Теория информационно-компьютерного обеспечения криминалистической деятельности, 2023: 44-45]. Характер этих следов может варьироваться в зависимости от квалификации преступника, примененных им программных средств, способов маскировки действий и удаленности от места совершения преступления. Преступники с высоким уровнем ИТ-подготовки, как правило, оставляют минимальный объем прямых цифровых следов, тогда как действия менее компетентных лиц фиксируются в системных логах, сетевых журналах, временных файлах и иных хранилищах.

В литературе выделяют три взаимосвязанные стадии процесса формирования цифрового следа. Первая стадия – физическое проявление характеристик следообразующего объекта, то есть момента взаимодействия субъекта с техническим устройством. Вторая стадия охватывает преобразование проявленных признаков в цифровую форму, обеспечивающую возможность их фиксации и дальнейшего анализа. На третьем этапе происходит предварительная обработка, передача и сохранение полученной информации, что завершает процесс формирования криминалистически значимого цифрового следа.

К числу ключевых элементов криминалистической характеристики преступления относится обстановка, в которой реализуется противоправное деяние. Эта категория охватывает совокупность внешних условий и ситуационных факторов, непосредственно влияющих на характер, динамику и особенности преступного поведения. Анализ обстановки имеет важнейшее значение для реконструкции механизма преступления, поскольку определяет специфику подготовки, выбор способа реализации преступного замысла, тактику сокрытия следов, а также оказывает воздействие на поведенческую модель участников противоправной деятельности.

Спецификой преступлений в сфере компьютерной информации является то, что они совершаются без непосредственного контакта с потерпевшим, в особом нематериальном пространстве, которое называют «киберпространством» [Рассолов, 2009: 11], «виртуальным пространством» [Ищенко, 2013: 16-23], «цифровым пространством» [Иванова, Пережогина, 2020: 158-160]. В Стратегии развития информационного общества РФ используется термин

«информационное пространство»<sup>1</sup>. Несмотря на терминологические различия, указанные понятия объединяет то, что взаимодействия в таком пространстве осуществляются посредством цифровых технологий, «...прямой контакт между правонарушителем и потерпевшим отсутствует, что качественно отличает онлайн-мошенничество от классических форм имущественных преступлений» [Пестрякова, 2025: 85].

Одной из характерных черт киберпреступлений является высокая степень подготовленности со стороны субъектов противоправной деятельности. Особенно это касается лиц, обладающих углубленными техническими знаниями и навыками. Подобная тенденция напрямую обусловлена влиянием специфической обстановки, формирующейся в цифровом пространстве, на выбор способов совершения деяния.

На этапе предварительной подготовки преступники, как правило, предпринимают целенаправленные меры по модификации обстановки после реализации преступного действия. Основное внимание при этом уделяется уничтожению следовой информации, которая могла бы быть использована в процессе расследования. Среди распространенных приемов решения данной задачи можно выделить следующие: применение программного обеспечения с функцией автоматического удаления данных, использование самоуничтожающихся скриптов, ликвидация журналов активности, файлов регистрации, системных логов и других цифровых артефактов, способных свидетельствовать о вмешательстве в информационную систему.

Соответственно, наметившаяся в преступной практике устойчивая тенденция к активному воздействию на обстановку как до, так и после совершения деяния, требует от правоохранительных органов применения нестандартных подходов к фиксации и восстановлению цифровой следовой информации, а также пересмотра традиционных методик оценки криминалистической обстановки с учетом ее виртуализированного характера.

К основным элементам обстановки совершения преступления следует отнести место и время.

В условиях стремительной цифровизации и перехода пространства в виртуальную форму понятие места преступления в сфере информационно-коммуникационных технологий приобретает специфические черты.

В научной литературе сформировались различные подходы к определению места совершения преступлений, относящихся к области компьютерной информации. Так, согласно позиции Л.В. Ивановой и Г.В. Пережогойной, под местом совершения подобного рода деяний следует понимать точку, в которой осуществляется ввод данных или подключение к информационно-телекоммуникационной сети, откуда запускается противоправная активность. При этом, в трактовке указанных авторов, территориальная локализация

---

<sup>1</sup> О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

наступивших последствий значения не имеет [Иванова, Пережогина, 2020: 166].

В рамках альтернативной точки зрения В.В. Коломинов подчеркивает, что, в контексте мошенничества с использованием цифровых технологий, «кроме телекоммуникационной сети, местом совершения мошенничества являются места обналичивания денежных средств, полученных путем обмана» [Коломинов, 2015: 267].

Анализ судебной и следственной практики свидетельствует о том, что местом совершения рассматриваемой категории преступлений признаются как место совершения деяния, так и место наступления общественно опасных последствий. Кроме того, криминалистической значимостью обладают и места обналичивания денежных средств, полученных преступным путем, поскольку часто такие места оборудованы средствами видеонаблюдения, что позволяет получить доказательственную информацию. Записи с таких устройств могут быть использованы для идентификации лица, совершившего преступление, а также для верификации времени и способа реализации соответствующих действий.

При дистанционном способе совершения преступлений ключевым объектом криминалистического анализа становится место размещения устройств потерпевшего. Именно на них фиксируются цифровые следы, позволяющие выявить вредоносную активность, включая функционирование вредоносного программного обеспечения, и восстановить хронологию преступных действий. Это особенно актуально при посягательствах на инфраструктуру банковских учреждений.

Как отмечалось выше, отличительной чертой киберпреступлений является опосредованный характер взаимодействия между их участниками. Отсутствие физического контакта обусловлено использованием сетевых каналов связи, что позволяет преступнику и потерпевшему находиться в различных регионах, включая территории иностранных государств. Такая специфика усиливает трансграничную природу преступных деяний и порождает дополнительные сложности в расследовании и юрисдикционном определении. Отмеченная трансграничность существенно осложняет проведение процессуальных действий и межгосударственного взаимодействия в рамках расследования. На практике зафиксированы случаи, когда деятельность преступных сообществ охватывала более сорока юрисдикций, что стало возможным благодаря использованию глобальной информационно-коммуникационной инфраструктуры<sup>1</sup>.

Временной фактор представляет собой важный элемент обстановки совершения киберпреступлений. Учитывая особенности функционирования компьютерных устройств, обладающих встроенными механизмами хронометража операций пользователей и системных процессов, установление времени совершения противоправного деяния, как правило, не представляет

---

<sup>1</sup> Кольчева А.Н., Васюков В.Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие. М., 2020. С. 24-25.

значительных трудностей. Однако с криминалистической точки зрения особое внимание следует уделять вопросам достоверности таких временных меток. Не исключается возможность преднамеренной коррекции системного времени с целью искажения следовой информации и сокрытия факта преступного вмешательства.

Хронологические особенности совершения онлайн-мошенничества во многом зависят от способа реализации преступного замысла. В частности, при хищениях, осуществляемых посредством неправомерного доступа к информационной инфраструктуре кредитных организаций, преступники, как правило, прибегают к предварительной, тщательно спланированной подготовке [Харина, 2023а]. На этом этапе возможны тестовые подключения, анализ защищенных сегментов сети, сбор служебной информации и подбор уязвимостей. От момента первичного проникновения в систему до реализации хищения может пройти значительное время, от нескольких дней до нескольких недель. Заключительная фаза преступления, как показывает практика, нередко осуществляется в вечернее время последнего рабочего дня недели, а также в выходные и праздничные дни, когда контроль со стороны специалистов по информационной безопасности ослаблен, а оперативное реагирование на инциденты затруднено.

Аналогичная временная специфика наблюдается при совершении преступлений, связанных с физическим вмешательством в функционирование банкоматов. Такие действия, как показывает практика, преимущественно совершаются в ночное либо позднее вечернее время. Данный выбор обусловлен стремлением минимизировать риск визуального обнаружения, в том числе с использованием систем видеонаблюдения, а также исключить вероятность наличия случайных очевидцев.

В противоположность этому, в преступлениях, совершаемых с использованием служебного положения, например, сотрудниками финансово-кредитных учреждений, преступный замысел реализуется преимущественно в рабочие часы [Харина, 2023а], когда у лиц, обладающих доступом к компьютерной банковской инфраструктуре, есть возможность законного входа в систему и совершения преступных действий без выхода за рамки их формальных служебных полномочий.

В структуру обстановки можно обоснованно включить «обладание соответствующими компьютерными устройствами, программно-аппаратными и другими техническими средствами, с помощью которых и совершаются преступления данной категории» [Харина, 2024: 12]. Наличие или отсутствие таких технических ресурсов во многом определяет способ совершения деяния, механизмы сокрытия следов, а также влияет на успешность или провал преступного замысла. Уровень технического оснащения преступника, в частности, наличие дорогостоящего оборудования, высокотехнологичных вредоносных программ, обладающих способностями к маскировке, самоуничтожению, а также преодолению систем информационной безопасности, формирует искусственно созданную обстановку высокой

устойчивости к обнаружению.

Важным элементом криминалистической характеристики онлайн-мошенничества выступают данные о личности преступника.

Наряду с обобщенным образом личности преступника в криминологии подчеркивается, что в зависимости от характера преступной направленности, конкретной социальной среды, способа совершения преступления и его цели личность правонарушителя может обладать рядом специфических черт, отличающих ее от иных категорий преступников. Эти особенности проявляются в поведенческих установках, мотивационной структуре, уровне подготовки, а также в характере отношения к потерпевшему и выбранному объекту посягательства.

Совершение онлайн-мошенничества требует от злоумышленника применения «...специальных знаний в области информационно-телекоммуникационных технологий. Уровень таких познаний напрямую зависит от способа совершения деяния и сложности применяемых технических решений» [Пестрякова, 2025: 86].

Анализ личности преступника, совершающего киберпреступления, позволяет выделить одну из наиболее характерных черт – отстраненность от личности жертвы. Как правило, субъект подобных деяний не находится в непосредственном контакте с потерпевшим, не обладает информацией о его индивидуально-личностных качествах и не стремится к их получению. Для него значение имеет не жертва как личность, а ее функциональное положение как носителя определенных цифровых, финансовых или иных ресурсов. Определяющим фактором мотивации таких правонарушителей выступает факт обладания жертвы ценным объектом посягательства, доступ к которому и составляет основную задачу преступника.

Анализ данных Судебного департамента при Верховном Суде РФ позволяет выделить типичный социально-демографический профиль лица, осужденного за киберпреступления. Преобладающее большинство таких преступников – мужчины от 18 до 35 лет, имеющие высшее или среднее профессиональное образование, что свидетельствует о вовлечении в преступную деятельность относительно молодых и образованных лиц, обладающих базовыми или углубленными навыками работы с цифровыми технологиями и компьютерными системами. Возрастной диапазон объясняется тем, что именно в данном периоде жизни лицо, с одной стороны, обладает уже сформированными профессиональными навыками, с другой – сохраняет гибкость восприятия, активность в цифровой среде, а также склонность к экспериментированию и риску. Наличие профессионального образования, в свою очередь, создает техническую основу для реализации преступных схем различной степени сложности.

В рамках анализа социальных и психологических характеристик лиц, совершающих киберпреступления, представляется целесообразным выделить ряд устойчивых негативных поведенческих черт, которые, в большинстве случаев, проявляются в процессе их социальной адаптации и профессионального

позиционирования. К числу таких особенностей относятся: негативное отношение к физическому труду; отсутствие патриотических установок; ограниченность социальных контактов; гипертрофированная самооценка и убежденность в безнаказанности [Харина, 2023b: 54].

В рамках криминалистической характеристики преступлений указанной категории обоснованным представляется выделение элемента, связанного с личностью потерпевшего, как значимой структурной единицы.

Круг лиц, признаваемых потерпевшими от действий онлайн-мошенников, отличается высокой степенью охвата и включает как физических, так и юридических лиц, независимо от формы собственности. Киберпреступления посягают на имущественные интересы, информационные ресурсы, банковские счета, персональные данные и иные цифровые активы, что делает уязвимыми как частных граждан, так и коммерческие структуры, государственные учреждения, финансовые организации.

Ключевая отличительная черта онлайн-мошенничества заключается в отсутствии непосредственного контакта между преступником и потерпевшим. Данный фактор обусловлен спецификой цифровой среды, в которой субъекты противоправной деятельности действуют удаленно, нередко анонимно, используя сложные схемы сокрытия своего присутствия.

Выбор жертв киберпреступлений напрямую зависит от уровня организации и цели преступной деятельности. При атаках на систему дистанционного банковского обслуживания решающим фактором является наличие средств на счете, вне зависимости от личности владельца. Типичным признаком потерпевшего является также наличие материальных ресурсов, доступ к которым возможен через цифровые каналы. Еще одним важным фактором выступает пренебрежение мерами информационной безопасности, включая неосведомленность о способах защиты и недооценку угроз.

К числу лиц, наиболее подверженных риску стать потерпевшими от онлайн-мошенничества, относятся, прежде всего, активные пользователи сети Интернет, в особенности те, кто регулярно осуществляет платежные операции, приобретает товары и услуги онлайн, а также использует системы дистанционного банковского обслуживания. Постоянное обращение к цифровым сервисам и передача персональных данных через сетевые каналы значительно увеличивает вероятность незаконного использования информации и, как следствие, вовлечения пользователя в преступную схему.

Кроме того, определенной уязвимостью обладают и юридические лица, в том числе коммерческие и государственные структуры, в чьем распоряжении находятся программно-технические комплексы, обеспечивающие доступ к корпоративным, финансовым и персонализированным данным. Даже при наличии формализованных мер информационной безопасности, наличие уязвимостей в архитектуре систем, ошибок в конфигурации или использование устаревших средств защиты создает реальные условия для несанкционированного доступа со стороны преступников.

## Выводы

Рассмотренные группы криминалистически значимых сведений «...позволяют сформировать функциональную модель преступной деятельности в виде онлайн-мошенничества. Эта модель может использоваться для разработки эффективной тактики первоначальных следственных действий, построения версий, прогнозирования развития событий и повышения раскрываемости цифровых преступлений» [Пестрякова, 2025: 87].

Методика расследования онлайн-мошенничеств во многом зависит от правильного использования криминалистической характеристики этих преступлений. Возможности, которые предоставляет криминалистическая характеристика следователям, дознавателям и др., помогают строить версии по делу, целенаправленно организовывать поиск преступника, обнаруживать доказательства.

Процесс познания в ходе раскрытия онлайн-мошенничества основывается на сборе, накоплении, переработке, исследовании и использовании фактической информации, которая обобщается в связанных между собой элементах криминалистической характеристики. Выявление таких связей и установление закономерностей, по которым они образуются, осуществляется на основе данных обобщения следственной практики, изучения статистических совокупностей уголовных дел об онлайн-мошенничестве.

## Список литературы (References)

1. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М.: Норма, 2001.

Belkin R.S. (2001) *Criminalistics: Contemporary Problems. Burning issues of Russian criminalistics*. Moscow: Norma Publ. (In Russ.).

2. Иванова Л.В., Пережогина Г.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6. № 4 (24). С. 155-171. DOI: 10.21684/2411-7897-2020-6-4-155-171.

Ivanova L.V., Perezhogina G.V. (2020) The digital space as a crime scene under global constraints. *Tyumen State University Herald. Social, Economic, and Law Research*. Vol. 6. No. 4 (24). P. 155-171. DOI: 10.21684/2411-7897-2020-6-4-155-171. (In Russ.).

3. Ищенко Е.П. Виртуальное пространство как объект криминалистического познания // Криминалистика и судебно-экспертная деятельность в условиях современности: материалы Международной науч.-практ. конф.: в 2 т. Т. 1. Краснодар: Краснодарский университет МВД России, 2013. С. 16-23.

Ishchenko E.P. (2013) Virtual Space as an Object of Criminalistics Knowledge. *Criminalistic Science and Forensic Activity in Modern Conditions: Proceedings of the International Scientific and Practical Conference: in 2 volumes*. Vol. 1. Krasnodar: Krasnodar University of the Ministry of Internal Affairs of Russia Publ. P. 16-23. (In Russ.).

4. Коломинов В.В. Установление места совершения преступления в процессе расследования мошенничества в сфере компьютерной информации // Криминалистические чтения на Байкале – 2015: материалы Международной науч.-практ. конф. Иркутск: Восточно-Сибирский филиал РГУП, 2015. С. 264-268.

Kolominov V.V. (2015) Establishing the Crime in the Process of Investigation of Fraud in the Sphere of Computer Information. *Criminalistic Readings on the Baikal – 2015: Proceedings of the International Scientific and Practical Conference*. Irkutsk: East Siberian Branch of the Lebedev Russian State University of Justice Publ. P. 264-268. (In Russ.).

5. Пестрякова А.А. Криминалистические признаки онлайн-мошенничества // Современные тенденции развития управления и производства в условиях цифровизации: материалы V Международной науч.-практ. студенческой конференции. М.: Академия управления и производства, 2025. С. 84-87.

Pestryakova A.A. (2025). Forensic features of online fraud. *Modern trends in the development of management and production in the context of digitalization: Proceedings of the V International Scientific and Practical Student Conference*. Moscow: Academy of Management and Production Publ. P. 84-87. (In Russ.).

6. Рассолов И.М. Право и Интернет: теоретические проблемы. 2-е изд., доп. М.: Норма, 2009.

Rassolov I.M. (2009) Law and the Internet: Theoretical Issues. 2nd ed., suppl. Moscow: Norma. (In Russ.).

7. Теория информационно-компьютерного обеспечения криминалистической деятельности / под ред. Е.Р. Россинской. М.: Проспект, 2023.

Theory of Information and Computer Support for Criminalistic Activity (2023) / ed. by E.R. Rossinskaya. Moscow: Prospect. (In Russ.).

8. Харина Е.А. К вопросу о криминалистической характеристике мошенничества в сфере компьютерной информации // Российский следователь. 2023а. № 11. С. 11-15. DOI: 10.18572/1812-3783-2023-11-11-15.

Kharina E.A. (2023a) On the Criminalistic Characteristics of Cyber Fraud. *Russian Investigator*. No. 11. P. 11-15. DOI: 10.18572/1812-3783-2023-11-11-15. (In Russ.).

9. Харина Е.А. Личность типичного преступника, совершившего мошенничество в сфере компьютерной информации // Российский следователь. 2023б. № 9. С. 53-57. DOI: 10.18572/1812-3783-2023-9-53-57.

Kharina E.A. (2023b) The Identity of a Typical Cybercrime Perpetrator. *Russian Investigator*. No. 9. P. 53-57. DOI: 10.18572/1812-3783-2023-9-53-57. (In Russ.).

10. Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: автореф. дис. канд. юрид. наук. Краснодар, 2024.

Kharina E.A. (2024) Methodology for investigating computer fraud. Abstract of thesis on competition of a scientific degree of Candidate of Law Sciences. Krasnodar. (In Russ.).

**Сведения об авторе**

**Пестрякова Алена Анатольевна** – магистрант, Академия управления и производства.

**E-mail:** Alena\_krivova@mail.ru

**About the author**

**Pestryakova Alena Anatolievna** – undergraduate, Academy of Management and Production.

**E-mail:** Alena\_krivova@mail.ru

Поступила 15.12.2025; одобрена после рецензирования 29.12.2025; принята к публикации 30.12.2025.

Submitted 15.12.2025; revised 29.12.2025; accepted 30.12.2025.