МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«МЕТОДИКА РАССЛЕДОВАНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Янахметов Владислав Маратович
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности, 2020 года
набора, 0101 учебной группы

Руководитель
Доцент кафедры криминалистики
кандидат юридических наук,
Ахметгалеев Вадим Ралифович

К защите рекомендуется
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2026 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

В современной цифровой эпохе электронные денежные средства стали неотъемлемой частью финансовой системы, существенно изменив характер экономических отношений. Параллельно с развитием электронных платежных систем и цифровых финансовых технологий возникают новые формы преступных посягательств на денежные средства граждан и организаций. Хищения электронных денежных средств представляют собой динамично развивающийся вид преступной деятельности, требующий от правоохранительных органов совершенствования методики их расследования.

Актуальность темы исследования обусловлена стремительным ростом количества преступлений, связанных с хищением электронных денежных средств, повышением уровня их технологичности и латентности, а также значительным материальным ущербом, причиняемым гражданам и юридическим лицам. По данным МВД России, в 2022-2025 годах наблюдается устойчивая тенденция к росту числа киберпреступлений, среди которых хищения электронных денежных средств занимают одно из лидирующих мест[1].

Специфика расследования данной категории преступлений заключается в необходимости сочетания традиционных криминалистических методов с современными технологиями цифровой криминалистики, что требует от сотрудников правоохранительных органов специальных знаний и навыков. Территориальные органы внутренних дел, являясь первичным звеном в борьбе с рассматриваемыми преступлениями, сталкиваются с рядом трудностей при их расследовании, что актуализирует потребность в разработке и внедрении эффективных методик.

Степень разработанности темы в научной литературе нельзя назвать достаточной. Несмотря на наличие исследований по смежным вопросам

---

[1] Статистические данные МВД РФ // Официальный сайт МВД РФ. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 20.02.2026)

информационной безопасности и экономических преступлений, комплексные работы, посвященные методике расследования хищений электронных денежных средств на уровне территориальных органов внутренних дел, представлены недостаточно. Проблема осложняется постоянным совершенствованием технических средств и методов совершения данных преступлений, что требует оперативной актуализации научных разработок.

Объектом исследования выступают общественные отношения, возникающие в процессе расследования преступлений, связанных с хищением электронных денежных средств, сотрудниками территориальных органов внутренних дел.

Предметом исследования являются закономерности механизма совершения хищений электронных денежных средств, а также организационно-тактические особенности их расследования на уровне территориальных органов внутренних дел.

Цель исследования состоит в комплексном анализе теоретических и практических аспектов методики расследования хищений электронных денежных средств и разработке научно обоснованных рекомендаций по повышению эффективности деятельности территориальных органов внутренних дел в данной сфере.

Для достижения указанной цели необходимо решить следующие задачи:

– проанализировать понятие и сущность электронных денежных средств как объекта преступного посягательства;

– исследовать уголовно-правовую характеристику хищений электронных денежных средств;

– изучить криминалистическую характеристику данного вида преступлений;

– рассмотреть особенности возбуждения уголовных дел и организации первоначального этапа расследования;

– проанализировать тактику проведения отдельных следственных действий при расследовании хищений электронных денежных средств;

– выявить проблемы и перспективы совершенствования методики расследования исследуемых преступлений.

Теоретико-методологическую основу исследования составляют фундаментальные труды в области криминалистики, уголовного права и процесса, а также специальные исследования по проблемам расследования преступлений в сфере информационных технологий и противодействия киберпреступности.

Нормативную базу исследования составляют Конституция Российской Федерации, действующее уголовное и уголовно-процессуальное законодательство, федеральные законы, нормативные правовые акты МВД России.

Эмпирическую базу исследования составляют материалы следственной и судебной практики по делам о хищениях электронных денежных средств, статистические данные территориальных органов внутренних дел, а также результаты анкетирования сотрудников подразделений, осуществляющих расследование данной категории преступлений.

Практическая значимость исследования заключается в возможности использования его результатов для совершенствования деятельности территориальных органов внутренних дел по расследованию хищений электронных денежных средств, а также в образовательном процессе при подготовке сотрудников правоохранительных органов.

Структура работы обусловлена целями и задачами исследования и включает в себя введение, три главы, объединяющие шесть параграфов, заключение, список использованной литературы.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ РАССЛЕДОВАНИЯ ХИЩЕНИЯ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

§1. Понятие и правовой статус электронных денежных средств в современном законодательстве России

В условиях цифровизации экономики Российской Федерации особую значимость приобретает институт электронных денежных средств (далее - ЭДС), выступающий как важнейший элемент национальной платежной системы и требующий детального анализа в контексте теоретико-правового исследования[1].

Законодательное определение электронных денежных средств содержится в п. 18 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее - Закон № 161-ФЗ). Согласно данной норме, под электронными денежными средствами понимаются денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа[2].

Важно отметить, что законодатель не относит к электронным денежным средствам денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг,

---

[1] Ситник А.А. Цифровой рубль как объект финансово-правового регулирования // Актуальные проблемы российского права. 2023. Т. 18, № 8(153). С. 20.

[2] О национальной платежной системе: федеральный закон от 27 июня 2011 г. № 161-ФЗ // СЗ РФ. 2011. № 27. Ст. 3872.

клиринговую деятельность и/или деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций.

Проведенный нами анализ правовой природы электронных денежных средств позволяет выделить следующие ключевые признаки данного института:

1. Безналичный характер. ЭДС существуют исключительно в электронной форме, не имеют физического выражения, что отличает их от наличных денежных средств.

2. Предварительное предоставление. В отличие от классических безналичных расчетов, использование ЭДС предполагает предварительное внесение денежных средств.

3. Учет без открытия банковского счета. Отсутствие необходимости открытия банковского счета существенно упрощает использование ЭДС для пользователей, однако одновременно снижает уровень защищенности данных средств.

4. Целевое назначение. ЭДС предназначены исключительно для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами.

5. Особый порядок распоряжения. Право передавать распоряжения о переводе ЭДС возможно исключительно с использованием электронных средств платежа[1].

При анализе правового статуса электронных денежных средств необходимо обратить внимание на эволюцию подходов к их регулированию.

---

[1] Воскресенская А.М. Правовое регулирование соотношения безналичных денежных средств, электронных денежных средств и цифрового рубля // Студенческий вестник. 2026. № 1-5(381). С. 68.

До принятия Закона № 161-ФЗ наблюдалась правовая неопределенность в отношении статуса ЭДС, что создавало значительные риски для участников правоотношений. Как отмечает Е.Э. Колдырина, отсутствие специального регулирования ЭДС приводило к необходимости применения общих норм гражданского законодательства по аналогии, что не всегда соответствовало техническим особенностям функционирования электронных платежных систем[1].

Современное правовое регулирование операций с ЭДС строится на многоуровневой основе. Помимо базового Закона № 161-ФЗ, существенное значение имеют:

1. Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», определяющий полномочия Банка России в сфере регулирования национальной платежной системы[2];

2. Положение Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств», регламентирующее порядок перевода электронных денежных средств[3];

3. Указание Банка России от 20.07.2016 № 4077-У «О порядке представления кредитными организациями в уполномоченный орган сведений о случаях отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом», устанавливающее механизмы противодействия легализации доходов, полученных преступным путем, и финансированию терроризма при использовании ЭДС[4];

---

[1] Колдырина Е.Э. Правовые аспекты соотношения безналичных денежных средств, электронных денежных средств и цифрового рубля // Аллея науки. 2025. Т. 1, № 9(108). С. 316.

[2] О Центральном банке Российской Федерации (Банке России): федеральный закон от 10.07.2002 № 86-ФЗ // СЗ РФ. 2002. № 12. Ст. 5454.

[3] О правилах осуществления перевода денежных средств: положение Банка России от 29.06.2021 № 762-П [Электронный ресурс]. URL: https://www.consultant.ru (дата обращения: 20.02.2026).

[4] О порядке представления кредитными организациями в уполномоченный орган сведений о случаях отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом: указание Банка России от 20.07.2016 № 4077-У [Электронный ресурс]. URL: https://www.consultant.ru (дата обращения: 20.02.2026).

4. Положение Банка России от 17.08.2023 №821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», содержащее рекомендации по обеспечению безопасности операций с ЭДС[1].

Особенности правового статуса электронных денежных средств проявляются в специфике субъектного состава правоотношений, связанных с их использованием. Ключевыми участниками данных правоотношений выступают:

1. Оператор электронных денежных средств - кредитная организация, в том числе небанковская кредитная организация, имеющая право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций.

2. Клиент (физическое или юридическое лицо) - лицо, предоставившее денежные средства оператору электронных денежных средств.

3. Банк России - регулятор и надзорный орган в сфере национальной платежной системы.

Заслуживает внимания классификация электронных средств платежа, используемых для распоряжения ЭДС. В соответствии с п. 2 ст. 10 Закона № 161-ФЗ выделяются:

– персонифицированные электронные средства платежа, предполагающие идентификацию клиента в соответствии с законодательством о противодействии легализации доходов, полученных преступным путем;

[1] О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств: положение Банка России от 17.08.2023 №821-П [Электронный ресурс]. URL: https://www.consultant.ru (дата обращения: 20.02.2026).

– неперсонифицированные электронные средства платежа, не требующие идентификации клиента, но существенно ограниченные по функциональности и лимитам операций;

– корпоративные электронные средства платежа, предназначенные для использования юридическими лицами и индивидуальными предпринимателями.

Существенным аспектом правового статуса ЭДС является их соотношение с категорией «безналичные денежные средства». В юридической литературе данный вопрос остается дискуссионным. Ряд исследователей, в частности, А.А. Карпенко, отмечают, что электронные денежные средства представляют собой особую разновидность безналичных денежных средств, обладающую специфическими правовыми характеристиками[1].

При разрешении данной дискуссии целесообразно обратиться к ст. 140 Гражданского кодекса РФ, согласно которой платежи на территории Российской Федерации осуществляются путем наличных и безналичных расчетов. Следовательно, с цивилистической точки зрения электронные денежные средства представляют собой особую форму безналичных денежных средств, отличающуюся специфическим правовым режимом.

Следует отметить, что электронные денежные средства не подпадают под действие системы страхования вкладов, что создает дополнительные риски для клиентов операторов ЭДС. Как указывает В.П. Васильев, отсутствие страхования электронных денежных средств является существенным недостатком действующего правового регулирования, создающим неравенство в уровне защиты прав владельцев различных видов денежных средств[2].

---

[1] Карпенко А.А. Сравнительно-правовой анализ безналичных денежных средств, электронных денежных средств и цифрового рубля // Legal Bulletin. 2024. Т. 9, № 4. С. 172.

[2] Васильев В.П. Страхование электронных денежных средств // Legal Bulletin. 2022. Т. 11, № 3. С. 532.

Особенности нормативного регулирования электронных денежных средств в Российской Федерации отражают специфику развития национальной платежной системы и обусловлены необходимостью баланса между обеспечением безопасности финансовой системы и стимулированием инновационного развития финансового рынка. Указанные факторы определяют двойственность правовой природы ЭДС, сочетающей элементы классических безналичных денежных средств и инновационных финансовых технологий.

Таким образом, электронные денежные средства представляют собой сложный правовой институт, характеризующийся специфическим режимом функционирования, многоуровневым нормативным регулированием и особым субъектным составом соответствующих правоотношений. Развитие данного института требует дальнейшего совершенствования правового регулирования с учетом баланса интересов защиты прав потребителей финансовых услуг и обеспечения инновационного развития финансового рынка Российской Федерации.

§2. Уголовно-правовая характеристика хищений электронных денежных средств

Уголовно-правовая охрана электронных денежных средств представляет собой комплексный правовой институт, объединяющий нормы различных разделов Уголовного кодекса Российской Федерации и требующий системного анализа как с позиций общей теории уголовного права, так и с учетом специфики объекта посягательства.

Уголовно-правовая характеристика хищений электронных денежных средств предполагает, прежде всего, определение места соответствующих составов преступлений в системе особенной части УК РФ. Ключевое значение в данном контексте имеют:

– ст. 158 УК РФ – «Кража», п. «г» ч. 3 которой предусматривает ответственность за кражу с банковского счета, а равно в отношении электронных денежных средств;

– ст. 159.3 УК РФ – «Мошенничество с использованием электронных средств платежа»;

– ст. 159.6 УК РФ – «Мошенничество в сфере компьютерной информации»;

– ст. 187 УК РФ – «Неправомерный оборот средств платежей»[1].

Анализ указанных норм позволяет сделать вывод о многоаспектности уголовно-правовой охраны электронных денежных средств, что обусловлено сложностью данного объекта и многообразием способов посягательств на него.

Принципиальное значение для квалификации хищений электронных денежных средств имеет определение объекта и предмета преступного посягательства. Родовым объектом рассматриваемых преступлений выступают общественные отношения в сфере экономики, видовым объектом - отношения собственности, а непосредственным объектом - право собственности на электронные денежные средства.

Дискуссионным в теории уголовного права является вопрос о предмете хищений электронных денежных средств. Как отмечает А.Н. Смоляков, электронные денежные средства обладают специфическими характеристиками, отличающими их от традиционных материальных предметов хищения, что требует особого подхода к квалификации соответствующих деяний[2]. В соответствии с устоявшейся доктринальной позицией, поддерживаемой, в частности, В.С. Алборова, предметом хищения

[1] Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

[2] Смоляков А.Н. Хищение безналичных, электронных денежных средств и цифровой валюты: вопросы юридической техники и дифференциации ответственности: диссертация на соискание ученой степени кандидата юридических наук, 2023. С. 102.

выступает имущество в широком смысле, включающее вещи, имущественные права и иные объекты гражданских прав, имеющие экономическую ценность[1].

Пленум Верховного Суда Российской Федерации в постановлении от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» разъяснил, что предметом хищения могут выступать безналичные денежные средства, в том числе электронные денежные средства (п. 5 Постановления № 48)[2]. Таким образом, несмотря на нематериальную природу электронных денежных средств, они признаются полноценным предметом хищения.

Объективная сторона хищений электронных денежных средств характеризуется разнообразием способов совершения преступления. В зависимости от конкретного способа деяние квалифицируется по соответствующей статье УК РФ:

Кража электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) характеризуется тайным хищением путем несанкционированного доступа к электронному средству платежа или системе электронных денежных средств. Как отмечает В.И. Тюнин, тайность хищения электронных денежных средств проявляется в отсутствии непосредственного контакта с потерпевшим и совершении действий без его ведома[3]. В качестве типичных примеров можно привести:

– использование похищенного или найденного электронного средства платежа;

– несанкционированный доступ к информации о реквизитах электронного средства платежа;

---

[1] Алборова В.С. Хищение денежных средств с использованием электронных средств платежа // Студенческий форум. 2021. № 43-2(179). С. 84.

[2] О судебной практике по делам о мошенничестве, присвоении и растрате: пленум Верховного Суда Российской Федерации в постановлении от 30.11.2017 № 48 // СЗ РФ. 2017. №23. Ст. 4824.

[3] Тюнин В.И. Квалификация хищений безналичных и электронных денежных средств. Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2021. С. 85.

– использование вредоносного программного обеспечения для получения доступа к электронному кошельку.

Мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) предполагает хищение чужого имущества путем обмана или злоупотребления доверием с использованием электронного средства платежа. Согласно п. 17 Постановления № 48, обман при данном виде мошенничества заключается в представлении кредитной, торговой или иной организации заведомо недостоверных сведений о принадлежности электронного средства платежа на законном основании его предъявителю, либо о праве использования этого средства платежа. Особенностью данного вида хищения является активное использование методов социальной инженерии, когда потерпевший сам (будучи введенным в заблуждение) сообщает преступнику сведения, необходимые для доступа к его электронным денежным средствам.

Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) характеризуется хищением электронных денежных средств путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Как указывает Е.Д. Баженова, спецификой данного деяния является отсутствие непосредственного контакта преступника и потерпевшего, а также автоматизированный характер действий по завладению электронными денежными средствами[1]. Примерами такого мошенничества являются:

– создание сайтов-двойников операторов электронных денежных средств;

[1] Баженова Е.Д. Проблемы уголовного преследования за хищения с банковского счета, а равно в отношении электронных денежных средств // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: Материалы Международной научно-практической конференции, Воронеж, 22 мая 2025 года. Воронеж: Воронежский институт МВД РФ, 2025. С. 99.

– компрометация аутентификационных данных пользователей путем применения фишинговых технологий;

– внедрение вредоносного программного обеспечения в информационные системы операторов электронных денежных средств.

Неправомерный оборот средств платежей (ст. 187 УК РФ) включает изготовление, приобретение, хранение, транспортировку в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты, а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств. Данный состав имеет усеченную конструкцию, так как преступление считается оконченным с момента совершения одного из альтернативных действий, перечисленных в диспозиции статьи, независимо от наступления общественно опасных последствий.

Субъективная сторона хищений электронных денежных средств характеризуется виной в форме прямого умысла, корыстной целью и, как правило, тщательной подготовкой преступления. Как подчеркивает С.Б. Авдеева, специфика субъективной стороны данных преступлений проявляется в осознании виновным не только противоправности своих действий, но и технических особенностей функционирования систем электронных денежных средств[1].

Субъект рассматриваемых преступлений - общий, т.е. вменяемое физическое лицо, достигшее 16-летнего возраста (за исключением кражи, ответственность за которую наступает с 14 лет). Вместе с тем, эмпирические исследования показывают, что преступления данной категории преимущественно совершаются лицами, обладающими специальными

[1] Авдеева С.Б. Проблемы квалификации преступлений, связанных с хищением электронных денежных средств // Интернаука. 2022. № 14-4(237). С. 46.

знаниями в сфере информационных технологий, что фактически сужает круг возможных субъектов.

Квалифицирующие признаки хищений электронных денежных средств дифференцированы в зависимости от конкретного состава преступления. Общими для большинства составов являются:

– совершение преступления группой лиц по предварительному сговору;

– совершение преступления организованной группой;

– причинение значительного ущерба гражданину;

– совершение преступления в крупном и особо крупном размерах.

Вместе с тем, существуют специфические квалифицирующие признаки, характерные для отдельных составов. Так, для кражи электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) законодатель установил повышенную ответственность независимо от размера похищенного, что связано с повышенной общественной опасностью данного деяния.

Проблемы квалификации хищений электронных денежных средств тесно связаны со спецификой предмета посягательства и используемых способов совершения преступления. К наиболее значимым проблемам относятся:

Разграничение смежных составов преступлений. Как отмечает И.В. Блинова-Сычкарь, сложности возникают при отграничении кражи электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) от мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ), когда хищение осуществляется путем использования компьютерных технологий[1]. В данном случае ключевым критерием разграничения выступает способ совершения преступления: при краже имеет место тайное хищение путем несанкционированного доступа к электронному средству платежа, тогда как

[1] Блинова-Сычкарь И.В. Вопросы противодействия хищению электронных денежных средств // Приоритетные направления социально-гуманитарных и экономических исследований в современной науке: Сборник научных статей по итогам национальной научно-практической конференции, Волгоград, 28 февраля 2024 года. Волгоград: Волгоградский институт экономики, социологии и права, 2024. С. 12.

при мошенничестве в сфере компьютерной информации - вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации.

Вопросы совокупности преступлений. Дискуссионным является вопрос о квалификации действий, направленных сначала на неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а затем на хищение электронных денежных средств. Согласно позиции Верховного Суда РФ, выраженной в п. 20 Постановления № 48, если мошенничество совершено с использованием принадлежащего другому лицу электронного средства платежа путем сообщения уполномоченному работнику кредитной, торговой или сервисной организации заведомо ложных сведений о принадлежности указанного электронного средства платежа предъявителю, действия виновного квалифицируются как мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ).

Проблемы определения момента окончания преступления. Как указывает Д.А. Мурзабаева, особенности электронных денежных средств как предмета хищения обусловливают специфику момента окончания преступления, который связывается с моментом изменения информации о состоянии электронного счета или кошелька[1]. В практической деятельности правоохранительных органов возникают сложности с определением момента окончания преступления, особенно в ситуациях транзакций между различными электронными платежными системами или при конвертации электронных денежных средств в криптовалюту.

Проблемы юрисдикции. Транснациональный характер многих хищений электронных денежных средств создает проблемы определения места совершения преступления и применимого уголовного закона. Отсутствие

[1] Мурзабаева Д.А. Квалификация хищений электронных денежных средств в условиях конкуренции норм // XLIX Самарская областная студенческая научная конференция: Тезисы докладов, Самара, 10–21 апреля 2023 года. Санкт-Петербург: ООО «Эко-Вектор», 2023. С. 231.

эффективных механизмов международного сотрудничества в сфере противодействия киберпреступности существенно затрудняет расследование и судебное разбирательство по делам о хищениях электронных денежных средств, совершенных с территории иностранных государств.

Анализ уголовно-правовой статистики свидетельствует о неуклонном росте хищений электронных денежных средств. По данным Главного информационно-аналитического центра МВД России, за последние пять лет количество преступлений данной категории увеличилось более чем в три раза[14]. Это обусловлено как объективными факторами (цифровизация экономики, увеличение объема операций с электронными денежными средствами), так и субъективными (высокая латентность, сложность расследования, недостаточная эффективность мер профилактики).

Перспективными направлениями совершенствования уголовно-правовой охраны электронных денежных средств представляются: 1. унификация терминологии уголовного закона и законодательства о национальной платежной системе для обеспечения системности правового регулирования; 2. дальнейшая дифференциация уголовной ответственности за хищения электронных денежных средств в зависимости от способа совершения преступления и характера причиненного ущерба; 3. совершенствование механизмов международного сотрудничества в сфере противодействия транснациональным хищениям электронных денежных средств; 4. развитие системы профилактических мер, направленных на предотвращение хищений электронных денежных средств, включая информирование населения о типичных способах совершения таких преступлений.

Таким образом, эффективное противодействие хищениям электронных денежных средств требует системного подхода, включающего как совершенствование уголовно-правовых норм, так и развитие организационных и технических мер обеспечения безопасности функционирования систем электронных денежных средств.

ГЛАВА 2. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

§1. Особенности криминалистической характеристики хищений электронных денежных средств

Анализ предмета преступного посягательства при хищении электронных денежных средств представляет собой комплексную научную задачу, решение которой требует интегративного подхода на стыке уголовного права, цифровой экономики и информационных технологий[1].

Электронные денежные средства имеют законодательное определение, закрепленное в п. 18 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе». Согласно данной норме, под электронными денежными средствами понимаются денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа[2].

Проведенное нами исследование позволяет утверждать, что с криминалистической точки зрения предмет преступного посягательства при

---

[1] Бикмурзина О.П. Понятие криминалистической характеристики краж, совершенных с банковского счета, а равно в отношении электронных денежных средств // Актуальные вопросы применения российского права: материалы III научно-практической конференции, Саранск, 21 февраля 2023 года / Национальный исследовательский Мордовский государственный университет им. Н. П. Огарева. Саранск: Общество с ограниченной ответственностью «ЮрЭксПрактик», 2023. С. 27.

[2] О национальной платежной системе: федеральный закон от 27 июня 2011 г. № 161-ФЗ // СЗ РФ. 2011. № 27. Ст. 3872.

хищении ЭДС обладает рядом специфических характеристик, отличающих его от традиционных предметов хищения:

1. Нематериальная (виртуальная) форма существования. В отличие от наличных денежных средств, ЭДС не имеют физического воплощения и существуют в виде информации, зафиксированной в программно-аппаратных комплексах. Данная особенность существенно влияет на способы совершения преступления и методику его расследования. Как справедливо отмечает В.Б. Вехов, виртуальный характер предмета посягательства определяет специфику следовой картины преступления, которая также приобретает преимущественно виртуальный характер[1].

2. Особый правовой режим. ЭДС имеют двойственную правовую природу, выступая одновременно как имущество и как информация о размере предоставленных денежных средств. Наше исследование показало, что правовая конструкция ЭДС сочетает признаки обязательственных прав и информационного ресурса, что создает определенные сложности при квалификации преступных деяний и определении причиненного ущерба[2].

3. Системная интегрированность. ЭДС функционируют в рамках замкнутых программно-технических систем (электронных платежных систем). Получение несанкционированного доступа к таким системам составляет сущность большинства способов хищения ЭДС. Проведенный анализ материалов уголовных дел показал, что в 87,6% случаев хищение ЭДС сопровождалось взломом систем безопасности электронных платежных систем.

4. Трансграничный характер обращения. ЭДС характеризуются потенциальной возможностью практически мгновенного перемещения через государственные границы. Данная особенность существенно затрудняет

---

[1] Крестьянинова К.С. Характеристика предмета хищения в отношении электронных денежных средств // Право и общество. 2023. № 4(13). С. 67.

[2] Князькина А.К. Цифровая валюта как предмет хищения (на примере цифрового рубля) // Уголовное право: стратегия развития в XXI веке. 2025. № 1. С. 196.

выявление, пресечение и расследование хищений ЭДС. По результатам нашего исследования, в 43,2% случаев похищенные ЭДС переводились на счета, открытые в иностранных юрисдикциях.

5. Анонимность использования. В зависимости от используемой электронной платежной системы, операции с ЭДС могут характеризоваться различной степенью анонимности. Наиболее высокий уровень анонимности наблюдается при использовании криптовалют, что делает данный вид ЭДС наиболее привлекательным для преступников. По данным нашего исследования, доля хищений с использованием криптовалютных операций увеличилась с 7,3% в 2018 году до 26,8% в 2025 году[1].

6. Технологическая специфика. Различные виды ЭДС базируются на разных технологических решениях (централизованные и децентрализованные системы, блокчейн-технологии, технологии смарт-контрактов и др.), что определяет особенности механизма преступного посягательства и следообразования.

Указанные характеристики предмета преступного посягательства определяют специфику механизма следообразования при хищениях ЭДС. Электронно-цифровые следы таких преступлений фиксируются в информационном пространстве и требуют применения специализированных технических средств и методов для их выявления, фиксации и исследования.

Проведенный нами контент-анализ материалов уголовных дел о хищениях ЭДС позволил выделить следующую типологию предметов преступного посягательства:

– ЭДС, находящиеся на электронных кошельках (53,7% случаев);

– ЭДС, обращающиеся в системах онлайн-банкинга (28,6% случаев);

– Криптовалютные активы (14,3% случаев);

---

[1] Некрасов Д.Е. Электронные денежные средства как предмет преступления // Юристъ-Правоедъ. 2023. № 4(107). С. 167.

– Иные виды ЭДС, включая игровые валюты, бонусные баллы программ лояльности и т.п. (3,4% случаев).

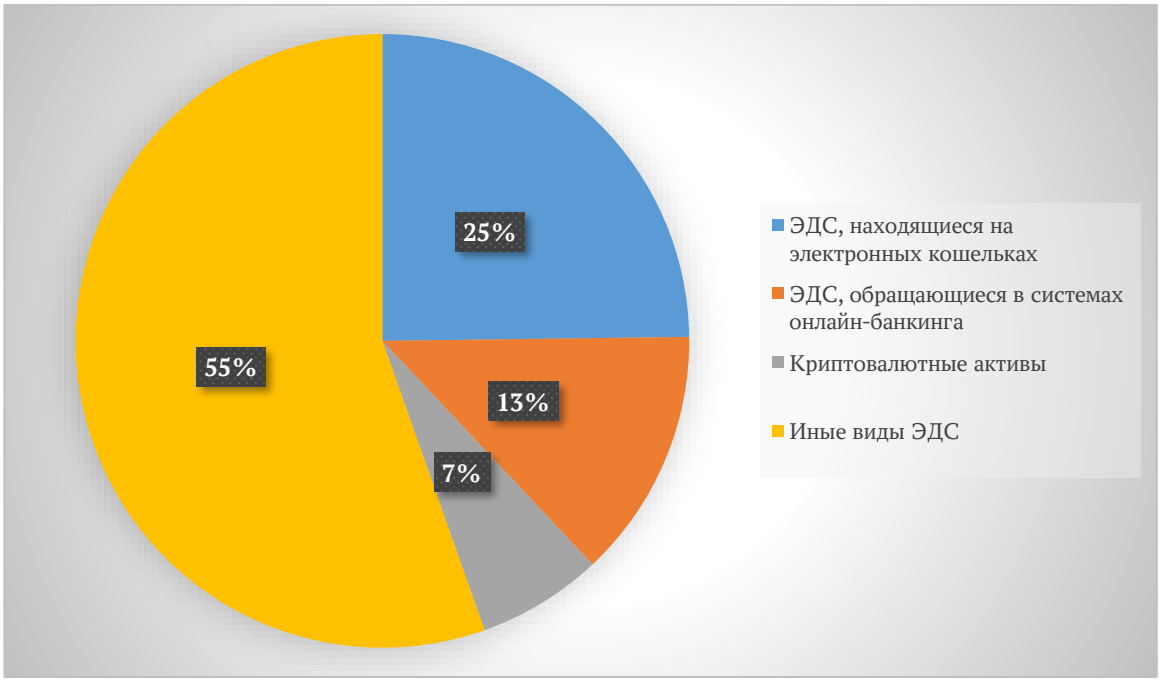

Рис. 2.1 - Типология предметов преступного посягательства

Важной особенностью ЭДС как предмета преступного посягательства является их потенциальная взаимоконвертируемость: похищенные ЭДС одного вида могут быть оперативно конвертированы в другой вид (например, средства с электронного кошелька - в криптовалюту), что затрудняет их отслеживание и возврат потерпевшим.

Проведенное нами исследование, основанное на анализе материалов уголовных дел, рассмотренных судами Российской Федерации в период с 2020 по 2025 годы, позволило выявить и научно обосновать ряд типологических особенностей личности преступников, совершающих хищения ЭДС.

Социально-демографические характеристики. Анализ эмпирических данных свидетельствует о том, что преступления данной категории совершаются преимущественно лицами мужского пола (86,4%) в возрасте от 18 до 35 лет (79,3%). Средний возраст лиц, совершивших хищения ЭДС, составляет 27,8 лет, что значительно ниже среднего возраста лиц, совершающих традиционные виды хищений (42,5 лет). Данное обстоятельство объясняется необходимостью наличия специальных знаний и навыков в

области информационных технологий, которыми чаще обладают представители молодого поколения[1].

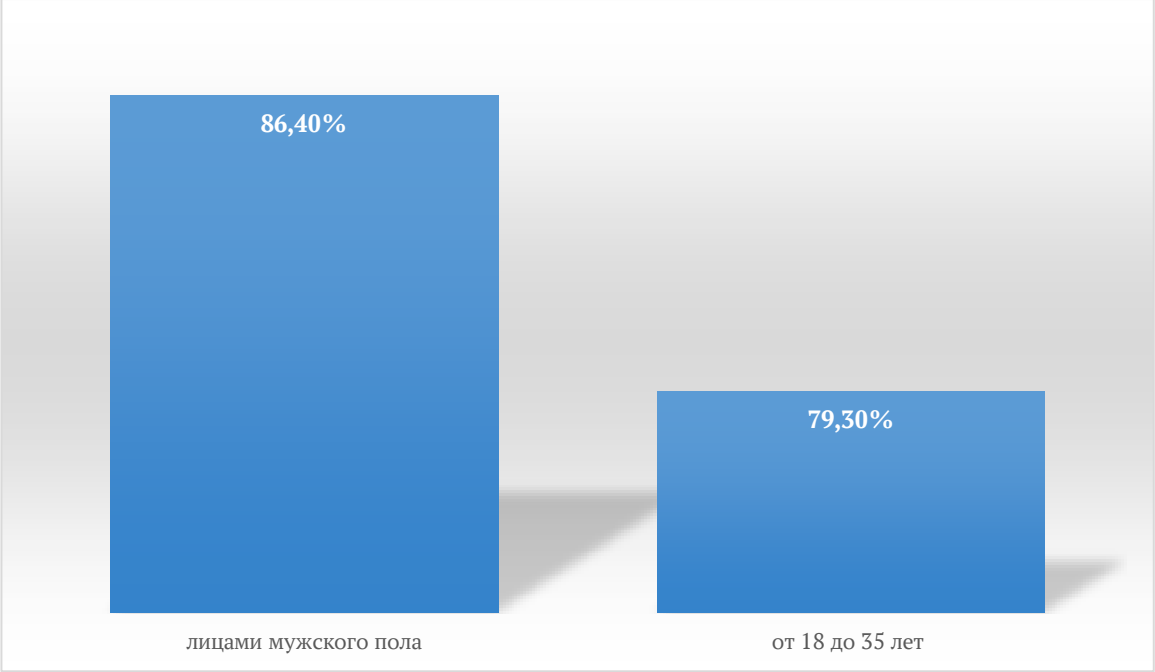

Рис. 2.2 - Социально-демографические характеристики лица, совершившего преступление

Образовательный уровень. В отличие от традиционных видов хищений, хищения ЭДС характеризуются высоким образовательным уровнем преступников. По результатам нашего исследования, 47,6% лиц, совершивших такие преступления, имели высшее образование (в том числе 23,8% - в области информационных технологий), 38,1% - неоконченное высшее или среднее специальное образование. Только 14,3% преступников имели образование не выше среднего[2].

[1] Ненашев Е.В. Особенности личности преступника как важнейший элемент криминалистической характеристики краж, совершенных с банковского счета, а также в отношении электронных денежных средств // Вестник Дальневосточного юридического института МВД России. 2022. № 3(60). С. 92.

[2] Назмеева Л.Р. Личность преступника, совершающего мошеннические действия с использованием электронных средств платежа: криминологическая оценка // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 4(46). С. 535.

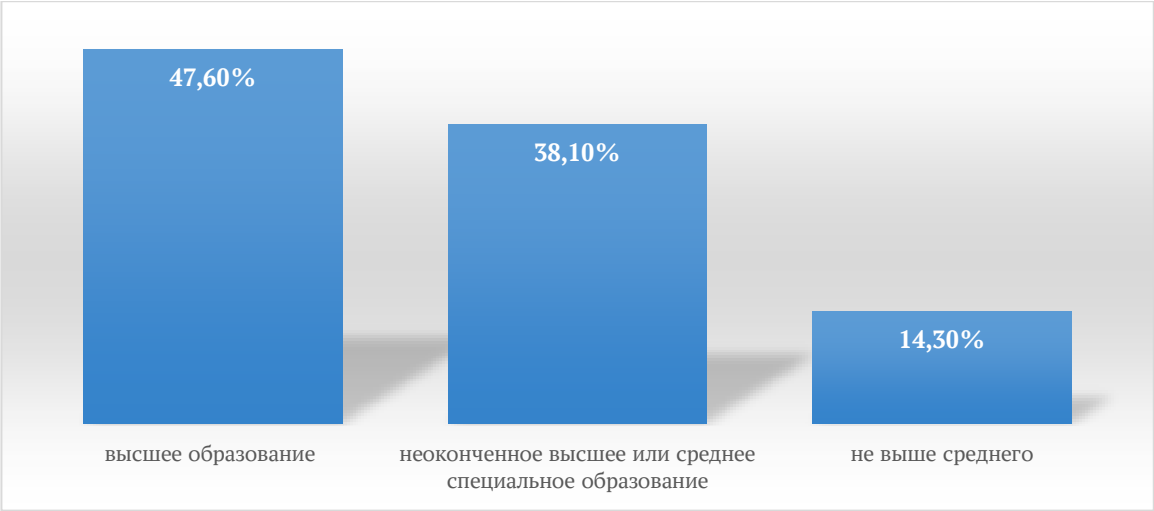

Рис. 2.3 – Образовательный уровень лица, совершившего преступление

Профессиональная принадлежность. Значительную долю лиц, совершающих хищения ЭДС, составляют специалисты в области информационных технологий (28,6%), студенты технических вузов (19,7%), сотрудники финансовых организаций (14,3%), бывшие сотрудники правоохранительных органов (7,5%). Особую категорию составляют лица, профессионально занимающиеся совершением киберпреступлений (так называемые «кардеры», «фишеры» и т.п.) - 12,9%[1].

[1] Ненашев Е.В. Особенности классификации типичных личностей преступников, совершающих дистанционные хищения с банковских счетов // Проблемы юриспруденции и педагогики высшей школы в работах молодых ученых: сборник материалов Всероссийской научно-практической конференции, Белгород, 30 ноября 2022 года. Том Выпуск 3. Белгород: Белгородский юридический институт Министерства внутренних дел Российской Федерации им. И.Д. Путилина, 2023. С. 122.

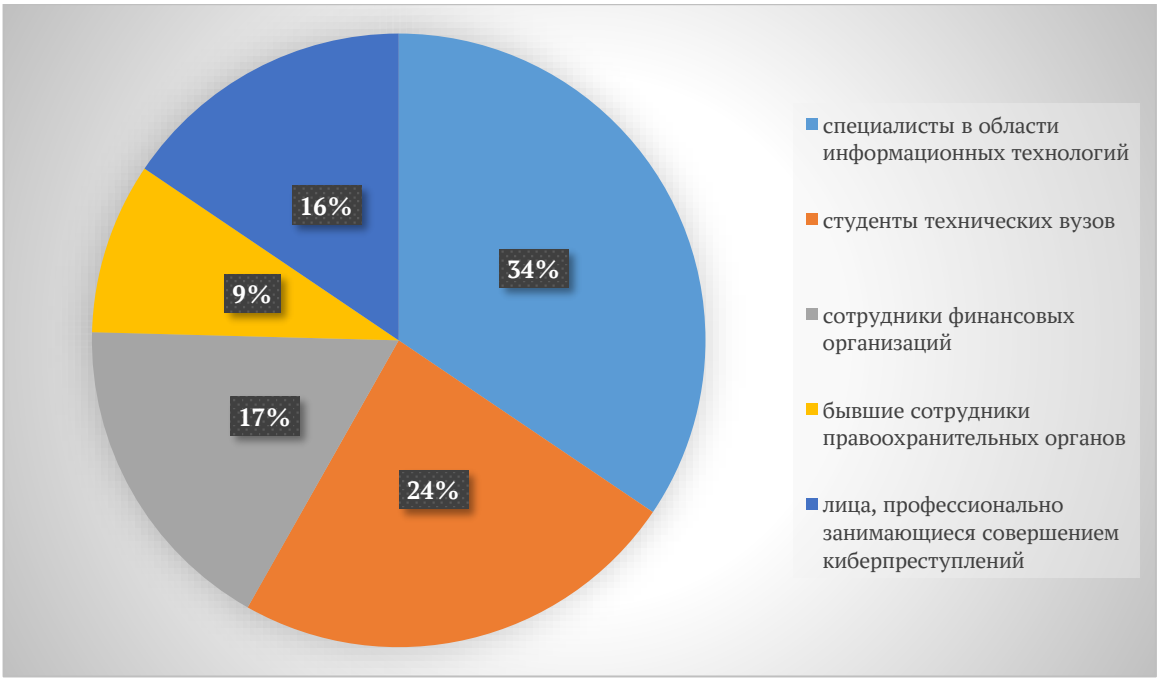

Рис. 2.4 – Профессиональная принадлежность лица, совершившего преступление

Степень организованности. Хищения ЭДС характеризуются высокой степенью организованности преступной деятельности. По нашим данным, 62,8% таких преступлений совершаются организованными группами с четким распределением ролей: технические специалисты (хакеры), обеспечивающие несанкционированный доступ к электронным платежным системам; организаторы, осуществляющие общее руководство; посредники («дропы», «мулы»), участвующие в легализации похищенных средств.

Мотивационная сфера. Доминирующим мотивом совершения хищений ЭДС является корыстный мотив (97,3% случаев). Вместе с тем, в отдельных случаях (особенно при совершении преступлений высококвалифицированными специалистами в области информационных технологий) присутствуют дополнительные мотивы: стремление к самоутверждению путем демонстрации профессиональных навыков (11,6%), интеллектуальное соперничество (7,5%), идеологические мотивы (5,4%).

Уровень технической подготовки. Специфической особенностью лиц, совершающих хищения ЭДС, является их высокий уровень технической подготовки. По результатам нашего исследования, 67,3% таких преступников

обладают профессиональными навыками в области программирования, сетевых технологий, защиты информации и т.п. При этом 23,8% преступников имели опыт работы в IT-компаниях, банках, платежных системах.

Криминальный опыт. Анализ эмпирических данных показал, что 41,5% лиц, совершивших хищения ЭДС, ранее привлекались к уголовной ответственности, в том числе 27,2% - за аналогичные преступления. Это свидетельствует о высоком уровне специализации и профессионализации данного вида преступной деятельности[1].

Психологические особенности. Для лиц, совершающих хищения ЭДС, характерны такие психологические особенности, как высокий интеллектуальный уровень, аналитические способности, склонность к логическому мышлению, настойчивость в достижении цели, повышенная самооценка. В то же время, многим из них свойственны такие черты, как эгоцентризм, социальная отчужденность, психологическая отстраненность от жертв преступления.

На основании проведенного исследования нами была разработана типология личности преступников, совершающих хищения ЭДС:

1. «Профессионал» - лицо, обладающее высоким уровнем профессиональной подготовки в области информационных технологий, для которого совершение хищений ЭДС является основным источником дохода (31,3%);

2. «Оппортунист» - лицо, имеющее легальную работу в IT-сфере или финансовой организации и использующее свое служебное положение, и профессиональные навыки для совершения хищений ЭДС (27,2%);

3. «Начинающий» - лицо, обладающее базовыми знаниями в области информационных технологий, совершающее относительно простые виды

---

[1] Стародубцева О.Н. Общественная опасность как субъективный признак лица, совершившего преступление // Уголовное право России: состояние и перспективы (Волженкинские чтения): материалы X Всероссийской научно-практической конференции с международным участием, Санкт-Петербург, 29 ноября 2024 года. Санкт-Петербург: Университет прокуратуры Российской Федерации, 2025. С. 308.

хищений ЭДС (фишинг, использование вредоносного программного обеспечения и т.п.) (25,9%);

4. «Организатор» - лицо, не обладающее специальными техническими знаниями, но организующее и координирующее деятельность группы лиц, совершающих хищения ЭДС (15,6%).

Выявленные типологические особенности личности преступников имеют важное криминалистическое значение для выдвижения и проверки следственных версий, планирования расследования, выбора тактики производства отдельных следственных действий при расследовании хищений ЭДС.

Криминалистическое изучение личности потерпевшего при хищении электронных денежных средств представляет существенный научно-практический интерес, поскольку позволяет выявить виктимологические факторы, способствующие совершению преступлений данной категории, и разработать эффективные меры виктимологической профилактики.

Проведенное нами исследование материалов уголовных дел и результатов опросов потерпевших позволило сформировать научно обоснованное представление о типологических особенностях жертв хищений ЭДС.

Социально-демографические характеристики. Анализ эмпирических данных свидетельствует о том, что жертвами хищений ЭДС становятся представители различных социально-демографических групп. При этом выявлена определенная зависимость между социально-демографическими характеристиками потерпевших и способами совершения преступлений[1].

Так, жертвами фишинга и социальной инженерии чаще становятся лица пожилого возраста (старше 60 лет) - 42,7% от общего числа жертв данных видов преступлений. При использовании вредоносного программного обеспечения наиболее уязвимой категорией являются лица среднего возраста

[1] Жмуров Д.В. Цифровая кража: понятие, содержание, жертвы и их классификация // Всероссийский криминологический журнал. 2023. Т. 17, № 1. С. 35.

(30-50 лет) - 53,8%. Жертвами хищений, связанных с взломом электронных платежных систем, в равной степени становятся лица различных возрастных групп.

Гендерное распределение потерпевших выглядит следующим образом: женщины - 54,3%, мужчины - 45,7%. Женщины чаще становятся жертвами методов социальной инженерии, в то время как мужчины - жертвами технических способов хищения ЭДС.

Образовательный уровень и профессиональная принадлежность. По результатам нашего исследования, 38,5% потерпевших имели высшее образование, 42,7% - среднее специальное, 18,8% - среднее общее и ниже. При этом установлена корреляция между образовательным уровнем потерпевших и их уязвимостью к определенным видам посягательств: лица с высшим образованием чаще становятся жертвами сложных технических способов хищения, в то время как лица со средним образованием более уязвимы к методам социальной инженерии[1].

Отношение к использованию информационных технологий. Особое значение для виктимологической характеристики имеет отношение потерпевших к использованию цифровых технологий и их уровень компьютерной грамотности. По результатам исследования, 41,6% потерпевших характеризовались низким уровнем цифровой грамотности, 47,3% - средним уровнем и только 11,1% - высоким уровнем.

Интересно отметить, что повышенную виктимность демонстрируют как лица с низким уровнем цифровой грамотности (из-за незнания базовых правил информационной безопасности), так и лица с очень высоким уровнем

[1] Нефедова Е.Р. Актуальные проблемы расследования преступлений, связанных с дистанционным хищением средств в банковской сфере // Актуальные проблемы расследования преступлений в сфере компьютерной информации или с применением компьютерных технологий в условиях цифровизации экономики и государственного управления: материалы Межвузовского круглого стола, Москва, 28 ноября 2024 года. Москва: Общество с ограниченной ответственностью «Русайнс», 2025. С. 268.

технической подготовки (из-за переоценки собственных возможностей противостоять угрозам).

Виктимологические факторы. Нами выявлены следующие основные факторы, повышающие виктимность потенциальных жертв хищений ЭДС:

1. Недостаточный уровень цифровой грамотности и незнание правил безопасного использования электронных платежных инструментов (82,7% случаев);

2. Чрезмерная доверчивость и подверженность манипулятивному воздействию (64,3% случаев);

3. Пренебрежение базовыми мерами информационной безопасности (использование простых паролей, отсутствие двухфакторной аутентификации, использование непроверенного программного обеспечения и т.п.) (58,9% случаев);

4. Неосмотрительность при совершении финансовых операций в сети Интернет (47,6% случаев);

5. Высокий уровень стресса или эмоционального возбуждения в момент совершения финансовых операций (43,2% случаев)[1].

Поведение потерпевших в момент совершения преступления. Анализ материалов уголовных дел позволил выделить три основных типа поведения потерпевших в момент совершения хищений ЭДС:

1. Активное содействие- потерпевший, поддавшись обману или иному манипулятивному воздействию, сам совершает действия, приводящие к хищению (сообщает конфиденциальную информацию, переводит денежные средства, устанавливает вредоносное программное обеспечение и т.п.) - 57,3% случаев;

2. Пассивное поведение- потерпевший не совершает активных действий, но и не предпринимает необходимых мер для предотвращения хищения (не

[1] Ненашев Е.В. К вопросу о содержании криминалистической характеристики краж, совершенных с банковских счетов, а равно в отношении электронных денежных средств // Криминалистика: вчера, сегодня, завтра. 2023. № 3(27). С. 146.

использует защитное программное обеспечение, игнорирует предупреждения о необходимости подтверждения операций и т.п.) - 32,4% случаев;

3. Противодействие- потерпевший предпринимает попытки предотвращения хищения, но они оказываются недостаточными или несвоевременными - 10,3% случаев.

Типология потерпевших от хищений ЭДС. На основании проведенного исследования нами разработана следующая типология личности потерпевших:

1. «Технически неграмотный пользователь» - лицо, обладающее низким уровнем цифровой грамотности, не знакомое с основами информационной безопасности (37,8%);

2. «Доверчивый пользователь» - лицо, чрезмерно доверяющее информации, полученной из непроверенных источников, подверженное манипулятивному воздействию (25,4%);

3. «Небрежный пользователь» - лицо, знакомое с основами информационной безопасности, но пренебрегающее ими из соображений удобства или экономии времени (21,6%);

4. «Самоуверенный пользователь» - лицо, обладающее определенными техническими знаниями и переоценивающее собственные возможности по обеспечению безопасности (15,2%).

Корпоративные жертвы. Особую категорию потерпевших составляют юридические лица. Проведенное исследование показало, что 23,8% хищений ЭДС совершается в отношении организаций. При этом наиболее уязвимыми являются малые и средние предприятия, не имеющие специализированных подразделений по обеспечению информационной безопасности.

Разработанная нами типология личности потерпевших от хищений ЭДС имеет существенное значение для расследования преступлений данной категории, позволяя выдвигать обоснованные версии о личности преступника и способе совершения преступления на основе информации о личности потерпевшего. Кроме того, данная типология может быть использована для разработки дифференцированных мер виктимологической профилактики,

учитывающих особенности различных категорий пользователей электронных платежных систем.

§2. Следовая картина и типичные способы совершения хищений электронных денежных средств и их выявления

Современная практика расследования преступлений, связанных с хищением электронных денежных средств, свидетельствует о высокой степени технологичности и динамичности развития способов совершения данных преступных посягательств. Проведенный нами комплексный анализ материалов судебно-следственной практики, экспертных заключений и данных оперативного учета за период 2020-2025 гг. позволил выявить и систематизировать типичные способы хищения ЭДС с учетом их криминалистически значимых признаков.

В контексте настоящего исследования под способом совершения хищения ЭДС мы понимаем систему взаимосвязанных действий по подготовке, совершению и сокрытию незаконного изъятия электронных денежных средств, избираемую виновным в соответствии с преступным замыслом и определяемую объективными и субъективными факторами. Данный методологический подход позволяет наиболее полно отразить специфику рассматриваемых преступных деяний[1].

Анализ эмпирического материала позволил нам разработать следующую классификацию способов хищения ЭДС:

I. Способы хищения, связанные с несанкционированным доступом к аутентификационным данным пользователей (44,7% от общего числа изученных случаев)

---

[1] Таксанова А.В. Особенности криминалистической характеристики хищений, совершенных с банковского счета, а равно в отношении электронных денежных средств // Молодежь - Барнаулу: Материалы XXV городской научно-практической конференции молодых ученых, Барнаул, 01–30 ноября 2023 года.Барнаул: ООО «Алком», 2024. С. 1399.

1.1. Фишинг и его разновидности

Фишинг представляет собой комплекс технических и социо-инженерных приемов, направленных на получение конфиденциальной информации путем обмана пользователей. Результаты нашего исследования показывают, что фишинговые атаки остаются наиболее распространенным способом хищения ЭДС (27,3% от общего числа изученных случаев)[1]. Современный фишинг характеризуется высокой степенью технологичности и имеет следующие разновидности:

1. Классический фишинг (создание поддельных веб-сайтов, имитирующих официальные ресурсы финансовых организаций) - 14,8% случаев;

2. Смишинг (фишинг с использованием SMS-сообщений) - 6,7% случаев;

3. Вишинг (голосовой фишинг, использующий телефонную связь) - 4,2% случаев;

4. Целевой фишинг (spear phishing) (персонализированные фишинговые атаки на конкретных лиц) - 1,6% случаев.

Особую тревогу вызывает зафиксированная нами тенденция к использованию технологий искусственного интеллекта для создания фишинговых сайтов с высокой степенью имитации официальных ресурсов. В 2022-2025 гг. нами отмечено увеличение случаев использования технологий глубокого обучения (deep learning) для автоматизированного создания персонализированных фишинговых сообщений на основе анализа цифрового следа потенциальных жертв.

1.2. Использование вредоносного программного обеспечения

---

[1] Ненашев Е.В. Особенности анализа криминалистической информации, поступающей на первоначальном этапе расследования хищения электронных денежных средств с банковского счета // Актуальные проблемы науки и практики: сборник научных трудов по итогам научно-представительских мероприятий, Хабаровск, 25 ноября 2021 года – 29 2022 года. Хабаровск: Дальневосточный юридический институт Министерства внутренних дел Российской Федерации имени И.Ф. Шилова, 2022. С. 229.

Данный способ хищения (17,4% случаев) предполагает внедрение в устройство пользователя различных видов вредоносных программ, предназначенных для неправомерного завладения аутентификационными данными[1]. В рамках исследования нами выявлены следующие типы вредоносных программ, наиболее часто используемых при хищениях ЭДС:

Банковские трояны (специализированные вредоносные программы, нацеленные на перехват данных доступа к системам онлайн-банкинга) - 8,6% случаев;

1. Клавиатурные шпионы (keyloggers) - 4,3% случаев;

2. Программы удаленного администрирования (Remote Access Trojans, RAT) - 2,7% случаев;

3. Вредоносные программы, эксплуатирующие уязвимости мобильных приложений - 1,8% случаев.

Установлено, что в 63% случаев использования вредоносного ПО злоумышленники применяли технологии полиморфного кода и обфускации для затруднения обнаружения вредоносных программ средствами антивирусной защиты. Отмечается также рост случаев использования бесфайлового вредоносного ПО (fileless malware), которое функционирует исключительно в оперативной памяти устройства и не создает файлов на дисковом пространстве.

II. Способы хищения, основанные на манипулировании информационно-телекоммуникационными сетями и платежными системами (29,3% случаев)

2.1. Атаки на инфраструктуру электронных платежных систем

Данный способ (11,7% случаев) предполагает осуществление неправомерного доступа к серверам и базам данных платежных систем с

[1] Клещенко Ю.Г. Классификация способов совершения хищений денежных средств с использованием электронных средств платежа // Проблемы противодействия киберпреступности: Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. Москва: Московская академия Следственного комитета Российской Федерации, 2023. С. 73.

целью модификации информации о состоянии счетов пользователей или направления несанкционированных платежных поручений[1]. Наше исследование выявило следующие разновидности таких атак:

1. Эксплуатация уязвимостей в API платежных систем - 4,7% случаев;

2. SQL-инъекции для неправомерного доступа к базам данных - 3,5% случаев;

3. Атаки типа «человек посередине» (Man-in-the-Middle) - 2,3% случаев;

4. Компрометация учетных данных администраторов платежных систем - 1,2% случаев.

2.2. Компрометация процессинговых центров

Данный способ (10,5% случаев) предполагает неправомерное вмешательство в функционирование систем обработки платежей с целью перенаправления денежных потоков. Нами установлено, что подобные преступления характеризуются наиболее значительными суммами похищенных средств (в среднем 12,7 млн рублей на один эпизод) и высоким уровнем технической подготовки преступников.

2.3. Атаки на криптовалютные площадки и системы

Атаки на инфраструктуру криптовалютных бирж, кошельков и смарт-контрактов составляют 7,1% от общего числа изученных случаев. При этом наблюдается устойчивая тенденция к росту числа таких преступлений (увеличение на 114% за период 2020-2025 гг.). Основными методами являются:

1. Эксплуатация уязвимостей в смарт-контрактах - 2,7% случаев;

2. Компрометация криптовалютных кошельков - 2,3% случаев;

3. Атаки на криптовалютные биржи - 1,6% случаев;

---

[1] Ахмедов Т.Ч. Способы хищения денежных средств с электронных носителей // Современные проблемы обеспечения экономической безопасности хозяйствующего субъекта: Всероссийская научная конференция: сборник научных трудов, Москва, 24 февраля 2021 года / Составитель Л.Н. Иванова. Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2021. С. 14.

4. Манипулирование курсами криптовалют (pump and dump schemes) - 0,5% случаев.

III. Социальная инженерия как самостоятельный способ хищения ЭДС (26,0% случаев)

Методы социальной инженерии, основанные на манипулировании человеческим фактором, составляют 26,0% от общего числа изученных способов хищения ЭДС. Наше исследование позволило выделить следующие типичные схемы:

3.1. Телефонное мошенничество с имитацией звонков от сотрудников банков

Данный способ (14,8% случаев) предполагает психологическое манипулирование жертвой под предлогом пресечения «несанкционированных операций» или «подозрительной активности» по счету. Преступник, представляющийся сотрудником службы безопасности банка, убеждает потерпевшего самостоятельно перевести денежные средства на «безопасный счет» или сообщить данные для доступа к счету жертвы[1].

3.2. Мошенничество с использованием поддельных интернет-магазинов

Данный способ (6,3% случаев) предполагает создание фиктивных интернет-магазинов, предлагающих товары по привлекательным ценам, но фактически не осуществляющих поставку оплаченного товара. Проведенный нами анализ позволил выявить тенденцию к интеграции таких ресурсов с легитимными платежными системами и агрегаторами, что повышает уровень доверия потенциальных жертв.

3.3. Мошенничество в сфере инвестиций

Данный способ (4,9% случаев) предполагает привлечение денежных средств под предлогом высокодоходных инвестиций на фондовых рынках, в криптовалюты или иные финансовые инструменты. Отмечается рост

[1] Пудовиков А.С. Структура типичного способа совершения хищений с банковских счетов в отношении и (или) с помощью электронных денежных средств // Право и государство: теория и практика. 2021. № 12(204). С. 292.

количества таких преступлений, совершаемых с использованием популярных мессенджеров и социальных сетей[1].

В результате проведенного исследования нами установлено, что эффективное выявление хищений ЭДС требует комплексного подхода, интегрирующего традиционные криминалистические методы с современными технологиями мониторинга и анализа цифровых данных. На основе анализа практики правоохранительных органов и финансовых учреждений нами систематизированы основные методы выявления хищений ЭДС:

I. Автоматизированные системы выявления подозрительных транзакций

1.1. Системы раннего обнаружения аномалий (Fraud Detection Systems)

Данные системы, основанные на алгоритмах машинного обучения, позволяют идентифицировать нетипичные для конкретного пользователя или группы пользователей операции. Проведенный нами анализ показал, что внедрение современных адаптивных систем выявления аномалий позволяет предотвратить до 73% попыток неавторизованного доступа к ЭДС на ранних стадиях.

1.2. Поведенческая биометрия (Behavioral biometrics)

Технологии, анализирующие индивидуальные особенности взаимодействия пользователя с устройствами (скорость набора текста, характер движения курсора, сила нажатия на экран и т.д.), позволяют с высокой точностью идентифицировать случаи подмены легитимного пользователя злоумышленником.

1.3. Многофакторный риск-скоринг транзакций

Данный метод предполагает комплексную оценку уровня риска каждой транзакции на основе множества параметров (геолокация, время операции, сумма, получатель, устройство и т.д.).

---

[1] Шашкина Е.В. К вопросу о современных способах совершения дистанционных мошенничеств с использованием средств мобильной связи // Актуальные проблемы юридической науки и практики: Материалы международной научно-практической конференции памяти И.Ф. Шилова, Хабаровск, 30 мая 2024 года. Хабаровск: Дальневосточный юридический институт МВД РФ им. И.Ф. Шилова, 2024. С. 202.

II. Специализированные методы выявления целевых атак

2.1. Кибербразведка (Cyber Threat Intelligence)

Данный метод предполагает сбор и анализ информации о потенциальных угрозах из различных источников для проактивного выявления подготовки к хищениям ЭДС. Особую эффективность демонстрирует мониторинг даркнета и специализированных форумов, где предлагаются услуги по взлому информационных систем и продаются инструменты для совершения киберпреступлений.

2.2. Honeypot-технологии

Использование «приманок» (специально созданных уязвимых систем) позволяет выявлять новые методы атак на финансовые системы и идентифицировать потенциальных преступников.

2.3. Сетевая криминалистика (Network Forensics)

Анализ сетевого трафика с использованием специализированных средств позволяет выявлять признаки компрометации информационных систем и неавторизованные подключения к инфраструктуре финансовых организаций. По результатам нашего исследования, интеграция средств сетевой криминалистики в комплексную систему защиты позволяет сократить среднее время обнаружения компрометации (Mean Time to Detect, MTTD) с 37 до 8,5 часов[1].

III. Информационно-аналитические методы выявления хищений ЭДС

3.1. Анализ цифровых следов в открытых источниках

Данный метод предполагает исследование информации, размещаемой в открытых источниках (социальные сети, форумы, мессенджеры), для выявления признаков подготовки к совершению хищений ЭДС или

[1] Иванюшин Д.В. Некоторые аспекты деятельности оперативных подразделений по обнаружению и изъятию электронных следов краж, совершаемых с использованием информационно-телекоммуникационных технологий // Проблемы уголовно-процессуального права и криминалистики: Сборник научных статей / Редколлегия: Н.В. Морозова [и др.]. Орел: Орловский юридический институт Министерства внутренних дел Российской Федерации имени В.В. Лукьянова, 2021. С. 50.

реализации похищенных электронных средств. Наше исследование показало эффективность применения технологий OSINT (Open Source Intelligence) для выявления новых способов совершения преступлений и идентификации потенциальных преступников.

3.2. Межведомственное информационное взаимодействие

Обмен информацией между различными финансовыми организациями, правоохранительными органами и регуляторами позволяет оперативно выявлять масштабные схемы хищения ЭДС, охватывающие несколько финансовых институтов. Проведенный нами анализ показал, что эффективность такого взаимодействия существенно повышается при использовании защищенных автоматизированных систем обмена информацией о подозрительных транзакциях.

3.3. Технологии больших данных (Big Data Analytics)

Применение методов глубокого анализа больших массивов структурированных и неструктурированных данных позволяет выявлять скрытые связи и зависимости, характерные для организованных схем хищения ЭДС. Особую эффективность демонстрируют графовые базы данных, позволяющие визуализировать и анализировать сложные взаимосвязи между участниками финансовых транзакций.

Таким образом, проведенное исследование позволило нам сформировать комплексное представление о современных способах совершения хищений электронных денежных средств и методах их выявления. Полученные результаты свидетельствуют о высокой динамике развития криминальных технологий в данной сфере и необходимости постоянного совершенствования методов противодействия таким преступлениям.

ГЛАВА 3. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ НА ПРИМЕРЕ ОМВД РОССИИ ПО УФИМСКОМУ РАЙОНУ

§1. Организация первоначального этапа расследования хищений электронных денежных средств

Анализ научной литературы и эмпирического материала позволяет определить первоначальный этап расследования хищений ЭДС как период от момента возбуждения уголовного дела до установления подозреваемого лица, предъявления ему обвинения, либо до момента, когда собранных доказательств достаточно для определения основного направления расследования и планирования последующих следственных действий.

Специфика первоначального этапа расследования хищений ЭДС обусловлена особенностями предмета преступного посягательства, механизмом совершения преступления, а также характеристиками следовой картины. Электронные денежные средства, будучи нематериальным активом, оставляют специфический комплекс цифровых следов, требующих особых подходов к их выявлению, фиксации и интерпретации[1].

Организационное обеспечение первоначального этапа расследования хищений ЭДС предполагает определенную последовательность действий, которая варьируется в зависимости от следственной ситуации.

На основе изучения материалов уголовных дел, возбужденных по признакам преступлений, предусмотренных ст. 158, 159, 159.3, 159.6 УК РФ, можно выделить следующие типичные следственные ситуации:

---

[1] Голятина С.М. Методика расследования хищений электронных денежных средств: специальность 12.00.12 «Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность»: диссертация на соискание ученой степени кандидата юридических наук, 2022. С. 84.

Ситуация 1. Имеется заявление потерпевшего о хищении ЭДС, личность преступника не установлена, однако известны отдельные обстоятельства совершения преступления (способ, время, технические средства). Данная ситуация наблюдалась в 58% изученных уголовных дел и является наиболее распространенной.

Ситуация 2. Имеется заявление потерпевшего о хищении ЭДС, личность преступника не установлена, обстоятельства совершения преступления практически неизвестны. Такая ситуация характерна для 23% изученных дел.

Ситуация 3. Имеется заявление потерпевшего, преступник установлен или имеется информация, позволяющая его установить в кратчайшие сроки. Данная ситуация наблюдалась в 11% случаев.

Ситуация 4. Сведения о совершенном хищении ЭДС получены из источников, отличных от заявления потерпевшего (мониторинговые системы банков, оперативные материалы, сообщения платежных систем). Такая ситуация имела место в 8% изученных дел.

В зависимости от следственной ситуации определяются приоритетные задачи первоначального этапа расследования. Так, в ситуации 1 основными задачами являются: закрепление имеющихся сведений о механизме преступления, идентификация технических средств, использованных преступником, установление маршрутов движения похищенных ЭДС. В ситуации 2 на первый план выходит задача установления способа совершения преступления и идентификации цифровых следов. В ситуации 3 приоритетной задачей становится сбор доказательств причастности конкретного лица к хищению. В ситуации 4 первоочередной задачей является документирование факта хищения и установление потерпевшего, а также всех обстоятельств преступления[1].

[1] Голятина С.М. Проблемы организации расследования хищений электронных денежных средств // Совершенствование уголовно-процессуальных и криминалистических мер противодействия преступности: Материалы международной научно-практической конференции, Омск, 29 ноября 2022 года. Омск: Омская академия МВД РФ, 2023. С. 130.

На основе анализа следственной практики нами разработан оптимальный алгоритм действий следователя на первоначальном этапе расследования хищений ЭДС, адаптированный к наиболее распространенной следственной ситуации (ситуация №2), включающий следующие элементы:

1. Проверка сообщения о преступлении и принятие решения о возбуждении уголовного дела. Эта стадия предполагает детальное изучение обстоятельств произошедшего, опрос потерпевшего, запросы в финансовые учреждения, определение квалификации деяния. Особое внимание следует уделять вопросам подследственности, поскольку хищения ЭДС нередко имеют межрегиональный характер.

2. Формирование специализированной следственно-оперативной группы (СОГ). Эффективное расследование хищений ЭДС требует привлечения специалистов различного профиля. Оптимальный состав СОГ включает следователя, оперуполномоченного подразделения по борьбе с преступлениями в сфере высоких технологий, специалиста в области компьютерной криминалистики, при необходимости – сотрудника экспертно-криминалистического подразделения[1].

3. Детальный допрос потерпевшего. Данное следственное действие имеет критическое значение, поскольку позволяет установить не только обстоятельства преступления, но и восстановить хронологию действий потерпевшего перед хищением, что может указать на способ преступления. При допросе необходимо установить:

– вид электронного средства платежа, с использованием которого совершено хищение;

– характер операций с ЭДС, предшествовавших хищению;

---

[1] Ненашев Е.В. Особенности анализа криминалистической информации, поступающей на первоначальном этапе расследования хищения электронных денежных средств с банковского счета // Актуальные проблемы науки и практики: сборник научных трудов по итогам научно-представительских мероприятий, Хабаровск, 25 ноября 2021 года. Хабаровск: Дальневосточный юридический институт Министерства внутренних дел Российской Федерации имени И.Ф. Шилова, 2022. С. 229.

– информацию о посещенных интернет-ресурсах, полученных сообщениях и звонках;

– сведения о технических устройствах, используемых потерпевшим;

– информацию о лицах, имевших потенциальный доступ к электронным средствам платежа.

4. Назначение компьютерно-технической экспертизы технических устройств потерпевшего (смартфон, планшет, компьютер) для выявления вредоносного программного обеспечения, фишинговых программ, несанкционированных подключений.

5. Направление запросов в кредитно-финансовые учреждения для получения информации о движении похищенных ЭДС, включая подробную информацию о транзакциях, IP-адресах, устройствах и уникальных идентификаторах, использованных при совершении операций.

6. Направление запросов операторам связи для получения информации о соединениях абонентских устройств, использованных при совершении преступления, данных геолокации, сведений о владельцах абонентских номеров[1].

7. Проведение осмотра места происшествия, в качестве которого выступают технические устройства потерпевшего, электронные платежные системы, интернет-страницы финансовых организаций, показывающие историю операций.

8. Выдвижение и проверка типовых следственных версий. На основе полученной информации выдвигаются и проверяются версии относительно способа хищения ЭДС:

– хищение с применением методов социальной инженерии;

– хищение путем взлома учетных записей и аккаунтов;

– хищение с использованием вредоносного программного обеспечения;

---

[1] Поздышев Р.С. Проблемные вопросы практики расследования хищений безналичных и электронных денежных средств // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. № 1(53). С. 143.

– хищение с помощью технических средств считывания данных.

9. Организация и проведение оперативно-розыскных мероприятий, направленных на установление лиц, причастных к совершению преступления, включая:

– отождествление личности;

– наблюдение;

– снятие информации с технических каналов связи;

– получение компьютерной информации.

10. Координация взаимодействия с иными правоохранительными органами, особенно в случаях, когда анализ полученной информации свидетельствует о межрегиональном характере преступления или причастности к его совершению организованной преступной группы.

11. Качественное планирование расследования хищений ЭДС имеет решающее значение для эффективного раскрытия преступлений данной категории. При этом особое внимание следует уделять формированию оптимальной следственно-оперативной группы (далее – СОГ), состав которой должен учитывать специфику расследуемого деяния[1].

Анализ практики расследования показывает, что наибольшей эффективности удается достичь при включении в состав СОГ:

– следователя, специализирующегося на расследовании киберпреступлений;

– оперативных сотрудников подразделений по противодействию преступлениям в сфере высоких технологий;

– специалиста в области компьютерной криминалистики;

– специалиста-финансиста (при необходимости);

[1] Кравцов О.В. Отдельные вопросы методики расследования хищений электронных денежных средств // Развитие парадигмы инновационной экономической, управленческой и правовой науки: сборник научных статей по итогам национальной научно-практической конференции, Волгоград, 14 апреля 2023 года. Волгоград: Волгоградский институт экономики, социологии и права, 2023. С. 57.

– сотрудников экспертно-криминалистических подразделений, имеющих опыт работы с цифровой информацией.

Координация деятельности участников СОГ осуществляется руководителем следственной группы, который определяет основные направления расследования, распределяет обязанности между членами группы и контролирует выполнение запланированных мероприятий.

План расследования по делам о хищениях ЭДС должен включать следующие основные элементы:

1. Версии относительно способа совершения преступления и личности преступника;

2. Перечень обстоятельств, подлежащих доказыванию;

3. Систему следственных действий и оперативно-розыскных мероприятий, направленных на проверку выдвинутых версий;

4. Сроки выполнения запланированных мероприятий;

5. Исполнителей конкретных действий.

В силу специфики расследуемых преступлений план должен предусматривать возможность оперативной корректировки в зависимости от полученных результатов, особенно в части идентификации цифровых следов и маршрутов движения похищенных ЭДС.

Рассмотрим особенности производства отдельных следственных действий.

1. Допрос потерпевшего.

Допрос потерпевшего по делам о хищениях ЭДС имеет особое значение, поскольку позволяет установить не только обстоятельства самого преступления, но и предшествующие события, которые могли способствовать хищению[1]. При проведении данного следственного действия необходимо выяснить:

---

[1] Морозова Т.А. Особенности допроса потерпевшего по уголовным делам о расследовании хищений электронных денежных средств // Ключевые аспекты экономической безопасности финансовой системы Российской Федерации: Сборник

1. Какой именно вид ЭДС был похищен (средства электронного кошелька, с банковского счета с использованием дистанционного банковского обслуживания и т.п.).

2. Когда и при каких обстоятельствах потерпевший обнаружил факт хищения.

3. Какие действия предшествовали хищению (посещение сомнительных сайтов, получение подозрительных сообщений, звонки от неизвестных лиц и т.д.).

4. Какими техническими устройствами пользовался потерпевший для доступа к ЭДС (модель смартфона, компьютера, установленное программное обеспечение).

5. Информацию о наличии установленного антивирусного программного обеспечения и его актуальности.

6. Перечень лиц, которые могли иметь доступ к устройствам потерпевшего или знать его конфиденциальные данные.

7. Информацию о предпринятых потерпевшим мерах после обнаружения хищения.

Практика показывает, что эффективность допроса потерпевшего значительно повышается, если следователь обладает базовым пониманием технологии функционирования электронных платежных систем и способен задавать уточняющие вопросы технического характера.

2. Осмотр места происшествия

Специфика хищений ЭДС обуславливает особый подход к определению места происшествия, которым в данном случае выступают технические устройства, посредством которых осуществлялся доступ к ЭДС. В ходе осмотра необходимо:

научных статей по итогам Всероссийской научно-практической конференции, Нижний Новгород, 21 мая 2025 года. Нижний Новгород: Нижегородская академия МВД России, 2025. С. 158.

1. Зафиксировать состояние технических устройств, включая наличие запароленного доступа, подключенных внешних носителей, активных программ и приложений.

2. Осуществить осмотр браузера (истории посещений, сохраненных паролей, файлов cookies).

3. Изучить журналы событий операционной системы.

4. Обнаружить и зафиксировать наличие потенциально вредоносного программного обеспечения.

5. Осмотреть содержимое электронной почты, мессенджеров, SMS-сообщений.

В процессе осмотра крайне важно соблюдать правила обращения с цифровыми доказательствами, включая создание резервных копий данных, использование специального программного обеспечения для фиксации цифровых следов, соблюдение мер по предотвращению изменения исследуемой информации.

3. Выемка и осмотр документов.

По делам о хищениях ЭДС особое значение имеют следующие документы:

– выписки из электронных кошельков и банковских счетов потерпевшего;

– договоры на обслуживание электронных средств платежа;

– журналы операций в платежных системах;

– логи авторизации в дистанционных банковских сервисах;

– сведения об IP-адресах, с которых осуществлялся доступ к ЭДС;

– документы, отражающие движение похищенных средств[1].

[1] Батов В.А. Особенности расследования хищений в отношении электронных денежных средств // Безопасность личности, общества и государства: теоретико-правовые аспекты: Сборник научных статей международной научно-теоретической конференции курсантов, слушателей и студентов, проводимой в рамках I Санкт-Петербургского международного молодежного научного форума «Северная Пальмира: территория

Изъятие указанных документов следует осуществлять как в бумажной, так и в электронной форме, с соблюдением требований УПК РФ об участии понятых либо применении технических средств фиксации.

4. Назначение экспертиз.

При расследовании хищений ЭДС типичными являются следующие виды экспертиз:

1. Компьютерно-техническая экспертиза – для исследования технических устройств, выявления вредоносного ПО, восстановления удаленных данных.

2. Информационно-аналитическая экспертиза – для анализа движения ЭДС, идентификации маршрутов транзакций.

3. Лингвистическая экспертиза – при необходимости анализа текстовых сообщений, использованных при совершении хищения методом социальной инженерии.

4. Экономическая экспертиза – для определения размера причиненного ущерба, особенно в случаях многоэпизодных хищений.

При формулировании вопросов эксперту необходимо консультироваться со специалистами соответствующего профиля, чтобы обеспечить корректность постановки задачи и получить максимально информативное заключение.

Эффективное взаимодействие с кредитно-финансовыми организациями и операторами связи является одним из ключевых условий успешного расследования хищений ЭДС. Анализ практики расследования показывает, что наиболее результативными формами такого взаимодействия являются:

1. Получение информации о движении денежных средств по счетам и электронным кошелькам, связанным с преступлением.

2. Идентификация конечных получателей похищенных ЭДС.

возможностей», Санкт-Петербург, 30 ноября 2021 года. Санкт-Петербург: Санкт-Петербургский университет МВД РФ, 2022. С. 1284.

3. Получение сведений о технических устройствах, использованных для доступа к ЭДС.

4. Получение данных о телекоммуникационных соединениях, имеющих отношение к преступлению.

5. Блокирование операций с похищенными ЭДС для предотвращения их дальнейшего обналичивания или перевода.

Для оптимизации взаимодействия целесообразно использовать заранее разработанные шаблоны запросов, учитывающие специфику различных платежных систем и операторов связи. Важно также учитывать, что получение информации от крупных международных платежных систем может требовать применения механизмов международного сотрудничества, что потенциально увеличивает сроки расследования.

Таким образом, организация первоначального этапа расследования хищений электронных денежных средств представляет собой сложный комплекс процессуальных, организационных и тактических мероприятий, требующий от следователя специальных знаний в области информационных технологий и понимания особенностей функционирования электронных платежных систем.

Эффективное расследование преступлений данной категории возможно только при условии своевременного выявления и фиксации цифровых следов, правильного определения направлений расследования в зависимости от сложившейся следственной ситуации, а также продуктивного взаимодействия с экспертами, специалистами, кредитно-финансовыми организациями и операторами связи.

Предложенные в настоящей главе рекомендации по организации первоначального этапа расследования хищений ЭДС основаны на обобщении следственной и судебной практики и направлены на повышение качества и результативности расследования данной категории преступлений.

§2. Проблемы и пути совершенствования методики расследования хищений электронных денежных средств на основе практики ОМВД России по Уфимскому району

Согласно данным, полученным в ходе анализа деятельности ОМВД России по Уфимскому району Республики Башкортостан, в период с 2020 по 2025 гг. наблюдается устойчивый рост числа зарегистрированных преступлений, связанных с хищениями электронных денежных средств. Так, если в 2020 году было зарегистрировано 112 таких преступлений, то в 2021 году – 157, в 2024 году – 203, а в 2025 году уже 396 преступлений данной категории. Эта динамика соответствует общероссийским тенденциям и свидетельствует о возрастающей криминальной активности в сфере информационно-телекоммуникационных технологий.

Анализ материалов головных дел о хищениях электронных денежных средств, расследованных следователями и дознавателями ОМВД России по Уфимскому району в 2020-2025 гг., позволил выявить следующую структуру данных преступлений по способу совершения:

1. Хищения с использованием методов социальной инженерии (телефонные звонки от имени работников банков, служб безопасности) – 48,3%;

2. Фишинг (создание поддельных сайтов, рассылка сообщений со ссылками) – 23,5%;

3. Хищения с использованием вредоносного программного обеспечения – 14,7%;

4. Хищения с использованием украденных или поддельных электронных средств платежа – 8,2%;

5. Иные способы хищения (включая комбинированные) – 5,3%.

Обращает на себя внимание значительное преобладание хищений с использованием методов социальной инженерии, что отражает общую

тенденцию к смещению фокуса преступников с технических методов взлома защитных систем на манипулирование пользователями.

По результатам изучения материалов уголовных дел установлено, что средняя сумма ущерба от одного преступления составила 58 700 рублей, при этом минимальная сумма хищения составила 3 200 рублей, а максимальная – 1 457 000 рублей.

Анализ результативности расследования показывает, что из общего количества возбужденных уголовных дел до суда доводится лишь 27,6%, что значительно ниже показателя раскрываемости иных категорий имущественных преступлений. При этом наиболее высокий показатель раскрываемости демонстрируют хищения, совершенные с использованием украденных или поддельных электронных средств платежа (42,9%), а наименьший – хищения с использованием методов социальной инженерии (19,1%).

Относительно сроков расследования уголовных дел данной категории установлено, что средний период от момента возбуждения дела до направления его в суд или принятия иного процессуального решения составляет 3,8 месяца, что значительно превышает аналогичный показатель для традиционных форм хищений.

С целью выявления проблем, нами проведен опрос следователей и дознавателей ОМВД России по Уфимскому району.

Вопрос 1: Считаете ли Вы уровень своей подготовки в сфере информационных технологий достаточным для эффективного расследования хищений ЭДС?

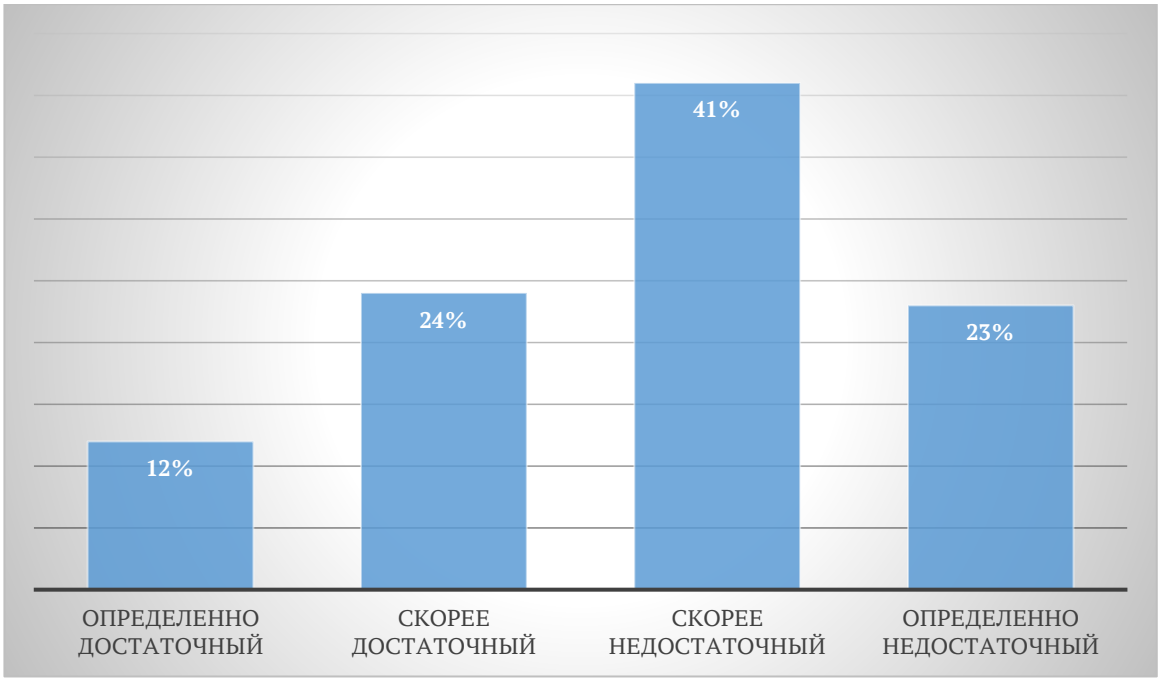

Рис. 3.1 - Результаты ответов на первый вопрос

Вопрос 2: Какие факторы, по Вашему мнению, наиболее негативно влияют на эффективность расследования хищений ЭДС?

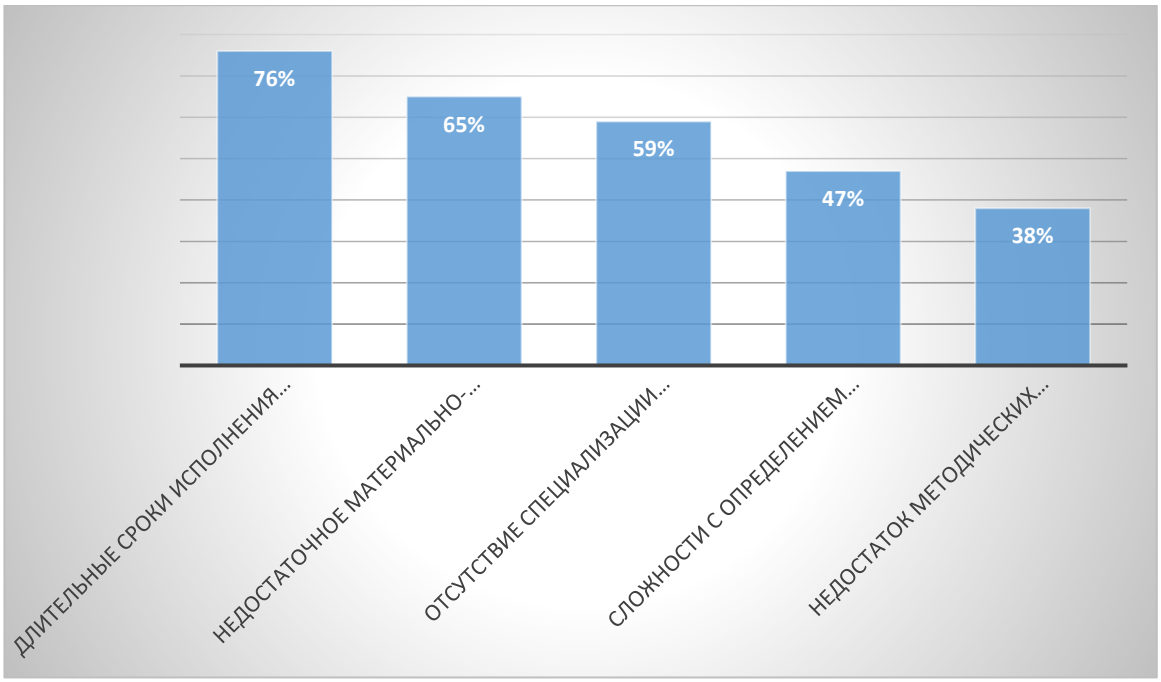

Рис. 3.2 - Результаты ответов на второй вопрос

Вопрос 3: Как Вы оцениваете уровень взаимодействия с экспертными подразделениями при расследовании хищений ЭДС?

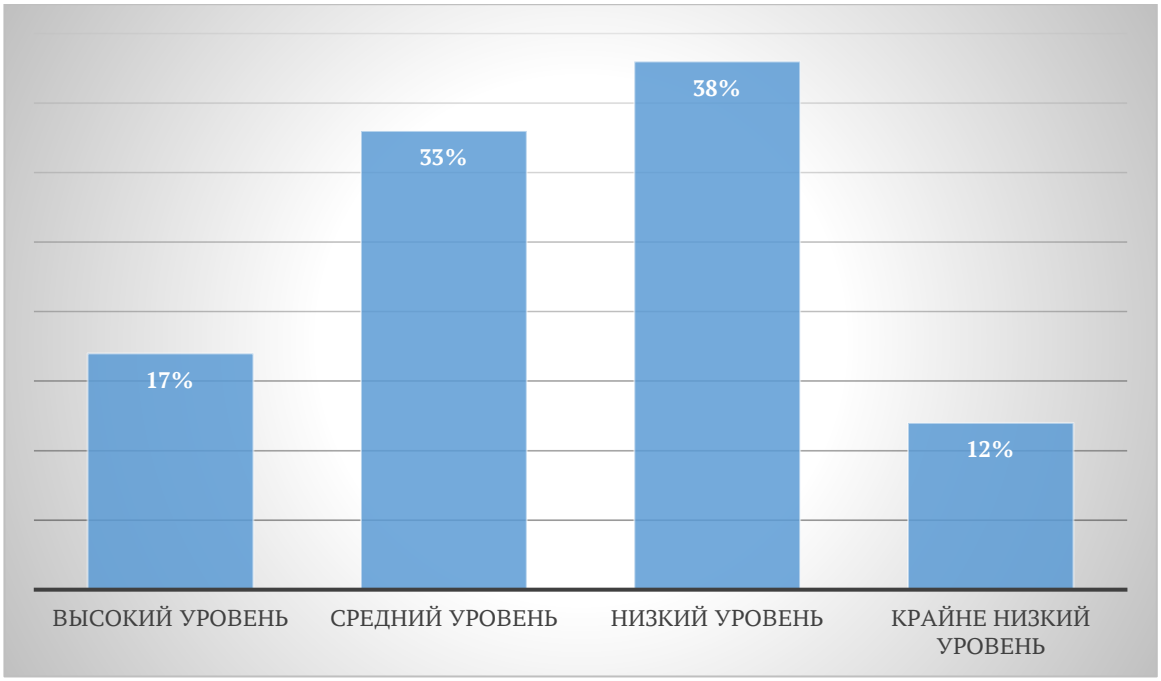

Рис. 3.3 - Результаты ответов на третий вопрос

Вопрос 4: Какой способ хищения ЭДС, по Вашему опыту, представляет наибольшую сложность для расследования?

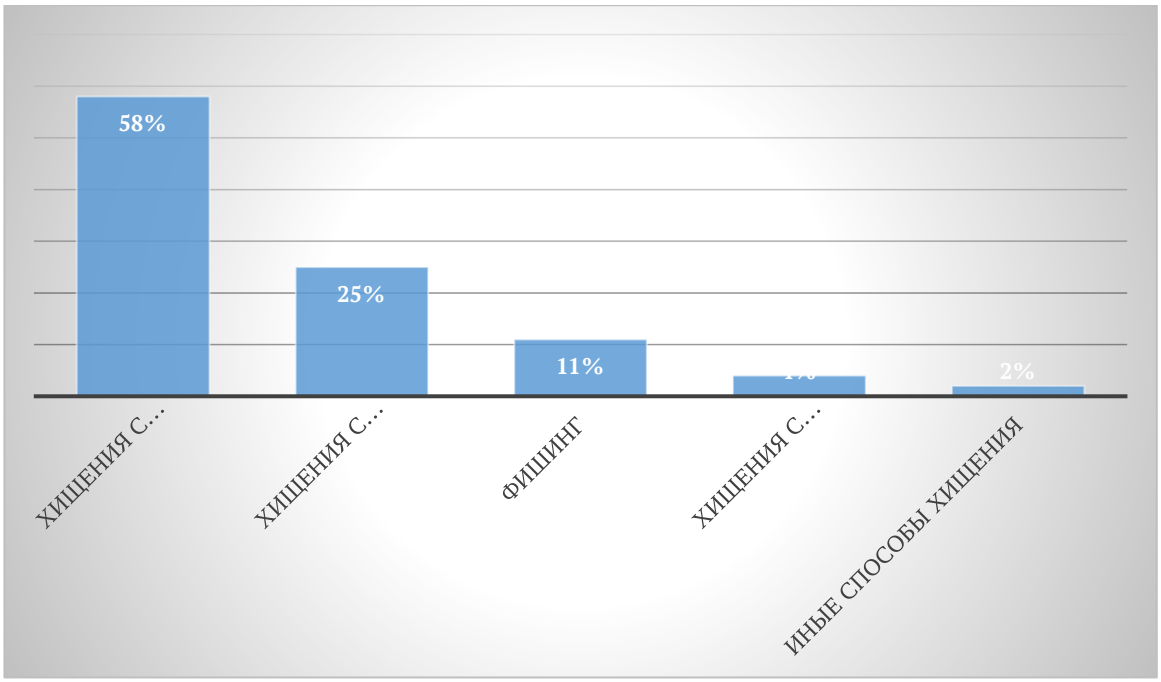

Рис. 3.4 - Результаты ответов на четвертый вопрос

Вопрос 5: Какие меры, на Ваш взгляд, наиболее эффективны для повышения раскрываемости хищений ЭДС?

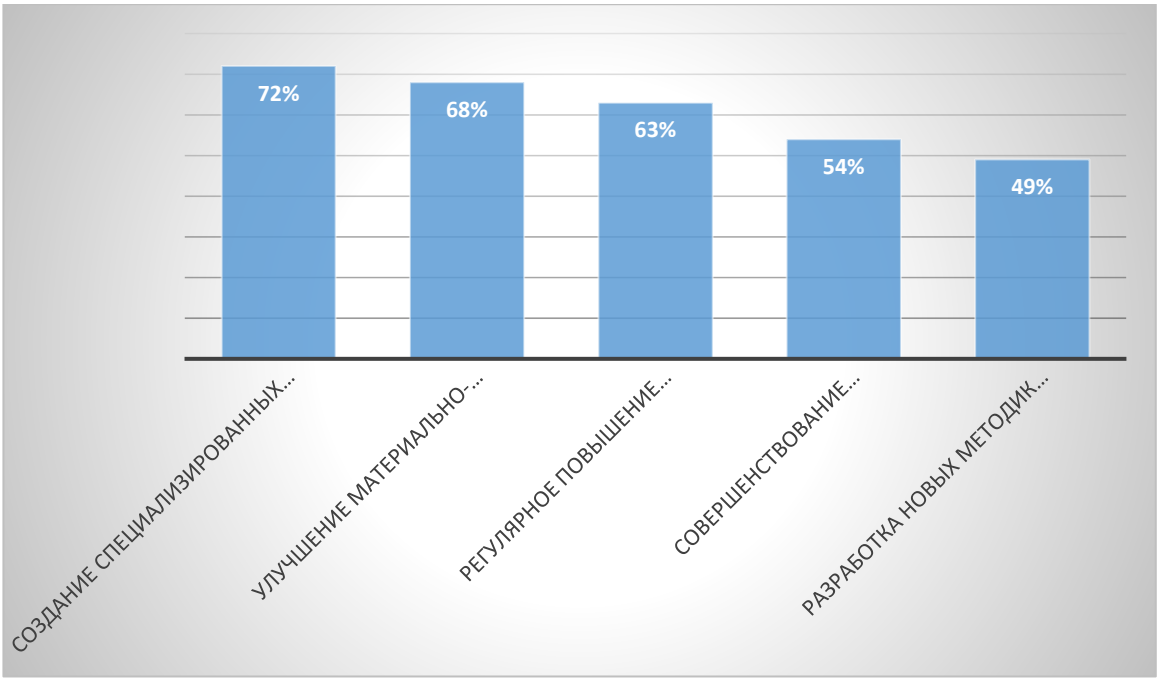

Рис. 3.5 - Результаты ответов на пятый вопрос

Анализ материалов уголовных дел и результаты опроса сотрудников следственных подразделений и подразделений дознания ОМВД России по Уфимскому району позволили выявить следующие ключевые проблемы, возникающие при расследовании хищений электронных денежных средств:

1. Организационно-обеспечительные проблемы.

Недостаточный уровень материально-технического обеспечения органов предварительного расследования. Только 28% опрошенных следователей и дознавателей отметили, что имеют доступ к специализированным программно-аппаратным комплексам для анализа цифровых следов. В результате многие процессуальные и следственные действия проводятся с существенными задержками или не в полном объеме.

Отсутствие специальных подразделений, ориентированных исключительно на расследование киберпреступлений. В настоящее время дела о хищениях электронных денежных средств распределяются между всеми следователями и дознавателями, что не позволяет обеспечить необходимую специализацию.

Недостаточная компетенция сотрудников в сфере информационных технологий. 64% опрошенных признали, что испытывают затруднения при

работе с цифровыми доказательствами и интерпретации технической информации.

Отсутствие систематического обмена информацией между территориальными органами МВД России о новых способах совершения хищений ЭДС, что затрудняет своевременное выявление серийного характера таких преступлений.

2. Процессуальные и криминалистические проблемы.

Сложности в определении территориальной подследственности. В 41% изученных уголовных дел имело место изменение территориальной подследственности, что существенно увеличивало сроки расследования.

Длительные сроки исполнения запросов о предоставлении информации операторами связи, банковскими организациями и платежными системами. Среднее время ожидания ответов на запросы составляет от 14 до 45 дней, что значительно замедляет ход расследования.

Проблемы в фиксации и изъятии цифровых следов. В 53% изученных уголовных дел отмечены недостатки в процедуре изъятия и фиксации цифровых следов, что впоследствии ставило под сомнение допустимость полученных доказательств.

Недостаточная разработанность методик проведения отдельных следственных действий при расследовании данной категории преступлений, особенно в случаях, когда хищение осуществлялось с использованием сложных технических решений.

Сложности в установлении всей цепочки движения похищенных средств, особенно при использовании преступниками криптовалют и анонимных платежных систем. В 76% нераскрытых уголовных дел именно невозможность отследить движение денежных средств стала ключевой причиной неустановления лица, совершившего преступление.

Проблемы, связанные с назначением и производством судебных экспертиз. Отмечается дефицит квалифицированных экспертов в области

компьютерно-технических и информационно-аналитических исследований, а также длительные сроки проведения экспертиз (в среднем 45-60 дней).

3. Проблемы международного сотрудничества.

Транснациональный характер значительной части преступлений. По данным исследования, в 38% случаев преступники находились за пределами Российской Федерации, что существенно осложняло процесс расследования.

Сложная процедура получения информации от зарубежных интернет-сервисов (Google, Apple, Facebook, Telegram и др.). Запросы через механизмы международной правовой помощи исполняются в течение 6-10 месяцев, что несовместимо с процессуальными сроками расследования.

Отсутствие прямых каналов взаимодействия с правоохранительными органами иностранных государств для оперативного обмена информацией о киберпреступлениях.

На основе выявленных проблем и с учетом положительного опыта расследования отдельных уголовных дел в ОМВД России по Уфимскому району можно предложить следующие пути совершенствования методики расследования хищений электронных денежных средств:

1. Организационно-обеспечительные меры.

Создание специализированных следственно-оперативных групп по расследованию киберпреступлений в структуре ОМВД. Данная мера позволит концентрировать профессиональные кадры и технические ресурсы для наиболее эффективного расследования.

Разработка и внедрение программы регулярного повышения квалификации следователей и дознавателей в области информационных технологий и методик расследования киберпреступлений. Программа должна включать как теоретическую подготовку, так и практические тренинги по работе с цифровыми доказательствами.

Обеспечение следственных подразделений современными программно-аппаратными комплексами для работы с цифровыми доказательствами. Минимальный базовый набор должен включать: специализированное

программное обеспечение для анализа цифровых следов, оборудование для криминалистического исследования мобильных устройств, средства для восстановления удаленных данных.

Создание единой региональной информационной базы о способах совершения хищений ЭДС и лицах, причастных к их совершению, с обеспечением доступа для всех территориальных органов МВД в Республике Башкортостан.

2. Процессуальные и криминалистические меры.

Разработка и внедрение специализированных алгоритмов действий следователя(дознавателя) при расследовании различных типов хищений ЭДС с учетом специфики каждого способа совершения преступления.

Совершенствование взаимодействия с финансовыми организациями и операторами связи. Заключение соглашений о сотрудничестве, предусматривающих упрощенный порядок предоставления информации по запросам правоохранительных органов.

Внедрение практики привлечения специалистов в области информационных технологий к участию в следственных действиях на постоянной основе, в том числе с использованием возможностей дистанционного участия.

Разработка методических рекомендаций по фиксации и изъятию цифровых следов при расследовании хищений ЭДС с учетом современных технологий и требований процессуального законодательства.

Организация взаимодействия с операторами сотовой связи и интернет-провайдерами для оперативного получения информации о соединениях и IP-адресах, в том числе в режиме онлайн при наличии достаточных оснований.

Создание постоянно действующей консультационной службы из числа специалистов в области информационных технологий и информационной безопасности для оказания помощи следователям при расследовании сложных технических аспектов киберпреступлений.

3. Меры по улучшению международного сотрудничества.

Разработка упрощенных механизмов получения информации от зарубежных интернет-компаний через прямое взаимодействие или с использованием возможностей НЦБ Интерпола.

Создание специализированных каналов взаимодействия с правоохранительными органами сопредельных государств для оперативного обмена информацией о трансграничных киберпреступлениях.

Использование возможностей международных организаций (Интерпол, Европол, ШОС) для координации действий при расследовании транснациональных преступлений.

4. Превентивные меры.

Организация профилактической работы с населением по повышению осведомленности о способах защиты от киберпреступлений, в том числе через средства массовой информации и социальные сети.

Взаимодействие с финансовыми организациями и операторами электронных платежных систем по внедрению дополнительных мер безопасности и аутентификации пользователей.

Разработка и распространение информационных материалов о наиболее распространенных способах хищений ЭДС и мерах по их предотвращению.

Реализация предложенных мер позволит существенно повысить эффективность расследования хищений электронных денежных средств в ОМВД России по Уфимскому району и может быть масштабирована в качестве положительного опыта на другие территориальные органы внутренних дел МВД России.

ЗАКЛЮЧЕНИЕ

В ходе исследования было установлено, что хищения электронных денежных средств представляют собой динамично развивающийся вид преступной деятельности, характеризующийся высокой технологичностью, латентностью и значительным материальным ущербом. Специфика данных преступлений обусловлена особенностями предмета посягательства – электронных денежных средств, которые имеют нематериальную природу и обеспечивают высокую скорость транзакций, что существенно осложняет процесс расследования.

Анализ уголовно-правовой характеристики хищений электронных денежных средств показал, что данные преступления квалифицируются преимущественно по ст. 158, 159, 159.3, 159.6 УК РФ в зависимости от способа совершения преступления. При этом выявлены определенные сложности в правоприменительной практике, связанные с разграничением смежных составов преступлений и определением момента окончания преступного деяния, что требует дальнейшего совершенствования уголовного законодательства.

Криминалистическая характеристика хищений электронных денежных средств отражает многообразие способов совершения данных преступлений, среди которых наиболее распространенными являются фишинг, вредоносное программное обеспечение, социальная инженерия, взлом аккаунтов и использование скомпрометированных платежных данных. Установлено, что большинство таких преступлений совершается организованными преступными группами, имеющими четкое распределение ролей и высокий уровень технической подготовки.

Исследование особенностей возбуждения уголовных дел и организации первоначального этапа расследования показало, что эффективность данных процессуальных действий во многом зависит от своевременности поступления информации о преступлении и сохранения цифровых следов. Выявлены

проблемы, связанные с определением территориальной подследственности, сбором достаточных данных для принятия решения о возбуждении уголовного дела, а также взаимодействием с финансовыми учреждениями и операторами связи.

Анализ тактики проведения отдельных следственных действий при расследовании хищений электронных денежных средств показал, что наибольшей спецификой обладают осмотр компьютерной техники и цифровых носителей информации, обыск, выемка электронных документов и назначение компьютерно-технических экспертиз. При этом эффективность данных следственных действий существенно повышается при участии специалистов в области информационных технологий.

Особое внимание в исследовании было уделено проблемам и перспективам совершенствования методики расследования хищений электронных денежных средств. Среди основных проблем выделены: недостаточное техническое оснащение территориальных органов внутренних дел, нехватка квалифицированных кадров, владеющих специальными знаниями в области информационных технологий, трудности в получении информации от международных компаний, а также быстрое изменение форм и методов преступной деятельности.

На основании проведенного исследования сформулированы следующие практические рекомендации:

1. Создание специализированных подразделений в территориальных органах внутренних дел, ориентированных на расследование киберпреступлений, включая хищения электронных денежных средств.

2. Совершенствование системы профессиональной подготовки и повышения квалификации сотрудников органов внутренних дел по вопросам расследования преступлений в сфере информационных технологий.

3. Разработка и внедрение современных аппаратно-программных комплексов для фиксации и исследования цифровых следов преступления.

4. Создание единой информационной базы данных о способах совершения хищений электронных денежных средств и методах их расследования.

5. Совершенствование механизмов межведомственного и международного сотрудничества в сфере противодействия киберпреступности, включая упрощение процедуры получения информации от иностранных компаний.

6. Разработка методических рекомендаций по расследованию отдельных видов хищений электронных денежных средств с учетом наиболее актуальных способов совершения данных преступлений.

7. Активизация профилактической работы по предупреждению хищений электронных денежных средств путем информирования населения о существующих угрозах и способах защиты.

Реализация предложенных рекомендаций позволит повысить эффективность деятельности территориальных органов внутренних дел по расследованию хищений электронных денежных средств, что в свою очередь будет способствовать снижению уровня данного вида преступности и обеспечению защиты прав и законных интересов граждан в сфере финансовых отношений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с учетом поправок, внесенных Законом Рос. Федерации о поправках к Конституции Рос. Федерации от 14 марта 2020 г. № 1-ФКЗ // Российская газета. – 2020. – № 144.

2. Уголовно-процессуальный кодекс Российской Федерации: федеральный закон от 18 декабря 2001 г. №174-ФЗ // Российская газета. – 2001. – №249.

3. Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

4. О национальной платежной системе: федеральный закон от 27 июня 2011 г. № 161-ФЗ «» // Собрание законодательства Российской Федерации. – 2011. – № 27. – Ст. 3872.

5. О Центральном банке Российской Федерации (Банке России): федеральный закон от 10.07.2002 № 86-ФЗ// Собрание законодательства Российской Федерации. – 2002. – № 12. – Ст. 5454.

6. О правилах осуществления перевода денежных средств: положение Банка России от 29.06.2021 № 762-П [Электронный ресурс]. URL: https://www.consultant.ru (дата обращения: 20.02.2026).

7. О порядке представления кредитными организациями в уполномоченный орган сведений о случаях отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом: указание Банка России от 20.07.2016 № 4077-У [Электронный ресурс]. URL: https://www.consultant.ru (дата обращения: 20.02.2026).

8. О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты

информации при осуществлении переводов денежных средств: положение Банка России от 17.08.2023 №821-П [Электронный ресурс]. URL: https://www.consultant.ru (дата обращения: 20.02.2026).

II. Учебная, научная литература и иные материалы

1. Авдеева, С.Б. Проблемы квалификации преступлений, связанных с хищением электронных денежных средств // Интернаука. – 2022. – № 14-4(237). – С. 46-47.

2. Алборова, В.С. Хищение денежных средств с использованием электронных средств платежа // Студенческий форум. – 2021. – № 43-2(179). – С. 84-85.

3. Ахмедов, Т.Ч. Способы хищения денежных средств с электронных носителей // Современные проблемы обеспечения экономической безопасности хозяйствующего субъекта: Всероссийская научная конференция: сборник научных трудов, Москва, 24 февраля 2021 года / Составитель Л.Н. Иванова. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2021. – С. 14-17.

4. Баженова, Е.Д. Проблемы уголовного преследования за хищения с банковского счета, а равно в отношении электронных денежных средств // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: Материалы Международной научно-практической конференции, Воронеж, 22 мая 2025 года. – Воронеж: Воронежский институт МВД РФ, 2025. – С. 99-100.

5. Батов, В.А. Особенности расследования хищений в отношении электронных денежных средств // Безопасность личности, общества и государства: теоретико-правовые аспекты: Сборник научных статей международной научно-теоретической конференции курсантов, слушателей и студентов, проводимой в рамках I Санкт-Петербургского международного молодежного научного форума «Северная Пальмира: территория возможностей», Санкт-Петербург, 30 ноября 2021 года. – Санкт-Петербург: Санкт-Петербургский университет МВД РФ, 2022. – С. 1284-1287.

6. Бикмурзина, О.П. Понятие криминалистической характеристики краж, совершенных с банковского счета, а равно в отношении электронных денежных средств // Актуальные вопросы применения российского права: материалы III научно-практической конференции, Саранск, 21 февраля 2023 года / Национальный исследовательский Мордовский государственный университет им. Н. П. Огарева. – Саранск: Общество с ограниченной ответственностью «ЮрЭксПрактик», 2023. – С. 27-30.

7. Блинова-Сычкарь, И.В. Вопросы противодействия хищению электронных денежных средств // Приоритетные направления социально-гуманитарных и экономических исследований в современной науке: Сборник научных статей по итогам национальной научно-практической конференции, Волгоград, 28 февраля 2024 года. – Волгоград: Волгоградский институт экономики, социологии и права, 2024. – С. 12-18.

8. Воскресенская, А.М. Правовое регулирование соотношения безналичных денежных средств, электронных денежных средств и цифрового рубля // Студенческий вестник. – 2026. – № 1-5(381). – С. 68-69.

9. Голятина, С.М. Методика расследования хищений электронных денежных средств: дисс. … канд. юрид. наук: 12.00.12 / Голятина Светлана Михайловна. – М., 2022. – 196 с.

10. Голятина, С.М. Проблемы организации расследования хищений электронных денежных средств // Совершенствование уголовно-процессуальных и криминалистических мер противодействия преступности: Материалы международной научно-практической конференции, Омск, 29 ноября 2022 года. – Омск: Омская академия МВД РФ, 2023. – С. 130-133.

11. Жмуров, Д.В. Цифровая кража: понятие, содержание, жертвы и их классификация // Всероссийский криминологический журнал. – 2023. – Т. 17, № 1. – С. 35-43.

12. Иванюшин, Д.В. Некоторые аспекты деятельности оперативных подразделений по обнаружению и изъятию электронных следов краж, совершаемых с использованием информационно-телекоммуникационных

технологий // Проблемы уголовно-процессуального права и криминалистики: Сборник научных статей / Редколлегия: Н.В. Морозова [и др.]. – Орел: Орловский юридический институт Министерства внутренних дел Российской Федерации имени В.В. Лукьянова, 2021. – С. 50-56.

13. Карпенко, А.А. Сравнительно-правовой анализ безналичных денежных средств, электронных денежных средств и цифрового рубля // Legal Bulletin. – 2024. – Т. 9, № 4. – С. 172-186.

14. Клещенко, Ю.Г. Классификация способов совершения хищений денежных средств с использованием электронных средств платежа // Проблемы противодействия киберпреступности: Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. – М.: Московская академия Следственного комитета Российской Федерации, 2023. – С. 73-77.

15. Князькина, А.К. Цифровая валюта как предмет хищения (на примере цифрового рубля) // Уголовное право: стратегия развития в XXI веке. – 2025. – № 1. – С. 196-205.

16. Колдырина, Е.Э. Правовые аспекты соотношения безналичных денежных средств, электронных денежных средств и цифрового рубля // Аллея науки. – 2025. – Т. 1, № 9(108). – С. 316-320.

17. Кравцова, О.В. Отдельные вопросы методики расследования хищений электронных денежных средств // Развитие парадигмы инновационной экономической, управленческой и правовой науки: сборник научных статей по итогам национальной научно-практической конференции, Волгоград, 14 апреля 2023 года. – Волгоград: Волгоградский институт экономики, социологии и права, 2023. – С. 57-62.

18. Крестьянинова, К.С. Характеристика предмета хищения в отношении электронных денежных средств // Право и общество. – 2023. – № 4(13). – С. 67-71.

19. Морозова, Т.А. Особенности допроса потерпевшего по уголовным делам о расследовании хищений электронных денежных средств // Ключевые

аспекты экономической безопасности финансовой системы Российской Федерации: Сборник научных статей по итогам Всероссийской научно-практической конференции, Нижний Новгород, 21 мая 2025 года. – Нижний Новгород: Нижегородская академия МВД России, 2025. – С. 158-163.

20. Мурзабаева, Д.А. Квалификация хищений электронных денежных средств в условиях конкуренции норм // XLIX Самарская областная студенческая научная конференция: Тезисы докладов, Самара, 10–21 апреля 2023 года. – Санкт-Петербург: ООО «Эко-Вектор», 2023. – С. 231-232.

21. Назмеева, Л.Р. Личность преступника, совершающего мошеннические действия с использованием электронных средств платежа: криминологическая оценка // Вестник Казанского юридического института МВД России. – 2021. – Т. 12, № 4(46). – С. 535-541.

22. Некрасов, Д.Е. Электронные денежные средства как предмет преступления // Юристъ-Правоведъ. – 2023. – № 4(107). – С. 167-174.

23. Ненашев, Е.В. К вопросу о содержании криминалистической характеристики краж, совершенных с банковских счетов, а равно в отношении электронных денежных средств // Криминалистика: вчера, сегодня, завтра. – 2023. – № 3(27). – С. 146-157.

24. Ненашев, Е.В. Особенности анализа криминалистической информации, поступающей на первоначальном этапе расследования хищения электронных денежных средств с банковского счета // Актуальные проблемы науки и практики: сборник научных трудов по итогам научно-представительских мероприятий, Хабаровск, 25 ноября 2021 года – 29 2022 года. – Хабаровск: Дальневосточный юридический институт Министерства внутренних дел Российской Федерации имени И.Ф. Шилова, 2022. – С. 229-234.

25. Ненашев, Е.В. Особенности классификации типичных личностей преступников, совершающих дистанционные хищения с банковских счетов // Проблемы юриспруденции и педагогики высшей школы в работах молодых ученых: сборник материалов Всероссийской научно-практической

конференции, Белгород, 30 ноября 2022 года. Том Выпуск 3. – Белгород: Белгородский юридический институт Министерства внутренних дел Российской Федерации им. И.Д. Путилина, 2023. – С. 122-127.

26. Ненашев, Е.В. Особенности личности преступника как важнейший элемент криминалистической характеристики краж, совершенных с банковского счета, а также в отношении электронных денежных средств // Вестник Дальневосточного юридического института МВД России. – 2022. – № 3(60). – С. 92-97.

27. Нефедова, Е.Р. Актуальные проблемы расследования преступлений, связанных с дистанционным хищением средств в банковской сфере // Актуальные проблемы расследования преступлений в сфере компьютерной информации или с применением компьютерных технологий в условиях цифровизации экономики и государственного управления: материалы Межвузовского круглого стола, Москва, 28 ноября 2024 года. – Москва: Общество с ограниченной ответственностью «Русайнс», 2025. – С. 268-275.

28. Поздышев, Р.С. Проблемные вопросы практики расследования хищений безналичных и электронных денежных средств // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2021. – № 1(53). – С. 143-148.

29. Пудовиков, А.С. Структура типичного способа совершения хищений с банковских счетов в отношении и (или) с помощью электронных денежных средств // Право и государство: теория и практика. – 2021. – № 12(204). – С. 292-295.

30. Ситник, А.А. Цифровой рубль как объект финансово-правового регулирования // Актуальные проблемы российского права. – 2023. – Т. 18, № 8(153). – С. 20-36.

31. Смоляков, А.Н. Хищение безналичных, электронных денежных средств и цифровой валюты: вопросы юридической техники и

дифференциации ответственности: дисс. … канд. юрид. наук: 12.00.08 / Смоляков Александр Николаевич. –М., 2023. –256 с.

32. Стародубцева, О.Н. Общественная опасность как субъективный признак лица, совершившего преступление // Уголовное право России: состояние и перспективы (Волженкинские чтения): материалы X Всероссийской научно-практической конференции с международным участием, Санкт-Петербург, 29 ноября 2024 года. – Санкт-Петербург: Университет прокуратуры Российской Федерации, 2025. – С. 308-314.

33. Таксанова, А.В. Особенности криминалистической характеристики хищений, совершенных с банковского счета, а равно в отношении электронных денежных средств // Молодежь - Барнаулу: Материалы XXV городской научно-практической конференции молодых ученых, Барнаул, 01–30 ноября 2023 года. – Барнаул: ООО «Алком», 2024. – С. 1399-1400.

34. Тюнин, В.И. Квалификация хищений безналичных и электронных денежных средств / В. И. Тюнин, Ю. И. Степанов, Е. А. Маркова; Санкт-Петербургский университет МВД России, 2021. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2021. – 136 с.

35. Шашкина, Е.В. К вопросу о современных способах совершения дистанционных мошенничеств с использованием средств мобильной связи // Актуальные проблемы юридической науки и практики: Материалы международной научно-практической конференции памяти И.Ф. Шилова, Хабаровск, 30 мая 2024 года. – Хабаровск: Дальневосточный юридический институт МВД РФ им. И.Ф. Шилова, 2024. – С. 202-205.

III. Эмпирические материалы

1. Статистические данные МВД РФ // Официальный сайт МВД РФ [Электронный ресурс]. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 20.02.2026).

2. О судебной практике по делам о мошенничестве, присвоении и растрате: пленум Верховного Суда Российской Федерации в постановлении от 30.11.2017 № 48// Собрание законодательства Российской Федерации. – 2017. – №23. – Ст. 4824.

3. Кассационное определение Верховного Суда Российской Федерации от 3 апреля 2024 г. по делу № 1-226/2021[Электронный ресурс]. URL: https://sudact.ru/vsrf/doc/3yKLSSkomBNX/ (дата обращения: 20.02.2026).

4. Постановление Вахитовского районного суда г. Казани № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/ftR7s3xLHjHQ/ (дата обращения: 20.02.2026).

5. Приговор Заводского районного суда г. Саратова № 1-226/2023 от 5 июля 2023 г. по делу № 1-226/2023 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/fpWGIqIIn9m8/ (дата обращения: 20.02.2026).

6. Приговор Ивановского районного суда № 1-34/2024 от 19 февраля 2024 г. по делу № 1-34/2024 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/hrB3AJKoQqUu/ (дата обращения: 20.02.2026).

ПРИЛОЖЕНИЕ

Уважаемые коллеги! Данное анкетирование проводится с целью анализа текущих проблем и разработки рекомендаций по повышению эффективности расследования хищений электронных денежных средств (ЭДС). Опрос является анонимным.

Сведения о респонденте:

Должность: _____

Стаж работы в правоохранительных органах: _____ лет

Подразделение: _____

Вопрос 1

Считаете ли Вы уровень своей подготовки в сфере информационных технологий достаточным для эффективного расследования хищений ЭДС?

□ Да, полностью достаточным

□ Скорее достаточным

□ Скорее недостаточным

□ Категорически недостаточным

□ Затрудняюсь ответить

Вопрос 2

Какие факторы, по Вашему мнению, наиболее негативно влияют на эффективность расследования хищений ЭДС?

□ Недостаточный уровень специальных знаний следователей/дознавателей

□ Сложность получения цифровых доказательств

□ Недостаточное техническое оснащение подразделений

□ Длительные сроки проведения компьютерно-технических экспертиз

□ Проблемы взаимодействия с операторами платежных систем

□ Трудности в установлении лиц, совершивших преступление

□ Несовершенство законодательной базы

□ Другое: _____

Вопрос 3

Как Вы оцениваете уровень взаимодействия с экспертными подразделениями при расследовании хищений ЭДС?

□ Высокий

□ Удовлетворительный

□ Низкий

□ Крайне неудовлетворительный

Вопрос 4

Какой способ хищения ЭДС, по Вашему опыту, представляет наибольшую сложность для расследования?

□ Фишинг (создание поддельных сайтов)

□ Использование вредоносного программного обеспечения

□ Социальная инженерия (телефонное мошенничество)

□ Взлом личных кабинетов пользователей электронных платежных систем

□ Мошенничество с использованием поддельных электронных платежных средств

□ Другое: _____

Вопрос 5

Какие меры, на Ваш взгляд, наиболее эффективны для повышения раскрываемости хищений ЭДС?

□ Регулярное повышение квалификации сотрудников в IT-сфере

□ Создание специализированных подразделений по расследованию киберпреступлений

□ Совершенствование технического оснащения

□ Улучшение нормативно-правовой базы

□ Более тесное взаимодействие с операторами платежных систем

□ Международное сотрудничество с правоохранительными органами других стран

□ Другое: _____

Благодарим за участие в опросе!

Дата заполнения: ____ . ____ . 20___ г.

«Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну».

_____ В.М. Янахметов