*На правах рукописи*

**Харина Елена Алексеевна**

# ОСОБЕННОСТИ МЕТОДИКИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Специальность 5.1.4. Уголовно-правовые науки
(юридические науки)

**Автореферат**
диссертации на соискание ученой степени
кандидата юридических наук

Краснодар – 2024

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Красноярский государственный аграрный университет»

**Научный руководитель:** доктор юридических наук, профессор
**Гармаев Юрий Петрович**

**Официальные оппоненты:** **Давыдов Владимир Олегович**
доктор юридических наук, доцент, ФГБОУ ВО «Тульский государственный университет», профессор кафедры правосудия и правоохранительной деятельности

**Науменко Оксана Александровна**
кандидат юридических наук, доцент, ФГКОУ ВО «Краснодарский университет Министерства внутренних дел Российской Федерации», профессор кафедры криминалистики

**Ведущая организация:** **ФГБОУ ВО «Алтайский государственный университет»**

Защита диссертации состоится « 17 » мая 2024 г. в $10^{\underline{00}}$ часов на заседании диссертационного совета 35.2.019.01 на базе ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина» по адресу: 350044, г. Краснодар, ул. Калинина, 13, главный корпус университета, ауд. 215.

С диссертацией можно ознакомиться в библиотеке университета и на сайтах: ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина» – www.kubsau.ru и ВАК – https://vak.minobrnauki.gov.ru

Автореферат разослан «____» _____ 2024 г.

И.о. ученого секретаря
диссертационного совета
доктор юридических наук А.А. Тушев

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования.** Современный цивилизационный этап развития можно смело назвать эпохой информационно-телекоммуникационных технологий (далее ИТТ), характеризующейся нацеленностью на цифровизацию и компьютеризацию всех сфер жизни общества. Наряду с многочисленными положительными тенденциями цифровая реальность таит в себе немало рисков, таких как виртуализация социума, уязвимость состояния защиты различного рода информации.

Происходящие трансформации общества в целом неминуемо отразились на состоянии преступности, где отчетливо наметились тенденции «переполюсации» в сторону совершения преступлений посредством использования возможностей ИТТ. Данное обстоятельство не могло не стать объектом пристального внимания со стороны государства.

Вероятно, именно поэтому одним из принципов Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента РФ от 09 мая 2017 г. № 203, обозначено обеспечение государственной защиты интересов российских граждан в информационной сфере (п. е ст. 3)[1].

20 марта 2023 г. на ежегодном расширенном заседании коллегии МВД России В.В. Путин отметил, что по итогам 2022 г. число преступлений с использованием информационных технологий составило четверть от всех уголовно наказуемых правонарушений, в связи с чем борьба с ними является одним из безусловных приоритетов работы министерства[2].

Действительно, анализ официальных статистических данных МВД России свидетельствует о систематическом увеличении доли рассматриваемой категории преступлений. Так, в 2022 г. зарегистрировано 522 065 таких преступлений, что

[1] О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 09 мая 2017 г. № 203. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 26.01.2023).

[2] Расширенное заседание коллегии МВД // Официальный сайт президента Российской Федерации. URL: http://www.kremlin.ru/events/president/news/70744 (дата обращения: 01.07.2023).

составляет 26,5 % от общего количества всех зарегистрированных преступных посягательств, тогда как еще пять лет назад, в 2017 г., этот показатель был почти в шесть раз ниже и составлял всего 4,4 %[3].

В этой связи совершенно обоснована нацеленность государства противостоять возникающим угрозам, в т. ч. посредством криминализации различного рода новых преступных посягательств. Одним из таких проявлений явилось введение в 2012 г. в Уголовный кодекс Российской Федерации (далее – УК РФ) ст. 159.6 «Мошенничество в сфере компьютерной информации»[4].

Анализ официальных данных МВД России относительно количества зарегистрированных преступлений, квалифицированных по ст. 159.6 УК РФ, указывает на динамику постепенного увеличения таких показателей с 2012 по 2015 г. и их резкого снижения с 2018 г. (в 2012 г. – 43, в 2013 г. – 693, в 2014 г. – 995, в 2015 г. – 5443, в 2016 г. – 4329, в 2017 г. – 2195, в 2018 г. – 970, в 2019 г. – 687, в 2020 г. – 761, в 2021 г. – 431, в 2022 г. – 334 преступления)[5]. Проведенное исследование показало, что данный факт объясняется существовавшей неоднозначной судебно-следственной практикой, сложившейся в виду наличия проблемных вопросов квалификации деяния. Большинство имевшихся противоречий были устранены разъяснениями, изложенными в постановлении Пленума Верховного Суда РФ от 30.11.2017 № 48, результатом чего явилось снижение количества зарегистрированных преступлений, квалифицированных по ст. 159.6 УК РФ[6].

Показатели количества уголовных дел, переданных в суды относительно общего количества зарегистрированных преступлений, квалифицированных по ст. 159.6 УК РФ, также указывают на существование ряда проблемных вопросов, в частности в эффективности их раскрытия и расследования. Так, из 16 681 преступления, зарегистрированного с 2012 по 2022 г., в суды направлено 1 602

[3]Официальный сайт МВД России. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 01.11.2023).

[4] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон от 29.11.2012 № 207-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

[5] Официальный сайт МВД России. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 01.11.2023).

[6] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 : ред. от 15.12.2022. URL: https://www.consultant.ru/document/ cons_doc_LAW_283918 (дата обращения: 20.12.2023).

уголовных дела, т. е. в целом более чем в десять раз меньше, чем зарегистрированных преступлений. Более детально такие показатели можно представить следующим образом: в 2012 г. – ни одно уголовное дело в суд не направлено, в 2013 г. – в суды направлено 27 % уголовных дел от количества зарегистрированных преступлений, в 2014 г. – 24; в 2015 г. – 5; в 2016 г. – 7; в 2017 г. – 8; в 2018 г. – 8; в 2019 г. – 8; в 2020 г. – 13; в 2021 г. – 31; в 2022 г. – 21%[7].

Тенденция низкой раскрываемости прослеживается и в отношении сопутствующих преступлений, т. е. противоправных деяний, как правило, совершаемых одновременно и в совокупности с преступлениями, предусмотренными ст. 159.6 УК РФ (в контексте исследования и для удобства терминологии предлагаем называть их «основными» преступлениями). Анализ статистических данных показал, что такими преступлениями преимущественно являются деяния, предусмотренные гл. 28 УК РФ «Преступления в сфере компьютерной информации» (ст. 272–274, ст. 274.1, ст. 274.2 УК РФ). Так, из 24 277 преступлений, квалифицированных по статьям гл. 28 УК РФ и зарегистрированных в период с 2019 по 2022 г., в суды направлено 3 674 уголовных дела[8].

Проведенное исследование выявило, что одними из основных причин неэффективности выявления, раскрытия и расследования анализируемой группы преступлений являются специфическая сфера проявления противоправной деятельности – сфера компьютерной информации, требующая наличия соответствующих познаний; сложности в обнаружении специфической следовой картины преступной деятельности, образованной в результате взаимодействия с компьютерной информацией; постоянно совершенствующиеся способы преступлений в связи с появлением нового программного обеспечения и компьютерных устройств; использование в преступной деятельности средств общения, затрудняющих идентификацию пользователей; преимущественное привлечение к уголовной ответственности так называемых «низовых»

[7] Официальный сайт МВД России. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 01.11.2023).
[8] Там же.

исполнителей, в результате чего деятельность самих организованных преступных формирований не изобличается.

Специфичность указанных причин неэффективного противодействия исследуемой категории преступлений свидетельствует о необходимости соответствующего подхода и к их эффективному расследованию. Анализ мнения опрошенных экспертов, занимающих руководящие должности в следственных, оперативных подразделениях правоохранительных органов в 26 субъектах РФ, позволил сделать вывод, что такого рода противодействие должно носить системный характер и заключаться в оснащении современными техническими средствами, усовершенствовании методик проведения экспертных исследований, создании специализированных баз данных. Одну из ключевых позиций в системе мер повышения эффективности борьбы с мошенничеством в сфере компьютерной информации занимает повышение квалификации и соответствующей специализированной подготовки лиц, занимающихся выявлением, раскрытием и расследованием анализируемой категории преступлений. Так, в ходе проведенного анкетирования указанных сотрудников 23 %, т. е. практически каждый четвертый из всех опрошенных, отметили отсутствие специальных познаний и должной квалификации. При этом 80 % респондентов в качестве одной из мер повышения квалификации указали на необходимость разработки соответствующей отдельной криминалистической методики расследования мошенничества в сфере компьютерной информации, на что и направлено настоящее диссертационное исследование.

**Степень разработанности темы диссертационного исследования.** Мошенничество, в т. ч. в сфере компьютерной информации, а также иные преступления в этой сфере в разное время становились предметом исследований представителей различных юридических наук.

Значительный вклад в разработку криминалистических методик расследования различных видов мошенничества внесли исследования таких ученых, как Р. Н. Боровских (2018), К. А. Виноградова (2018), Р. К. Гитинов (2017), Г. Н. Карепанов (2018), А. В. Маилян (2021), С. Р. Низаева (2017),

Н. В. Поляков (2021), О. В. Трубкина (2015), Р. А. Тагиров (2022), М. М. Уразбахтин (2013), А. В. Чумаков (2018) и др.

Различные аспекты расследования разнообразных преступлений в сфере компьютерной информации рассматривались в криминалистических диссертационных и иных исследованиях таких ученых, как Р. С. Атаманов (2012), А. А. Балашова (2020), Р. А. Белевский (2006), Л. В. Бертовский, В. Б. Вехов (2008), А. С. Вражнов (2015), Г. З. Гаспарян (2020), С. М. Голятина (2022), А. С. Егорышев (2004), Д. В. Завьялова (2022), Н. С. Зиновьева (2021), И. Г. Иванова (2007), В. В. Крылов (1998), А. Н. Колычева (2018), С. В. Крыгин (2002), К. В. Костомаров (2012), М. Е. Мазуров (2017), В. А. Мещеряков (2001), В. А. Милашев (2004), А. В. Остроушко (2000), В. В. Поляков (2008), А. А. Рудых (2019), А. Г. Себякин (2021), Г. В. Семенов (2003), А. Д. Тлиш (2002), Е. С. Шевченко (2016) и др.

Вместе с тем анализ научной литературы свидетельствует, что вопросы расследования мошенничества в сфере компьютерной информации на монографическом уровне в силу относительной новизны преступного деяния остаются малоисследованными.

Различные аспекты расследования мошенничества в сфере компьютерной информации рассматривались преимущественно на уровне научных статей и пособий в работах таких ученых, как И. О. Антонов, О. П. Бердникова, В. Ф. Васюков, В. Б. Вехов, В. Р. Гайнельзянова, В. О. Давыдов, Е. С. Дубоносов, М. В. Жижина, Д. В. Завьялова, Е. Г. Кравец, М. Н. Кузьмин, Э. В. Лантух, Н. И. Малыхина, М. В. Меркулова, С. Н. Миронов, О. А. Науменко, А. Л. Осипенко, Н. Н. Потапова, К. С. Скоробогатов, А. Ю. Семенов и др.

Уголовно-правовые исследования мошенничества в сфере компьютерной информации отражены в диссертационных работах М. Д. Фролова «Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации» (2018), Г. Р. Григоряна «Мошенничество в сфере компьютерной информации: проблемы криминализации и квалификации» (2021).

Смежный с нашим предмет научного исследования избрал в кандидатской диссертации В. В. Коломинов «Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты начального этапа» (2017). Однако положения данной работы касаются только первоначального этапа расследования мошенничества в сфере компьютерной информации. При этом данное диссертационное исследование проведено до принятия постановления Пленума Верховного Суда РФ № 48 [9], внесшего существенные коррективы в понимание природы и квалификацию анализируемого преступного посягательства, что неминуемо отразилось на формируемой судебно-следственной практике.

Высоко оценивая труды указанных ученых, отметим, что до настоящего времени опубликованные работы монографического характера, посвященные криминалистической методике расследования мошенничества в сфере компьютерной информации, носят единичный характер. Постоянное совершенствование способов преступления указывает на необходимость повышения эффективности имеющихся и создание новых методик расследования исследуемой категории преступлений.

**Объектом исследования** является преступная деятельность в сфере компьютерной информации, сопутствующих преступных посягательств, а также деятельность правоохранительных органов по выявлению, раскрытию и расследованию данных преступных деяний.

**Предметом исследования** являются закономерности мошенничества в сфере компьютерной информации и сопутствующей преступной деятельности, а также связанные с ними закономерности деятельности правоохранительных органов по выявлению, раскрытию, расследованию указанных преступлений.

**Цель и задачи исследования**. Цель исследования состоит в разработке теоретических положений и прикладных рекомендаций в рамках особенностей

[9] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 …

криминалистической методики расследования мошенничества в сфере компьютерной информации и сопутствующих преступлений.

Достижение поставленной цели стало возможным посредством решения следующих поставленных задач:

– определить признаки мошенничества в сфере компьютерной информации и сформулировать понятие рассматриваемого вида преступной деятельности в криминалистическом аспекте;

– сформулировать понятие криминалистической методики расследования мошенничества в сфере компьютерной информации, определить критерии ее формирования и место в системе методик более высокого уровня общности;

– выделить типичные способы мошенничества в сфере компьютерной информации;

– определить обстановку совершения мошенничества в сфере компьютерной информации;

– выделить свойства личности типичного преступника и потерпевшего и их криминалистическое значение;

– определить типичные следы мошенничества в сфере компьютерной информации;

– выявить особенности доследственной проверки и возбуждения уголовных дел рассматриваемой категории;

– определить типичные следственные ситуации мошенничества в сфере компьютерной информации, предложить алгоритм их разрешения, выделить типичные версии;

– выявить особенности тактики производства отдельных следственных действий исследуемой преступной деятельности;

– раскрыть возможности использования специальных знаний, актуальные вопросы назначения и проведения разных видов судебных экспертиз.

**Методология и методы исследования.** Методологическая основа исследования представлена всеобщим диалектическим методом научного

познания, а также общенаучными методами эмпирического и теоретического познания.

Методологической основой исследования также явились частно-научные методы: статистический (при анализе различных аспектов состояния преступной деятельности), социологические (при проведении анкетирования, интервьюирования и метода экспертных оценок), кибернетический (при обработке статистических и социологических исследований), психологический (при определении психологической характеристики выделенных категорий типичных преступников, выработке тактических приемов); а также специальные научные методы: формально-догматический (при определении и формулировании понятий, признаков, классификаций и т. п.), структурно-криминалистические (при планировании расследования, формировании алгоритма действий в различных следственных ситуациях и т. п.), технико-криминалистические (при определении и работе со следовой картиной преступной деятельности и т. п.) и др.

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

**Теоретической основой исследования** послужили труды Т. В. Аверьяновой, Ю. М. Антоняна, Р. С. Белкина, В. Ю. Белицкого, Л. В. Бертовского, О. П. Бердниковой, В. В. Борисова, А. В. Варданяна, А. Г. Василиади, В. Б. Вехова, И. А. Возгрина, Т. С. Волчецкой, Б. Я. Гаврилова, Ю. В. Гаврилина, В. К. Гавло, Ю. П. Гармаева, А. Ю. Головина, В. О. Давыдова, В. Д. Зеленского, Г. Г. Зуйкова, Е. П. Ищенко, Р. Г. Камнева, И. М. Комарова, С. А. Куемжиевой, В. Н. Кудрявцева, А. М. Кустова, А. Ф. Лубина, В. В. Лунеева, М. Ш. Махтаева, Г. С. Меретукова, В. А. Мещерякова, О. А. Науменко, В. А. Образцова, В. В. Полякова, Е. Р. Россинской, Е. А. Русскевича, О. В. Старкова, Л. Г. Шапиро, А. В. Шмонина, Н. П. Яблокова и других ученых.

**Эмпирическую базу научного исследования** составили соответствующие статистические данные МВД России, Генеральной прокуратуры России за период

с 2012 по 2023 г., а также соответствующие данные Судебного департамента при Верховном суде РФ, ЦБ РФ, опубликованная судебная практика судов РФ, а также сведения, размещенные в средствах массовой информации.

В ходе проведения исследования изучены материалы 127 уголовных дел, возбужденных и расследованных по ст. 159.6 УК РФ и сопутствующим преступлениям в Сибирском федеральном округе. Помимо указанных дел проанализировано 76 приговоров, вынесенных судами общей юрисдикции по ст. 159.6 УК РФ и сопутствующим преступлениям.

Диссертантом по специально разработанной анкете в течение 2023 г. проведено анкетирование 1 240 сотрудников правоохранительных органов, занимающихся выявлением, раскрытием, расследованием преступлений в сфере компьютерной информации в 67 субъектах Российской Федерации: 215 оперуполномоченных, 612 следователей, 413 дознавателей. С использованием метода экспертных оценок проведено интервьюирование 28 сотрудников правоохранительных органов, имеющих большой практический опыт выявления, раскрытия, расследования преступлений в сфере компьютерной информации, а также занимающих руководящие должности в данных подразделениях из 26 субъектов Российской Федерации.

**Научная новизна** диссертационного исследования заключается в том, что оно является одной из первых работ монографического характера, посвященных методике расследования мошенничества в сфере компьютерной информации, сформированной на обновленной методологической основе и с учетом современной правоприменительной практики, существенно отличающейся от предшествующей. В работе сформулировано более широкое, чем имелось ранее в литературе, определение понятия мошенничества в сфере компьютерной информации, под которым в криминалистическом аспекте помимо «основного» деяния, т. е. предусмотренного ст. 159.6 УК РФ, понимается совершение ряда сопутствующих преступлений, как правило, предусмотренных гл. 28 УК РФ, а также других преступных посягательств.

Сформированная на этой основе криминалистическая методика имеет оригинальную структуру и содержание. Особое внимание уделено элементам криминалистической характеристики анализируемой преступной деятельности. В частности на основе системного анализа, в ситуации существования неоднозначной судебно-следственной практики, с учетом разъяснений, указанных в постановлении Пленума Верховного Суда РФ № 48[10], выделены способы исследуемой преступной деятельности. Дана классификация и характеристика типичных преступников, отражена специфика оставляемых ими следовых картин. В качестве дополнительного элемента обстановки преступления выделено обладание соответствующими компьютерными устройствами, программно-аппаратными и другими техническими средствами с помощью которых и совершаются преступления данной категории. Критерию научной новизны соответствует также выделение типичных следственных ситуаций первоначального и последующего этапов расследования; предложен алгоритм их разрешения, а также тактические рекомендации по производству отдельных следственных действий и использованию специальных знаний.

Научная новизна диссертационного исследования нашла свое отражение и в основных положениях, выносимых на защиту.

**Основные положения, выносимые на защиту:**

1. Понятие «мошенничество в сфере компьютерной информации» в криминалистическом аспекте не идентично соответствующей уголовно-правовой норме, а отражает совокупность преступлений, включающую «основное» общественно опасное деяние, предусмотренное ст. 159.6 УК РФ, и ряд сопутствующих, предусмотренных ст. 272–274, ст. 274.1, 274.2, 210 УК РФ и т. д., а также отражает соответствие ряду криминалистических признаков.

Таким образом, основанием формирования частной криминалистической методики расследования мошенничества в сфере компьютерной информации является сочетание уголовно-правового и криминалистических критериев.

[10] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 …

2. Методика расследования мошенничества в сфере компьютерной информации – это сформированная на основе и в дополнение к более общим методикам расследования мошенничества, преступлений в сфере компьютерной информации, а также иных сопутствующих преступлений, совокупность научных положений и прикладных рекомендаций, выделенных по уголовно-правовому (ст. 159.6 УК РФ и сопутствующие) и криминалистически значимым критериям, отражающим закономерности преступной деятельности, связанной с хищениями, посредством воздействия на компьютерную информацию, а также закономерностей расследования и предупреждения данных преступных посягательств.

Определены основные направления расследования мошенничества в сфере компьютерной информации:

– выявление, раскрытие и расследование «организованных» мошенничеств в сфере компьютерной информации;

– изобличение и пресечение преступной деятельности не только так называемых «низовых» исполнителей, а всех членов преступных формирований, прежде всего организаторов и руководителей различного уровня.

3. Системообразующим элементом криминалистической характеристики мошенничества в сфере компьютерной информации является его способ. Выделены наиболее распространенные способы преступлений:

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

2) посредством воздействия вредоносного программного обеспечения (далее – ВПО) на компьютерные устройства клиентов кредитных организаций;

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

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

5) посредством осуществления несанкционированного управления работой банкомата;

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

7) посредством создания и использования «фишинговых» сайтов.

Разработана криминалистическая типология мошенничества в сфере компьютерной информации:

1) в зависимости от степени организованности: а) «организованное»; б) «несложное», или «простое», мошенничество в сфере компьютерной информации;

2) в зависимости от уголовно-правовой квалификации: а) посредством совершения только «основного» преступления; б) посредством совершения «основного» и сопутствующих преступлений.

4. В качестве дополнительного элемента обстановки мошенничества в сфере компьютерной информации выделено наличие у преступников соответствующих компьютерных устройств, программно-аппаратных и других технических средств, с помощью и посредством которых совершаются данные преступления. Обладание соответствующими инструментами определяет способ преступления, является важным фактором благоприятных или неблагоприятных для преступника обстоятельств, которые может использовать следствие.

5. Приведены данные о личности типичных преступников, предложена их классификация в зависимости от обладания соответствующими специальными познаниями в сфере ИТТ:

1) высококвалифицированные специалисты, своего рода эксперты в сфере ИТТ;

2) опытные преступники в сфере ИТТ. В отличие от специалистов высокого уровня опытные преступники, как правило, не являются сами разработчиками соответствующего программного обеспечения, однако с большой степенью активности и профессионализма занимаются его использованием;

3) специалисты среднего уровня в сфере ИТТ. Характеризуются обладанием соответствующих познаний на уровне уверенных пользователей;

4) «бытовые», «случайные» преступники. Характеризуются невысоким, обывательским уровнем познаний в сфере ИТТ.

Определены специфические признаки, психологические портреты, способы мышления указанных категорий преступников.

Определена типичная структура организованного преступного формирования, занимающегося совершением мошенничества в сфере компьютерной информации: лидер, его заместители, исполнители («разработчики», «системные администраторы», «тестировщики», «взломщики», «заливщики», «скриптописатели», «обнальщики» и др.). Сформулированы характерные черты личности таких преступников.

6. Приведена классификация цифровых следов в зависимости от квалификации лица, явившегося разработчиком использованного ВПО, а также организовавшего и совершившего преступление:

1) следовая картина преступной деятельности *высококвалифицированных* специалистов в сфере ИТТ;

2) следовая картина преступной деятельности *опытных* преступников сфере ИТТ;

3) следовая картина преступной деятельности *специалистов среднего уровня* в сфере ИТТ;

4) следовая картина преступной деятельности «*случайных», «бытовых»* специалистов в сфере ИТТ.

Указаны специфические признаки, характерные черты каждой из групп следов.

7. Специфика преступлений рассматриваемой категории указывает на необходимость проведения комплекса оперативно-розыскных мероприятий (далее ОРМ): получение компьютерной информации, прослушивание телефонных переговоров, снятие информации с технических каналов связи, наблюдение, наведение справок, опрос, исследование предметов и документов и др. С целью изобличения преступной деятельности «организованного» типа мошенничества в

сфере компьютерной информации целесообразно проведение ОРМ «оперативное внедрение».

В целом весь комплекс ОРМ и следственных действий направлен на установление и доказывание прежде всего следующих обстоятельств: способа, места и времени совершения преступления; возможного использования соответствующего ВПО, компьютерных устройств, технических средств и других орудий преступления; совершения сопутствующих преступлений, например создание, использование, распространение вредоносных компьютерных программ (ст. 273 УК РФ) и других обстоятельств.

8. Определены типичные следственные ситуации, складывающиеся на различных этапах выявления, раскрытия, расследования мошенничества в сфере компьютерной информации: четыре следственные ситуации на этапе возбуждения уголовного дела и первоначальном этапе расследования (в зависимости от объема имеющейся информации), а также восемь типичных ситуаций на последующем этапе расследования мошенничества в сфере компьютерной информации.

Разработаны алгоритмы действий следователя в каждой из следственных ситуаций, в т. ч. с учетом нацеленности на изобличение «организованного» типа мошенничества в сфере компьютерной информации.

9. Специфика использования специальных знаний по делам рассматриваемой категории определяется особенностями способов преступлений, при которых преимущественный объем доказательственной информации содержат цифровые следы. Механизм образования таких следов, как правило, не распознаваем без специальных знаний. Определены, систематизированы и описаны формы использования специальных знаний:

1) при подготовке и проведении ОРМ, следственных действий;

2) при получении консультаций и заключений специалиста;

3) при назначении и проведении судебных экспертиз (компьютерно-технических, судебно-бухгалтерских, финансово-экономических, экспертиз реквизитов документов и ряда других).

Предложены рекомендации по недопущению типичных ошибок в рамках использования специальных знаний.

**Теоретическая значимость исследования** заключается в возможности использования сформулированных теоретических положений для дальнейших научных исследований в рамках одного из самых актуальных направлений развития науки, обозначаемого учеными-криминалистами как «использование в криминалистике высоких технологий», «высокотехнологичное право» и т. п., а также для совершенствования имеющихся и создания новых методик расследования преступлений в сфере ИТТ и других сопутствующих общественно-опасных деяний.

**Практическая значимость исследования** состоит в возможности использования его научных положений и прикладных рекомендаций в правоприменительной практике для повышения эффективности выявления, раскрытия и расследования мошенничества в сфере компьютерной информации и сопутствующих преступлений.

Положения, нашедшие отражение в различных разделах диссертационного исследования, могут использоваться для преподавания дисциплины «Криминалистика», спецкурсов по методике расследования преступлений, при подготовке различного рода пособий, а также для профессиональной переподготовки и повышения квалификации сотрудников правоохранительных органов и работников прокуратуры.

**Достоверность и обоснованность результатов исследования** обеспечивается диалектическим методом познания; изучением нормативно-правовых актов, актов нормативного характера, научной и учебной литературы по заявленной и смежным тематикам; изучением судебно-следственной практики и официальных статистических данных; анализом сведений, полученных в результате анкетирования и интервьюирования практических работников.

**Апробация результатов исследования.** Работа выполнена и обсуждена на кафедре уголовного процесса, криминалистики и основ судебной экспертизы юридического института Красноярского государственного аграрного

университета. Основные положения диссертации освещены в 10 научных статьях, 6 из которых опубликованы в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации для опубликования основных научных результатов диссертации.

Результаты исследования были доложены и обсуждены на следующих научно-практических конференциях: XXVI Межвузовская международная научно-практическая конференция студентов и аспирантов, посвященная 70-летию Красноярского ГАУ «Закон и общество: история, проблемы, перспективы» (Красноярск, 2022); XIX Всероссийская научно-практическая конференция «Криминалистические чтения на Алтае» (Барнаул, 2022); XV Всероссийская научно-практическая конференция «Енисейские политико-правовые чтения» (Красноярск, 2023); Научно-практическая конференция (с международным участием) «Криминалистическое изучение личности в правоприменительной деятельности» (Москва, 2023); XIV Всероссийская научно-практическая конференция «Криминалистические и уголовно-процессуальные средства обеспечения экономической безопасности России» (Нижний Новгород, 2023).

Результаты диссертационного исследования внедрены в образовательную деятельность Юридического института ФГБОУ ВО Красноярский ГАУ, Национального исследовательского университета «МИЭТ», Бурятского государственного университета имени Доржи Банзарова, а также в практическую деятельность ЭКЦ ГУ МВД России по Красноярскому краю, Управления криминалистики ГСУ СК России по Красноярскому краю, ГСУ ГУ МВД России по Красноярскому краю.

**Структура диссертационного исследования** определена логикой, целью и поставленными задачами. Диссертация состоит из введения, трех глав, включающих десять параграфов, заключения, списка литературы, приложений.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы исследования, проанализирована степень ее научной разработанности, определены предмет, объект, цель и задачи, методология, теоретическая и эмпирическая основы, сформулирована научная новизна, обоснованность и достоверность диссертационного исследования, изложены положения, выносимые на защиту, теоретическая и практическая значимость исследования, указаны сведения об апробации и внедрении полученных результатов.

**Первая глава «Правовая и теоретическая основы формирования криминалистической методики расследования мошенничества в сфере компьютерной информации»** состоит из двух параграфов.

***В первом параграфе «Мошенничество в сфере компьютерной информации как объект криминалистического исследования»*** приводится используемое в ходе диссертационного исследования понятие «мошенничество в сфере компьютерной информации» в криминалистическом аспекте (положение 1, выносимое на защиту). Указывается, что, как правило, сопутствующими преступлениями, совершаемыми в совокупности с деяниями, предусмотренными ст. 159.6 УК РФ, являются деяния, предусмотренные гл. 28 УК РФ. Кроме того, ими также могут являться преступления, предусмотренные ст. 174, 187, 210 УК РФ и ряд других.

Отмечается, что основанием формирования частной криминалистической методики расследования мошенничества в сфере компьютерной информации является сочетание уголовно-правового и криминалистических критериев.

Криминалистически значимыми критериями выделения исследуемой преступной деятельности являются: специфическая сфера экономической деятельности; специфические способы и предмет преступления; использование в преступной деятельности ресурсов ИТТ; совершение преступлений в определенном пространстве, которое различными учеными именуется, как «виртуальное пространство», «киберпространство», «цифровое пространство», «информационное пространство»; отсутствие непосредственного контакта между

преступником и потерпевшим; зачастую трансграничный характер преступной деятельности; совершение преступления становится возможным в связи с обладанием специальными познаниями в сфере ИТТ, наличием соответствующих уязвимостей информационной инфраструктуры; оставление специфической следовой картины и особый способ сокрытия преступлений.

Указывается, что в качестве предмета мошенничества в сфере компьютерной информации, как правило, используются безналичные денежные средства.

Также в параграфе обосновывается нацеленность методики на освещение наиболее актуальных вопросов расследования преступлений, затрагивающих применение знаний не только науки криминалистики, но и других юридических наук. В этой связи приводятся авторские размышления и мнения различных ученых о целесообразности отнесения составов преступлений, предусмотренных ст. 159.6 УК РФ, к разряду мошенничеств.

Проанализированы статистические данные количества зарегистрированных преступлений, квалифицированных по ст. 159.6 УК РФ с 2012 по 2022 г. Выявлена динамика увеличения указанных показателей до 5 443 к 2015 г. и их снижения до 334 к 2022 г. Определены причины сложившейся ситуации, заключающиеся в наличии проблемных вопросов квалификации деяния. Так, к примеру, деяния, совершенные посредством использования учетных данных собственника, подлежат квалификации по ст. 158 УК РФ, а преступления, совершенные посредством использования поддельных сайтов (например, сайтов интернет-магазинов) – по ст. 159 УК РФ.

***Во втором параграфе «Понятие и особенности формирования криминалистической методики расследования мошенничества в сфере компьютерной информации»*** обозначены принципы формирования методики расследования: нацеленность на изобличение преступной деятельности всего преступного формирования, а также на выявление, раскрытие и расследование сопутствующих преступлений. Определено место, а также сформулировано

понятие методики расследования мошенничества в сфере компьютерной информации (положение 2, выносимое на защиту).

В ходе проведенного исследования выявлены вопросы, вызывающие наибольшие трудности у сотрудников правоохранительных органов в процессе выявления, раскрытия и расследования анализируемой категории преступлений. В число допускаемых ими наиболее распространенных ошибок входит изобличение деятельности лиц, занимающих низшие должности в преступной иерархии преступных формирований, отсутствие нацеленности на изобличение «организованного» мошенничества в сфере компьютерной информации и нераскрытие сопутствующих преступлений. В связи с чем данному вопросу уделено отдельное внимание, в частности определены десять основных причин низкой раскрываемости «организованного» мошенничества.

В параграфе обосновывается необходимость формирования именно частной криминалистической методики расследования исследуемой преступной деятельности. Учитывая специфику такой деятельности, характеризующуюся объемностью и многоаспектностью, указывается на целесообразность включения в формируемую методику лишь ее наиболее значимых аспектов в виде особенностей расследования.

**Вторая глава «Особенности криминалистической характеристики мошенничества в сфере компьютерной информации»** состоит из четырех параграфов.

***В первом параграфе «Типичные способы мошенничества в сфере компьютерной информации»*** указываются выделенные на основе системного анализа наиболее распространенные способы исследуемой категории преступлений (положение 3, выносимое на защиту), проиллюстрированные примерами судебно-следственной практики.

К наиболее характерным действиям на этапе подготовки преступления, в зависимости от его способа, могут относиться следующие: разработка плана и механизма преступной деятельности; получение специальных познаний, навыков и умений в сфере ИТТ либо приискание лиц, ими обладающих; создание

преступного формирования; приобретение соответствующих компьютерных устройств, технических средств, средств связи, средств платежа (банковских, иных платежных карт и т. д.); регистрация электронной почты, установка мессенджеров, программ, сервисов, затрудняющих идентификацию; регистрация юридических лиц, открытие банковских счетов для перенаправления похищенных денежных средств; приобретение в собственность и/или аренда жилых, нежилых помещений; получение конфиденциальной информации, необходимой для совершения хищений; приискание, создание ВПО; поиск, аренда управляющих серверов; создание сайтов, имитирующих официальные сайты; использование в противоправных целях компьютерных сетей, позволяющих организовать доступ к информации, распространение которой в России запрещено; использование различных программ, направленных на сокрытие следов преступной деятельности; изучение деятельности объекта преступного посягательства.

Разработана криминалистическая типология мошенничества в сфере компьютерной информации (положение 3, выносимое на защиту):

1. В зависимости от степени организованности исследуемые преступные посягательства подразделяются на «организованное» и «несложное», или «простое», мошенничество. Указано, что основным критерием разграничения в данном случае является уровень сложности и незаурядности способа подготовки, совершения преступления и сокрытия его следов. Так, преступление, хоть и совершенное в группе лиц, но «несложным», «примитивным» способом, не всегда будет обладать признаками «организованного» мошенничества.

2. В зависимости от уголовно-правовой квалификации рассматриваемые преступления подразделяются на деяния, квалифицируемые только по ст. 159.6 УК РФ, а также квалифицируемые как по этой статье УК РФ, так и по ряду сопутствующих. Приводятся практические примеры указанных типов мошенничества.

***Во втором параграфе «Обстановка совершения мошенничества в сфере компьютерной информации»*** подробно рассмотрены факторы, влияющие на создание определенной плодородной среды, способствующей созданию

благоприятной обстановки исследуемых преступлений. Также определены неблагоприятные, с точки зрения преступников, факторы, влияющие на состояние такой обстановки.

В параграфе указывается на наличие в научном сообществе неоднозначного мнения относительно места совершения данного вида преступлений в связи с присущими ему специфическими особенностями. При этом делается вывод, что в целом одним из определяющих моментов установления места совершения преступления является его способ. Также указывается на наличие мест, обладающих значимой криминалистической информацией, из их числа: места обналичивания денежных средств, места создания, модификации ВПО и др.

Раскрывается одна из особенностей данной преступной деятельности – использование возможностей компьютерного пространства, именуемого как «киберпространство», «виртуальное пространство», «цифровое пространство».

Относительно особенностей еще одного элемента обстановки совершения преступления – времени указывается, что, как правило, на совершение преступления, относящегося к «организованному» типу, может уходить довольно продолжительное время – от нескольких недель до нескольких месяцев. К временным особенностям совершения «организованного» мошенничества также может относиться совершение хищений накануне, а также во время выходных или праздничных дней.

Проведенное исследование позволило сделать вывод о наличии отличительной черты совершения преступлений данной категории в виде обладания соответствующими компьютерными устройствами, программно-аппаратными и другими техническими средствами, что позволяет включить данное обстоятельство в качестве дополнительного элемента обстановки мошенничества в сфере компьютерной информации (положение 4, выносимое на защиту).

***В третьем параграфе «Личность типичных преступника и потерпевшего и их криминалистическое значение»*** приводится классификация личностей типичных преступников в зависимости от обладания

соответствующими специальными познаниями в сфере ИТТ (положение 5, выносимое на защиту).

*Высококвалифицированные специалисты* обладают незаурядными и глубокими познаниями в сфере ИТТ. Сами являются разработчиками высококачественного ВПО, генераторами идей по преодолению программно-технической защиты. Компьютерная среда является для них местом приложения, реализации и развития имеющегося творческого потенциала. Обладают большой степенью уверенности, а порой и самоуверенностью, в возможности успешной реализации преступного умысла в отношении любого объекта посягательства, выбор которого носит избирательный характер. Имеют высокий статус в «своих кругах», к жертвам преступления относятся пренебрежительно. Главной отличительной чертой психологического состояния является подготовка и совершение преступлений с высокой степенью азарта. Имеющийся уровень знаний и опыта, профессиональная интуиция, способность анализировать, сопоставлять, манипулировать имеющейся информацией, прогнозировать возможные исходы различных ситуаций, способность к образному видению отдельных элементов и ситуации в целом позволяют специалистам такого уровня с успехом добиваться поставленной цели.

*Опытные преступники* в сфере ИТТ. Как правило, сами не являются разработчиками программного обеспечения, при этом в процессе эксплуатации уже имеющегося могут заниматься его модификацией. Не всецело погружены в данную сферу деятельности и вполне могут иметь «легальную» работу. Особенностью психологического состояния является обладание неподдельным интересом к совершению таких преступлений, при этом избирательность объекта посягательства не имеет особого значения. Жадность уже не является преобладающим и побуждающим фактором к совершению преступлений. В социальной среде опытных преступников можно определить как психологов, умело подстраивающихся под возможные варианты социального общения. Сознание такого преступника не может образно охватить всю ситуацию по

организации преступной деятельности, в связи с чем ему требуется больше времени на осознание ее отдельных элементов.

*Специалисты среднего уровня* в сфере ИТТ являются обладателями соответствующих познаний на уровне уверенных пользователей. Особенностью психологического состояния является мечтательное представление о достижении возможного уровня высококвалифицированного специалиста, способного на совершение «громких», резонансных, безнаказанных преступлений. Специфическими чертами характера специалистов такого уровня является ворчливость, недовольство собой и окружающими, жадность и лень. Особенностью степени развитости сознания является фрагментарное видение ситуации.

*«Бытовые», «случайные»* преступники, характеризуются невысоким, обывательским уровнем познаний в сфере ИТТ, обладают неуверенностью в своих действиях и их результате. В общении эмоциональны, преобладает хвастовство, амбициозность.

Описана типичная структура организованного преступного формирования, занимающегося совершением преступлений исследуемой категории (положение 5, выносимое на защиту). Так, характеризуя *лидера* преступного формирования, можно отметить, что им, как правило, является высококвалифицированный специалист в сфере ИТТ. Главной психологической особенностью, наряду с обладанием сильными лидерскими качествами, является способность генерировать различные идеи по осуществлению преступной деятельности и проецировать их на других членов преступного формирования. Отличительной чертой *заместителей* является наделение ответственностью за определенное направление деятельности, умение ставить задачи и их контролировать. В параграфе также рассматриваются функциональные обязанности различного рода *исполнителей.* Одной из психологических особенностей исполнителей является мнимое осознание собственной значимости и действительной силы в осуществлении преступной деятельности.

В параграфе также приводятся характерные черты типичных потерпевших: обладание соответствующими материальными благами, доступ к которым осуществляется, в т. ч. посредством преодоления программно-технической защиты; уделение недостаточного внимания соблюдению мер защиты компьютерной информации.

***В четвертом параграфе «Типичные следы мошенничества в сфере компьютерной информации»*** рассматриваются традиционные материальные и идеальные следы, а также следы, образованные в результате взаимодействия с компьютерной информацией, так называемые цифровые следы. По каждой из категории следов приводятся их разновидности, применительно к анализируемой преступной деятельности.

Указывается на наличие специфических особенностей в характере оставляемых цифровых следов в зависимости от квалификации лица, явившегося автором использованного ВПО, а также организовавшего и совершившего преступление (положение 6, выносимое на защиту).

Особенностью *следовой картины преступной деятельности высококвалифицированных специалистов* является создание и применение высококачественного ВПО, которое работает довольно скрытно и изощренно, в связи с чем оставляет в компьютерных устройствах потерпевших незначительные следы и повреждения. *Следовая картина опытных компьютерных преступников* отличается от предыдущей наличием бóльших повреждений и разрушений системы информационной защиты потерпевшего. *Следовая картина специалиста среднего уровня* имеет еще более явный разрушительный характер. Распознать работу такого ВПО на компьютерном устройстве довольно нетрудно. *Следы преступной деятельности «случайных» или «бытовых» преступников* носят еще более распознаваемый, подчас примитивный характер. Довольно часто преступления, совершаемые преступниками такого уровня, характеризуются преимущественным совершением механических манипуляций, следы от которых носят явный характер.

**Третья глава «Особенности расследования мошенничества в сфере компьютерной информации»** состоит из четырех параграфов.

***В первом параграфе «Особенности доследственной проверки и возбуждения уголовного дела»*** указываются типичные источники получения информации о преступлениях исследуемой категории. Отмечается, что ими преимущественно являются заявления физических и юридических лиц, а также сведения, полученные в ходе ОРМ.

В ситуации, когда заявление о преступлении поступило от физических или юридических лиц, наиболее типичными действиями на этапе проверки сообщения являются: получение объяснений, осмотр места происшествия, направление запросов, назначение экспертиз, получение выписок, справок из кредитных организаций, от операторов сотовой связи, провайдеров, инициирование соответствующих финансовых проверок, ревизий и т. д. Особое внимание отводится проведению ОРМ.

При получении объяснений устанавливаются сведения об обстоятельствах совершения хищения, а также о событиях предшествовавших ему. К примеру, скачивание различного рода файлов, установка новых или обновление имеющихся приложений, получение электронных писем как от знакомых, так и незнакомых лиц, некорректная работа компьютерного устройства и т. д. При проведении осмотра места происшествия особое внимание уделяется обнаружению, правильному осмотру и изъятию электронных носителей информации с привлечением специалиста. Как правило, в случаях совершения «организованного» мошенничества при хищении крупных сумм денежных средств у юридических лиц потерпевшие еще до возбуждения уголовного дела обращаются за проведением соответствующих компьютерных экспертиз в организации, специализирующиеся на обеспечении информационной безопасности.

В ситуации, когда сведения о преступлении получены в ходе ОРМ, соответствующее внимание должно отводиться проведению всего необходимого комплекса таких мероприятий, что в случае совершения «организованного»

мошенничества может способствовать изобличению деятельности не только «низовых» исполнителей, но и всего преступного формирования.

Указываются наиболее типичные ОРМ, проводимые в ходе выявления, раскрытия и расследования данного вида противоправной деятельности, а также специфика их проведения. Определены обстоятельства, подлежащие доказыванию (положение 7, выносимое на защиту).

***Во втором параграфе «Типичные следственные ситуации и версии расследования мошенничества в сфере компьютерной информации»*** рассматриваются типичные ситуации на первоначальном и последующем этапах расследования, алгоритм их разрешения (положение 8, выносимое на защиту), а также выдвигаемые в процессе расследования версии.

В зависимости от способа преступления и конкретной ситуации первоначального этапа расследования алгоритм типичных действий по ее разрешению может включать все или часть следующих действий: проведение осмотра места происшествия; обнаружение, изъятие следов преступления, получение образцов для сравнительного исследования, изъятие электронных носителей информации, компьютерных устройств; направление соответствующих запросов, получение выписок о владельцах банковских счетов, движении денежных средств, расходных накладных и других финансовых документов; получение заключений о проведенных внутренних проверках, ревизиях и т. п.; истребование должностных инструкций, трудового договора, правил внутреннего трудового распорядка и т. п.; проверка имеющихся данных об использованных в ходе совершения преступления банковских счетах, абонентских номерах, сайтах в подсистеме «Дистанционное мошенничество» ИБД-Ф на предмет их использования при совершении других преступлений; проведение ОРМ; организация взаимодействия со специалистами Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России и их подразделениями; установление IP-адресов, MAC-адресов, Интернет-провайдеров и проведение выемки необходимой информации за интересующий период времени; организация взаимодействия со специалистами

в сфере ИТТ; назначение соответствующих экспертиз и получение по ним заключений; получение информации посредством изучения записей с камер видеонаблюдения; получение необходимой информации посредством проведения допросов; проведение обысков по месту жительства подозреваемых, в жилых и нежилых помещениях, используемых для совершения преступной деятельности; организация взаимодействия с правоохранительными структурами различных государств, в т. ч. посредством направления соответствующих запросов.

Относительно выделенных типичных ситуаций последующего этапа расследования, при которых собранных доказательств, как правило, уже достаточно, основными задачами являются тактически грамотное проведение следственных и иных действий, правильное оформление всех имеющихся в деле процессуальных документов, в т. ч. оформление и представление результатов ОРД, исключающие возможность признания доказательств недопустимыми.

В ситуациях, когда собранных доказательств недостаточно, целесообразно проведение повторных допросов, очных ставок, назначение экспертиз, проведение ОРМ и т. д.

Также в параграфе рассматриваются выдвигаемые в процессе расследования общие и частные криминалистические версии.

***В третьем параграфе «Тактика производства следственных действий при расследовании мошенничества в сфере компьютерной информации»*** рассматриваются особенности проведения следственных действий с учетом специфики преступлений анализируемой категории.

Особенностью проведения большинства таких действий является привлечение специалиста, обладающего соответствующими познаниями в сфере ИТТ. При проведении осмотра места происшествия, обыска характерна нацеленность на обнаружение и изъятие, наряду с другими видами следов, электронных носителей информации, содержащих цифровые следы. В ходе проведенного анкетирования 20 % респондентов в качестве наиболее распространенных ошибок, указали ошибки, допускаемые в ходе изъятия электронных носителей информации. При этом указывается на возможность

применения преступниками технических мер противодействия, рассматриваются варианты его нейтрализации. Приводятся особенности обращения с носителями цифровых следов на этапах их обнаружения и изъятия, а также указываются рекомендации по проведению их осмотра. Особое внимание обращается на установление видеозаписывающих устройств. С учетом специфики исследуемой преступной деятельности допрос также рекомендуется проводить в присутствии специалиста либо получить от него соответствующую консультацию на этапе подготовки проведения следственного действия.

В параграфе указывается на целесообразность в ходе проведения допроса и других вербальных следственных действий использования описанных в диссертации психологических особенностей и способов мышления различных категорий типичных преступников. Приведены особенности допросов относительно выбранной допрашиваемым позиции, а также с учетом занимаемой роли в преступном формировании.

***В четвертом параграфе «Использование специальных знаний при расследовании мошенничества в сфере компьютерной информации»*** рассматривается специфика применения таких знаний относительно рассматриваемой преступной деятельности (положение 9, выносимое на защиту):

– при подготовке и проведении ОРМ: в ходе проверки по имеющимся информационно-справочным учетам, проведении предварительных исследований, использовании технических средств и т. д. Особую значимость использование специальных знаний имеет в ходе проведения ОРМ. Так, получение компьютерной информации с удаленных компьютерных систем невозможно в рамках проведения следственных действий;

– при подготовке и проведении следственных действий: в ходе осмотра места происшествия (фиксации и изъятии различных видов следов и т. д.), осмотра электронных носителей информации, обыска, допроса и т. д.;

– при получении консультаций и заключений специалиста. Такими специалистами могут быть лица, обладающие специальными познаниями в сфере

ИТТ, оборота криптовалюты, организации сотовой связи, интернет соединений, банковского дела и т. д.;

– при назначении и проведении судебных экспертиз: компьютерно-технической, финансово-экономической, экспертизы реквизитов документов, технико-криминалистической и других видов. Так, 95 % проанкетированных сотрудников отметили компьютерно-техническую экспертизу как одну из наиболее часто назначаемых. Проведенное анкетирование выявило, что треть опрошенных сотрудников, которым приходилось назначать такого рода экспертизы, испытывали трудности в постановке вопросов, что естественным образом может отражаться на достижении целей ее проведения. В этой связи с учетом специфики рассматриваемой преступной деятельности, акцентировано внимание на целесообразности обращения к помощи специалиста уже на стадии назначения компьютерно-технических экспертиз.

В ***заключении*** сформулированы некоторые выводы, сделанные в ходе проведенного исследования.

В ***приложениях*** представлены результаты анкетирования оперуполномоченных, дознавателей, следователей МВД России, занимающихся выявлением, раскрытием, расследованием рассматриваемого вида преступной деятельности; лист интервьюирования практических работников и аналитическая справка по его результатам.

**Основные положения диссертационного исследования опубликованы в следующих научных трудах автора:**

***Статьи, опубликованные в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации:***

1. Харина, Е. А. Некоторые аспекты квалификации мошенничества в сфере компьютерной информации / Е. А. Харина // Российский следователь. – 2022. – № 6. – С. 38–41 (0,49 п. л.).

2. Харина, Е. А. К вопросу о проблемных аспектах квалификации и криминализации мошенничества в сфере компьютерной информации / Е. А. Харина // Российский следователь. – 2023. – № 3. – С. 29–33 (0,47 п. л.).

3. Харина, Е. А. Личность типичного преступника, совершившего мошенничество в сфере компьютерной информации / Е. А. Харина // Российский следователь. – 2023. – № 9. – С. 53–57 (0,45 п. л.).

4. Харина, Е. А. К вопросу о криминалистической характеристике мошенничества в сфере компьютерной информации / Е. А. Харина // Российский следователь. – 2023. – № 11. – С. 11–15 (0,47 п. л.).

5. Харина, Е. А. Типовые следственные ситуации первоначального этапа расследования мошенничества в сфере компьютерной информации / Е. А. Харина // Закон и право. – 2023. – № 11. – С. 273–277 (0,38 п. л.).

6. Харина, Е. А. Типовые следственные версии и планирование расследования мошенничества в сфере компьютерной информации / Е. А. Харина // Закон и право. – 2023. – № 12. – С. 276-279 (0,29 п. л.).

***Публикации в иных изданиях***

7. Харина, Е. А. Некоторые аспекты криминалистической характеристики мошенничества в сфере компьютерной информации / Е. А. Харина // Закон и общество: история, проблемы, перспективы : Материалы XXVI Межвузовской международной научно-практической конференции студентов и аспирантов, посвященной 70-летию Красноярского ГАУ, Красноярск, 21–22 апреля 2022 г. – Красноярск: Красноярский государственный аграрный университет, 2022. – С. 487–490 (0,36 п. л.).

8. Харина, Е. А. К вопросу о типичных способах мошенничества в сфере компьютерной информации / Е. А. Харина // Материалы криминалистических чтений : Материалы чтений, Барнаул, 24 ноября 2022 года / Под редакцией О.В. Кругликовой. – Барнаул: Федеральное государственное казенное образовательное учреждение высшего профессионального образования "Барнаульский юридический институт Министерства внутренних дел Российской Федерации", 2022. – С. 76-77 (0,28 п.л.).

9. Харина, Е. А. К вопросу о личности мошенника в сфере компьютерной информации / Е. А. Харина // Енисейские политико-правовые чтения : сборник научных статей по материалам XV Всероссийской научно-практической конференции, Красноярск, 29–30 сентября 2023 года. – Красноярск: Красноярская региональная общественная организация «Общественный комитет по защите прав человека», 2023. – С. 468-472 (0,26 п. л.).

10. Харина, Е. А. Типичные следы и обстановка мошенничества в сфере компьютерной информации / Е. А. Харина // Криминалистические и уголовно-процессуальные средства обеспечения экономической безопасности России : сборник научных статей по итогам XIV Всероссийской научно-практической конференции (г. Нижний Новгород, 30 ноября 2023 г.) / под редакцией А. Ф. Лубина, А. Ю. Афанасьева, А. В. Смолина. В 2 т. – Н. Новгород: Нижегородская академия МВД России, 2024. – Вып. 5. –Т. I. – С. 241–244 (0,2 п. л.).