Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Красноярский государственный аграрный университет»

На правах рукописи

Харина Елена Алексеевна

ОСОБЕННОСТИ МЕТОДИКИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Специальность 5.1.4. Уголовно-правовые науки
(юридические науки)

Диссертация
на соискание ученой степени
кандидата юридических наук

Научный руководитель –
доктор юридических наук, профессор
Гармаев Юрий Петрович

Красноярск – 2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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

---

[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).

преступления, зарегистрированного с 2012 по 2022 г., в суды направлено 1 602 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

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

привлечение к уголовной ответственности так называемых «низовых» 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.

Глава 1. ПРАВОВАЯ И ТЕОРЕТИЧЕСКАЯ ОСНОВЫ ФОРМИРОВАНИЯ КРИМИНАЛИСТИЧЕСКОЙ МЕТОДИКИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1. Мошенничество в сфере компьютерной информации как объект криминалистического исследования

Происходящие изменения в обществе, спроецированные на общую картину состояния преступного мира, в свою очередь, стимулируют постоянное совершенствование имеющихся и формирование новых методик расследования, научная и практическая значимость которых, во многом определяются предметом исследования, а также выбранным основанием криминалистической методики.

По этому поводу Л. В. Бертовский, В. А. Образцов справедливо заключают, что «в качестве объекта научного криминалистического исследования выступает та или иная проблема, актуальная с теоретической и (или) практической точек зрения, научная разработка которой осуществляется в целях совершенствования указанной выше деятельности. И делается это на основе сравнительного анализа, типизации, классификации, систематизации, дифференциации, интеграции собираемых, интерпретируемых, обобщенных учеными фактических данных, которые затем используются ими в целях создания, адресуемых практике, продуктов научного творчества»[11].

Несомненно, базисным моментом, определяющим направление и угол развития проводимой исследовательской работы и формируемого научного труда, является выбор основания криминалистической методики.

Рассуждения относительно критериев создания криминалистических методик и целесообразности выбора тех или иных оснований в научном сообществе ведутся уже давно.

[11]Бертовский Л. В., Образцов В. А. Понятие, объект и предмет криминалистики // Пробелы в российском законодательстве. 2016. № 4. С. 230.

Видится, что создание методики расследования, основанной только на уголовно-правовом критерии, т. е. на основе уголовно-правовой классификации преступлений, сужающей предмет проводимого исследования, не в полной мере может охватить весь спектр осуществляемой в этой связи преступной деятельности, и, соответственно, не позволит выработать полноценную методику, освещающую все или большинство аспектов в рамках расследования преступлений данной категории. Поэтому, создание криминалистической методики, основанной только на уголовно-правовом критерии, ориентированной на расследование преступления, предусмотренного исключительно введенной в действие ст. 159.6 УК РФ (основной нормы), не в полной мере соответствовало бы избранной нами позиции.

Так, относительно данного аспекта, В. К. Гавло отмечает, что в качестве таких критериев должно выступать *сочетание возможных оснований* (курсив мой. – *Е. Х.*): уголовно-правовых, уголовно-процессуальных, криминалистических, криминологических, позволяющих более точно выявить общие и специфические закономерности механизмов совершения преступлений и ситуаций расследования и познать тенденции формирования и функционирования методики расследования отдельных видов и групп преступлений[12].

При этом общепризнанной является позиция о применении при формировании методики расследования преступлений криминалистических классификаций, позволяющих выделить криминалистически значимые свойства, характерные для определенной группы (вида) преступлений.

Так, А. Ю. Головин отмечает, что «криминалистическая классификация преступлений осуществляется на основе более широкого круга оснований и критериев, чем классификация в науке уголовного права или криминологии»[13].

В. Ю. Белицкий указывает, что «разработка криминалистической классификации мошенничеств необходима для выделения общих, характерных

---

[12] Гавло В. К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск, 1985. С. 134–135.

[13] Головин А. Ю. Базовые криминалистические классификации преступлений // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 2-2. С. 33.

для всех преступлений рассматриваемого вида, криминалистически значимых свойств и признаков, наличие которых послужит основой для создания эффективной полноструктурной методики досудебного производства и судебного разбирательства мошенничеств в целом, а равно может быть использована для разработки частных методик расследования мошенничеств отдельных видов»[14].

Н. П. Яблоков отмечает, что именно «криминалистические основания классификации фактически призваны обеспечить ориентацию следователя в основных обстоятельствах расследуемого преступления, обеспечить собирание доказательств, достаточных для определения уголовно-правового вида расследуемого преступления и быстрейшего решения всех задач его раскрытия»[15].

Таким образом, в качестве выбора основания формирования криминалистической методики расследования преступлений исследуемой группы, определяем сочетание соответствующих уголовно-правовых и криминалистических критериев.

Р. С. Белкиным в качестве направлений формирования частных методик определено совершенствование существующих и разработка новых методик (обусловленных появлением новых составов и новых способов преступлений), а также создание комплексов частнометодических рекомендаций большей степени общности, охватывающих несколько видов и даже родов преступных посягательств, но совершаемых в определенных условиях места, времени либо лицами, характеризуемыми общим для них отличительным признаком[16].

Реализация принципа создания методик более высокого уровня, видится, в т. ч. посредством консолидации и использования знаний криминалистических методик сопутствующих преступлений. О целесообразности применения данного подхода указывается Ю. П. Гармаевым, который, рассматривая соответствующую категорию коррупционных преступлений, указывает, что «для повышения эффективности борьбы с коррупционными преступлениями необходимость

[14] Белицкий В. Ю. Мошенничества и возможные критерии их криминалистической классификации // Вестник Восточно-Сибирского института МВД России. 2021. № 4 (99). С. 179.

[15] Яблоков Н. П. Криминалистическая классификация преступлений в методике расследования и ее виды // Вестник Московского университета. Сер. 11, Право. 2015. № 5. С. 43.

[16] Белкин Р. С. Курс криминалистики : учеб. пособие. М., 2001. С. 751.

изучать криминалистическую характеристику и методику расследования наиболее распространенных «сопутствующих» преступных посягательств: мошенничества, присвоения или растраты, иных хищений, других экономических преступлений, преступлений против правосудия и т. д.»[17]

Действительно, проведенное исследование показало, что одним из отличительных признаков рассматриваемого преступного деяния является его совершение в совокупности с рядом других сопутствующих преступлений. Такими преступлениями преимущественно являются деяния, предусмотренные гл. 28 УК РФ «Преступления в сфере компьютерной информации»: ст. 272 (Неправомерный доступ к компьютерной информации), ст. 273 (Создание, использование и распространение вредоносных компьютерных программ), ст. 274 (Нарушение правил эксплуатации средств хранения…), ст. 274.1 (Неправомерное воздействие на критическую информационную инфраструктуру РФ), ст. 274.2 (Нарушение правил централизованного управления…) УК РФ.

Так, в ходе проведенного анкетирования сотрудников правоохранительных органов, занимающихся выявлением, раскрытием, расследованием рассматриваемых преступлений, на вопрос «Укажите, какие преступления являются сопутствующими при совершении мошенничества в сфере компьютерной информации?» 88,5 % правоприменителей указали ст. 272 УК РФ, 52,8 % отметили ст. 273 УК РФ, 28,1 % респондентов указали ст. 274 УК РФ, 11,6 % отметили ст. 274.1 УК РФ, 18 % правоприменителей указали ст. 274.2 УК РФ. Кроме того, респонденты, в качестве таких преступлений также отметили: ст. 137 (Нарушение неприкосновенности частной жизни), ст. 138 (Нарушение тайны переписки..), ст. 174 (Легализация (отмывание) денежных средств…), ст. 183 (Незаконное получение и разглашение сведений, составляющих коммерческую…), ст. 187 (Неправомерный оборот средств платежей) УК РФ (Приложение 1).

[17]Гармаев Ю. П. Основы методики расследования коррупционных преступлений : курс лекций. Улан-Удэ, 2018. С. 11.

Признак преимущественного совершения мошенничества в сфере компьютерной информации совместно с рядом сопутствующих преступлений получил отражение и в судебной практике. Так, в п. 20 постановления Пленума Верховного Суда РФ № 48, указано, что преступление, предусмотренное ст. 159.6 УК РФ, «совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ»[18].

Так, к примеру, гр. Ш., имевший умысел на хищение денежных средств, в процессе подготовки к совершению преступления приобрел соответствующую вредоносную компьютерную программу, предназначенную для выявления уязвимостей в компьютерных системах управления устройствами самообслуживания банков и получения возможности генерировать команды на выдачу денежных средств. В результате совершения преступления в нескольких регионах РФ были похищены денежные средства, принадлежащие различным банкам, на сумму более 2,5 млн руб. Судом действия фигуранта квалифицированы по ч. 2 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274, ч. 2 ст. 159.6 УК РФ, назначено наказание в виде 2 лет 6 месяцев лишения свободы[19].

Наряду с этим нередко для осуществления длительного, масштабного совершения преступлений рассматриваемой группы, создаются организованные преступные сообщества (преступные организации) (далее ОПС), действия участников которых требуют соответствующей квалификации по ст. 210 УК РФ. К примеру, такой уголовно-правовой оценке были подвергнуты действия участников известных преступных формирований под условными названиями Lurk и Cobalt. Необходимо отметить, что выявление, раскрытие и расследование мошенничества в сфере компьютерной информации, совершенного ОПС под условным наименованием Lurk (далее – дело Lurk), явилось беспрецедентным по

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

[19] Приговор Кировградского городского суда Свердловской области от 05 августа 2016 г. № 1-105/2016. URL: https://sudact.ru/regular/doc/b2ynlm3ERQJ9 (дата обращения: 15.12.2022).

новизне, сложности и рекордным по своему объему. Преступникам удалось похитить более 1,25 млрд руб., материалы уголовного дела насчитывали 2 539 томов, с момента задержания основных подозреваемых и до вынесения обвинительного приговора прошло более пяти лет. Учитывая практическую и научную значимость проведенной работы, не умаляя значимости других случаев раскрытия и расследования рассматриваемых преступных деяний, в данном диссертационном исследовании довольно часто будем обращаться к материалам расследования именно этого беспрецедентного дела.

Указанные обстоятельства еще раз свидетельствуют, что создание криминалистической методики, посвященной расследованию исключительно ст. 159.6 УК РФ, было бы принципиально неверным, существенно сужающим предмет исследования, обедняющим научную и практическую значимость научного труда.

Поэтому в качестве основополагающего избираем указанный Р. С. Белкиным принцип создания криминалистической методики более высокого уровня. Полагаем, что это позволит объединить уже имеющиеся знания о закономерностях расследования с новыми открывшимися аспектами и получить наиболее полное видение картины рассматриваемой преступной деятельности. Данное обстоятельство естественным образом отразится на качественном уровне проведения расследования (что крайне необходимо с учетом катастрофически низкого уровня раскрываемости рассматриваемой группы преступлений) и выявления (что также актуально, учитывая высокий уровень латентности) исследуемых преступных деяний.

Подводя итог вышесказанному, следует отметить, что принимаемое нами в качестве предмета диссертационного исследования понятие «мошенничество в сфере компьютерной информации» не идентично уголовно-правовой норме, а отражает совокупность как основного деяния (ст. 159.6 УК РФ), так и ряда сопутствующих (уголовно-правовой критерий), а также отражает соответствие ряду криминалистических признаков.

Проведенное исследование позволило выделить наиболее существенные криминалистические признаки рассматриваемой категории преступлений, отличающие ее от ряда других и освещение которых способствует более четкому уяснению ее правовой природы.

В качестве одних из основных криминалистических признаков исследуемой деятельности принимаем признаки, сформулированные в пояснительной записке к проекту Федерального закона от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[20], которые также верно отмечены А. В. Чумаковым в своем диссертационном исследовании, посвященном мошенничеству при получении выплат[21]. Итак, в данной пояснительной записке указано: «Уголовный кодекс Российской Федерации предлагается дополнить статьями 159.1–159.6, предусматривающими ответственность также за мошенничество, но специализированное сферой экономической деятельности, в которой оно совершается, и способом совершения преступления, а также особым предметом посягательства» [22] . Итак, рассмотрим данные и другие криминалистические признаки исследуемой преступной деятельности подробнее:

– специфическая сфера экономической деятельности. Рассматриваемые преступления совершаются в сфере отношений по обеспечению экономической безопасности, посредством обеспечения безопасности населения в сфере ИТТ;

– специфические способы совершения преступления, заключающиеся в осуществлении соответствующих неправомерных действий с компьютерной информацией, направленные на хищение денежных средств;

– специфический предмет преступного посягательства. В широком смысле слова им является имущество и право на чужое имущество. Однако,

---

[20] Пояснительная записка к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» // Паспорт проекта федерального закона № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы) // Доступ из справ.-правовой системы «КонсультантПлюс».

[21] Чумаков А. В. Особенности методики расследования мошенничества при получении выплат : дис. … канд. юрид. наук. Калининград, 2018. С. 27–32.

[22] Пояснительная записка к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» …

особенностью преступлений данного вида является то, что, как правило, преимущественное большинство преступлений совершается не в отношении наличных, а в отношении безналичных, электронных денежных средств и т. д.;

– совершение преступлений рассматриваемой категории осуществляется в результате использования ресурсов ИТТ. В зависимости от способа преступлений данные ресурсы могут быть различными: компьютеры, планшеты, смартфоны, различные технические средства, информационно-телекоммуникационная сеть и т. д. В большинстве случаев для совершения преступлений используется ВПО, позволяющее посредством нахождения соответствующих уязвимостей информационной инфраструктуры совершать хищения денежных средств;

– совершение преступлений осуществляется в определенном пространстве, которое различными учеными именуется как «виртуальное пространство» [23], «киберпространство» [24], «цифровое пространство» [25], «информационное пространство» [26]. Более подробно данные понятия будут рассмотрены в параграфе 2.2.;

– отсутствие непосредственного контакта между преступником и потерпевшим. Все имеющиеся на сегодняшний день способы рассматриваемого преступления позволяют констатировать совершение данных деяний без личного контакта преступника и его жертвы. Кроме того, в некоторых случаях, как правило, при списании денежных средств со счетов граждан, о совершении преступления потерпевшие узнают спустя некоторое время, при попытках рассчитаться за покупки, оплатить кредит, и даже после сообщения об этом следователя. Так, к примеру, в ходе расследования одного из уголовных дел было

[23] Ищенко Е. П. Виртуальное пространство как объект криминалистического познания // Криминалистика и судебно-экспертная деятельность в условиях современности : мат-лы Междунар. науч.-практ. конф. (26 апреля 2013 г.) : в 2 т. / Краснодарский университет МВД России. Т. 1. Краснодар, 2013. С. 16–23.

[24] Рассолов И. М. Право и Интернет. Теоретические проблемы. М., 2009. С. 11.

[25] Иванова Л. В., Пережогина Г. В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6, № 4 (24). С. 155–171.

[26] О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы …

выявлено, что сотрудники банка списывали денежные средства со счетов, которыми длительное время не пользовались их владельцы[27];

– трансграничный характер преступной деятельности. Современный уровень развития ИТТ предоставляет возможность совершать преступления на территории различных государств, независимо от места нахождения преступника и потерпевшего. Так, к примеру, преступное сообщество Cobalt совершило хищения денежных средств более чем в 40 странах мира, ущерб составил более чем 1 млрд евро[28];

– совершение преступления становится возможным в связи с обладанием соответствующими специальными познаниями в сфере ИТТ. В зависимости от способа преступления**,** степень обладания такими познаниями может значительно разниться. Так, при совершении преступления сотрудником банка посредством входа в банковскую компьютерную систему и осуществления действий по изменению состояния денежного счета требуются познания в обращении с соответствующими компьютерными средствами и процедуре осуществления банковских операций. А совершение преступления посредством написания высококачественной современной вредоносной компьютерной программы, обладающей способностями нераспознаваемости, самоустраняемости и позволяющей длительное время совершать хищения в крупных финансовых организациях, требует наличия специальных знаний и умений высокого уровня;

– оставление в результате совершения преступления специфической следовой картины. Существенной особенностью рассматриваемой категории преступлений является оставление в ходе совершения преступления, кроме традиционных материальных и идеальных следов, следовой картины, образуемой в результате взаимодействия с компьютерной информацией. Различными авторами такие следы именуются как «виртуальные следы» [29] , «бинарные

[27]Уголовное дело № 1-675/2019 // Архив Советского районного суда г. Красноярска.

[28]Cobalt (хакерская группа). URL: https://ru.wikipedia.org/wiki/Cobalt_(хакерская_группа) (дата обращения: 12.01.2022).

[29]Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001. С. 112.

следы»[30], «информационные следы»[31], «цифровые следы»[32]. В диссертационном исследовании приведена авторская классификация таких следов в зависимости от уровня квалификации лица, совершившего преступление;

– осуществление преступной деятельности становится возможным в результате наличия соответствующих уязвимостей информационной инфраструктуры. Так, к примеру, к их числу относятся уязвимости программно-технической защиты мобильных устройств, работающих на платформе Android, позволяющие совершать хищения денежных средств с банковских карт, подключенных к системе «Мобильный банк». Также к числу таких уязвимостей относятся различного рода уязвимости программно-технической защиты устройств дистанционного банковского самообслуживания (далее – ДБО), позволяющие посредством использования ВПО совершать хищения денежных средств. Особую пособническую роль в совершении рассматриваемой группы преступлений занимают утечки персональных данных и информации ограниченного доступа. Так, к примеру, в октябре 2019 г. за 300 млн руб. на продажу были выставлены данные 60 млн пластиковых карт «Сбербанка»[33]. В октябре 2023 г. Роскомнадзор подтвердил утечку персональных данных почти 1 млн клиентов МТС-банка[34];

– особый способ сокрытия следов осуществления преступной деятельности. Одной из особенностей рассматриваемых преступлений является совершение действий по сокрытию следовой картины преступления на этапе подготовки к его совершению. В этой связи преступниками предпринимаются меры по сокрытию мест совершения преступления, IP-адресов, MAC-адресов, использованию VPN-сервисов (от англ. Virtual Private Network – виртуальная частная сеть), программ-«ремейлеров», «анонимайзеров» и т. д., использование для общения

[30]Милашев В. А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. …канд. юрид. наук. М., 2004. С. 17.

[31] Борисов В. В. Об особенностях фиксации информационных следов в практике защиты информации // Известия ЮФУ. Технические науки. 2020. № 5 (94). С. 164–168.

[32] Цифровая криминалистика: учеб. для вузов / В. Б. Вехов [и др.]. 2-е изд. перераб. и доп. М., 2024. С. 97.

[33] 10 громких преступлений, за которыми стояли русские хакеры. URL: https://vc.ru/flood/92374-10-gromkih-prestupleniy-za-kotorymi-stoyali-russkie-hakery (дата обращения: 02.02.2023)

[34]Роскомнадзор подтвердил факт утечки данных из МТС-банка. URL: https://www.vedomosti.ru/finance/articles/2023/10/19/1001370-roskomnadzor-podtverdil-fakt-utechki-dannih-iz-mts-banka (дата обращения: 29.10.2023).

мессенджеров, затрудняющих идентификацию пользователей, написание и/или использование ВПО, нацеленного на минимизацию оставления следов преступной деятельности. Особенностью компьютерной информации является наличие возможности ее удаления независимо от близости соответствующих компьютерных средств. Нередко для уничтожения следов преступной деятельности используются специальные технические средства, позволяющие, к примеру, незамедлительно уничтожать цифровые следы при появлении сотрудников правоохранительных органов.

Полагаем, одним из принципиальных направлений формируемой криминалистической методики должна являться ее нацеленность на освещение наиболее актуальных вопросов расследования преступления, затрагивающих применение знаний не только науки криминалистики, но и других сопровождающих преступление юридических наук.

В научном сообществе и ранее обращалось внимание на необходимость применения данного подхода. Так, целесообразность создания криминалистической методики, сочетающей в себе знания двух юридических наук, криминалистики и оперативно-розыскной деятельности, была верно отражена Н. В. Поляковым, в ходе создания методики расследования незаконного обналичивания и транзитирования денежных средств, «так как ориентирована не только на следователей (как большинство криминалистических методик), но и оперативных сотрудников»[35].

Поддерживаем предложенную ученым стратегию и применительно к созданию данной криминалистической методики. Так, специфика расследования рассматриваемой категории преступлений позволяет сделать вывод о том, что важнейшая роль получения информации, способствующей наиболее рациональному и успешному проведению расследования, отводится проведению соответствующих мероприятий до возбуждения уголовного дела. Акцентирование внимания оперативных сотрудников на необходимость проведения определенных мероприятий и их особенностях, качественно повысит возможность получения

[35] Поляков Н. В. Особенности методики расследования незаконного обналичивания и транзитирования денежных средств : дис. ... канд. юрид. наук. Красноярск, 2021. С. 19.

наиболее полной информации и сделает неоценимым их вклад в процесс расследования преступления.

С целью получения наиболее системного научного знания о мошенничестве в сфере компьютерной информации как явления в целом, считаем целесообразным рассмотрение данного преступного деяния и с позиции уголовного права. Данная необходимость вызвана наличием дискуссионных вопросов о целесообразности криминализации введенной нормы в принципе, степени корректности отнесения законодателем данного преступления к разряду мошенничеств, а также наличием трудностей в квалификации деяния. И если своевременность, практическая необходимость и целесообразность законодательного урегулирования данного вида правоотношений не вызывает никаких сомнений, то степень актуальности обращения внимания ученых-юристов к рассмотрению второго вопроса считаем, безусловно, оправданной.

В научном сообществе по поводу корректности расположения ст. 159.6 в Особенной части УК РФ существуют различные точки зрения.

Так, Е. А. Русскевич предлагает именовать рассматриваемое преступное деяние «Статья 159.6. Хищение в сфере компьютерной информации», где часть первую изложить следующим образом: «Хищение чужого имущества или приобретение права на чужое имущество путем вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-коммуникационных сетей»[36].

По мнению М. А. Ефремовой, очевидна необходимость включения в ст. 158, 159, 160, 163 УК РФ специального признака – «с использованием информационно-телекоммуникационных технологий»[37].

Как считает М. А. Фролов, решение проблемы заключается не в исключении, а в переименовании ст. 159.6 УК РФ – «Хищение, совершенное с использованием информационно-телекоммуникационных технологий»[38].

---

[36] Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-телекоммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020. С. 415.

[37] Ефремова М. А. Уголовно-правовая охрана информационной безопасности : дис. … д-ра юрид. наук. М., 2017. С. 319.

[38] Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации : дис. ... канд. юрид. наук. М., 2018. С. 147.

С позиции А. А. Южина, норма о мошенничестве в сфере компьютерной информации была полностью провальной. Отнесение нормы в главу 21 («Преступления против собственности»), а не в гл. 28 («Преступления в сфере компьютерной информации»), было ошибочным[39].

Г. Р. Григорян полагает, что введение в близком или отдаленном будущем тех или иных новых составов имущественных нарушений одновременно потребует исключения из УК РФ положений, содержащихся в п. «г» ч. 3 ст. 158, ст. 159.3, ст. 159.6. Более реалистичным для эффективного уголовно-правового противодействия преступлениям против собственности в сфере компьютерной информации считает дополнение УК РФ новой ст. 165.1 «Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации»[40].

Как ранее отмечалось, наша принципиальная позиция заключается в поддержании целесообразности и необходимости криминализации данного преступления, а также в теоретическом восстановлении и проявлении его практической сути.

Как известно, основным принципом соотношения общей и специальной нормы является то, что специальная норма обладает всеми признаками общей нормы, при этом конкретизирует лишь определенные, специфические признаки преступления. Иначе говоря, эти два деяния в зеркале отображения должны быть идентичны по сути и различаться лишь по форме и характерным признакам, например, как соотносятся между собой «А» и «А1», но ни в коей мере не как «А» и «1».

Исходя из анализа составов объективной стороны преступлений, предусмотренных ст. 159 УК РФ и ст. 159.6 УК РФ, очевиден отход от этого базового принципа, породивший полную или частичную нераспознаваемость, повлекшую не единообразную практику правоприменения. В частности в п. 1

[39] Южин А. А. Мошенничество и его виды в российской уголовном праве : дис. .. канд. юрид. наук. М., 2016. С. 196.

[40] Григорян Г. Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации : дис. … канд. юрид. наук. Самара, 2021. С. 185–186.

постановления Пленума Верховного Суда РФ № 48 [41] указано, что обман и злоупотребление доверием не являются способами хищения чужого имущества или приобретения права на чужое имущество при мошенничестве в сфере компьютерной информации.

Очевидно, что ст. 159.6 УК РФ явилась единственным составом мошенничества, в котором отсутствует его ключевой признак – обман и злоупотребление доверием, т. е. исследуемое преступление является мошенничеством только по форме – названию, но не по сути[42].

Так, судом признаны несостоятельными доводы организатора ОПС Lurk гр. К., что обвинение по мошенничеству не конкретизировано, поскольку не указан способ совершения – путем обмана или злоупотребления доверием[43].

Таким образом, с учетом аргументирования изложенных доводов, считаем принципиально верной позицию Е. А. Русскевича, предлагающего теоретически скорректированное определение преступного деяния представить следующим образом: «Хищение в сфере компьютерной информации»[44].

Продолжая придерживаться выбранного стратегического направления по рассмотрению наиболее актуальных вопросов исследуемого деяния с позиции различных научных знаний, без учета которых его истинная картина была бы не полной, необходимо обратиться к категории его квалификации.

Анализ судебно-следственной практики указывает на существование различных, расходящихся между собой позиций правоприменителей относительно вопросов квалификации деяния, породив не единообразные варианты толкования уголовно-правовой нормы[45]. При этом принципиально верна

---

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

[42] Харина Е. А. К вопросу о проблемных аспектах квалификации и криминализации мошенничества в сфере компьютерной информации // Российский следователь. 2023. № 3. С. 29–33.

[43] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1. URL: https://kirovsky--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=2&name_op=doc&number=352801331&delo_id=1540006&new= 0&text_number=1(дата обращения: 10.10.2023).

[44] Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-телекоммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020. С. 415.

[45] Харина Е. А. Некоторые аспекты квалификации мошенничества в сфере компьютерной информации // Российский следователь. 2022. № 6. С. 39.

позиция Ю. П. Гармаева, что низкий уровень раскрываемости тех или иных преступных деяний заключается в феномене нераспознаваемости некоторых видов преступлений. В данном случае речь идет об упрощенных, шаблонных представлениях некоторых правоприменителей о преступности или непреступности, доказуемости или недоказуемости тех или иных преступных посягательств[46].

Иллюстрируя степень актуальности данного вопроса, для наглядности приведем схематичный образ количества зарегистрированных преступлений, квалифицированных по ст. 159.6 УК РФ с момента криминализации деяния по 2022 г. на диаграмме 1.

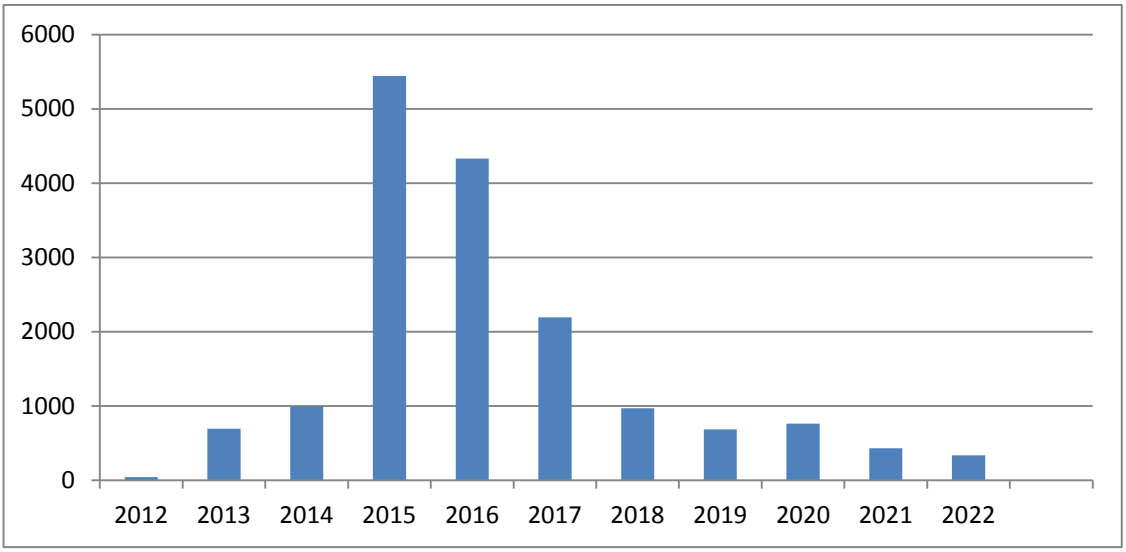

Диаграмма 1 – Количество зарегистрированных преступлений, квалифицированных по ст. 159.6 УК РФ

Итак, мы видим динамику постепенного увеличения количества зарегистрированных преступлений с 43 в 2012 г. до 5 443 в 2015 г. и их снижения до 334 к концу 2022 г. Данный факт объясняется реализацией в судебно-следственной практике разъяснений, изложенных в постановлении Пленума

[46] Гармаев Ю. П. Незаконная деятельность адвокатов в уголовном судопроизводстве : учебник. М., 2005. С. 113.

Верховного Суда РФ № 48. В частности в п. 21 даны разъяснения относительно совершения преступления с использованием сервиса «мобильный банк» – «в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия подлежат квалификации как кража[47].

Отметим, что ранее, с момента введения в действие исследуемого преступного посягательства, квалификация деяний, совершенных подобным способом вызывала немало трудностей и породила не единообразную правоприменительную практику. Так, подобные деяния квалифицировались и по ст. 159 УК РФ, по ст. 159.6 УК РФ, и по ст. 158 УК РФ.

Типичным примером подобной практики служат материалы уголовного дела, в соответствии с которыми Б. и малознакомая ей М. проходили лечение с детьми в «Братской детской городской больнице». Воспользовавшись временным отсутствием в палате М., Б. взяла с прикроватной тумбы сотовый телефон SamsungGT-S 5310, принадлежащий М., и увидела SMS-сообщение со специального номера «900» о балансе денежных средств лицевого счета банковской карты М. в ПАО «Сбербанк России». Путем использования подключенной к карте дистанционной финансовой услуги «Мобильный банк» Б. осуществила перевод денежных средств в сумме 5 000 руб. на лицевой счет карты указанного банка, оформленный на свое имя. Впоследствии данные денежные средства получила в банкомате в наличном виде[48]. Действия Б. судом квалифицированы по ч. 2 ст. 159.6 УК РФ[49].

Нельзя переоценить значимость разъяснений, данных во втором абзаце п. 21 постановления Пленума Верховного Суда РФ № 48, согласно которым, «если

---

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

[48] Харина Е. А. К вопросу о проблемных аспектах квалификации ... С. 29–33.

[49] Приговор Братского городского суда Иркутской области от 19 декабря 2016 г. № 1-558/2016. URL: https://sudact.ru/regular/doc/g09gU4WUC15J (дата обращения: 15.07.2022).

хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159, а не 159.6 УК РФ»[50].

Необходимо отметить, что ранее такие преступления, в частности совершенные посредством методов «социальной инженерии», квалифицировались как мошенничество в сфере компьютерной информации.

Указанное и другие обстоятельства, в т. ч. связанные с имеющимися пробелами уголовно-правового закона, сопровождавшиеся отсутствием у правоприменителей должного уровня специальных познаний в сфере ИТТ, способствовали увеличению количественных показателей совершаемых преступлений по ст. 159.6 УК РФ и отражали мнимое состояние действительности в данной сфере правоотношений [51].

Кроме того, проведенное исследование выявило, что, несмотря на имеющиеся законодательные разъяснения по вопросу квалификации данного деяния, у правоприменителей и в настоящее время имеются соответствующие правовые пробелы. Так, в качестве способов преступления респонденты отмечали методы социальной инженерии, обман и введение в заблуждение посредством осуществления телефонных звонков от сотрудников правоохранительных органов, банков и т. д., при том что 68,6 % лиц, принимавших участие в опросе, являются опытными сотрудниками, имеющими стаж работы от 5 и более лет. (Приложение 1).

Рассматривая мошенничество в сфере компьютерной информации с позиции уголовного права, необходимо упомянуть и о его предмете. Так, в ходе проведенного анкетирования на вопрос «Укажите, какие виды имущества наиболее часто становились предметами мошенничества в сфере компьютерной

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

[51] Харина Е. А. К вопросу о проблемных аспектах квалификации ... С. 29–33.

информации» 85,2 % сотрудников отметили безналичные денежные средства, 48,1 % указали электронные денежные средства, 27,8 % – криптовалюту, 21,3 % – наличные денежные средства, 14,7 % – цифровую валюту, 8 % – денежные суррогаты (премиальные мили, игровая валюта) (Приложение 1). Как можно заключить, как правило, действия преступников направлены на хищение безналичных денежных средств, что является отражением специфики способов совершения рассматриваемых преступлений.

Итак, как мы видим, криминализованный более десяти лет назад новый вид преступного деяния обладает определенными специфическими особенностями, что нередко вызывает у правоприменителей соответствующие трудности, на минимизацию которых и направлено настоящее диссертационное исследование.

1.2. Понятие и особенности формирования криминалистической методики расследования мошенничества в сфере компьютерной информации

Как уже отмечалось, возможности, предоставляемые постоянно совершенствующейся сферой ИТТ, не всегда используются исключительно в правовом поле. Ежедневно создающееся новое ВПО и другие плоды научно-технического прогресса способствуют усовершенствованию имеющихся и появлению новых способов преступлений в данной сфере. В связи с этим, возрастание степени уязвимости людей, связанное с расширением сферы влияния ИТТ на все сферы жизни общества, требует обращения к данному вопросу более пристального внимания и соответствующего государственного, в т. ч. уголовно-правового реагирования.

При этом необходимо признать, что достижение оптимального результата в противодействии данным преступным проявлениям требует системного подхода, выражающегося в искоренении причин и условий данного направления преступной деятельности. Видится, что достижению данной задачи может способствовать усовершенствование мер технической безопасности информационных продуктов, повышение компьютерной грамотности населения,

контролирование пространства теневого Интернета, профессиональное противодействие возможным кибератакам, привлечение к работе в сфере ИТТ высококвалифицированных специалистов, совершенствование механизма международного сотрудничества в расследовании преступлений в сфере ИТТ, а также применение других мер противодействия.

Применение ответных мер на ставшие явными проявления пренебрежения правовой охраны данной сферы отношений также должно носить системный характер и в том числе заключаться в оснащении правоохранительных структур современными техническими средствами, усовершенствовании методик проведения экспертных исследований, создании специализированных баз данных, подготовке соответствующих квалифицированных кадров и создании подразделений, специализирующихся на противодействии рассматриваемому виду преступлений (Приложение 3). При этом одну из ключевых позиций данной деятельности занимает создание новых и усовершенствование имеющихся методик расследования преступлений рассматриваемой категории.

Проведенный анализ статистических данных указывает и на наличие проблемных вопросов в эффективности расследования мошенничества в сфере компьютерной информации. Так, согласно официальным данным МВД РФ, в 2012 г. зарегистрировано 43 преступления, предусмотренного ст. 159.6 УК РФ, в суд ни одно из них не направлено; в 2013 г. – 693 преступления, в суд направлено 192; в 2014 г. – 995, в суд направлено 237; в 2015 г. – 5 443, в суд направлено 282; в 2016 г. – 4 329, в суд направлено 284; в 2017 г. – 2 195, в суд направлено 172; в 2018 г. – 970, в суд направлено 78; в 2019 г. – 687, в суд направлено 54; в 2020 г. – 761, в суд направлено 98; в 2021 г. – 431, в суд направлено 133; в 2022 г. зарегистрировано 334 преступления, в суд направлено 72. В целом из 16 681 зарегистрированного преступления в суд направлено 1 602 уголовных дела, т. е. более чем в десять раз меньше[52].

При этом необходимо учесть и высокую латентность рассматриваемого вида преступных посягательств. Определенная часть лиц, столкнувшихся с такого рода преступным воздействием, для которых, вероятно, причиненный ущерб

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

является не таким значительным, как правило, не спешат обращаться в правоохранительные органы по различным причинам, одной из которых является отсутствие должной уверенности в установлении преступника и возмещении причиненного ущерба. Анализ раскрываемости исследуемых преступлений не позволяет категорически отрицать возможность актуальности данных позиций.

Таким образом, официальные статистические данные, изучение практики расследования уголовных дел рассматриваемой категории, а также состояние ее латентности определенно указывают на наличие существенных трудностей изобличения преступной деятельности.

Одним из вариантов нивелирования сложившейся ситуации видится создание соответствующей методики расследования, которая способствовала бы наиболее эффективному выявлению, раскрытию и расследованию таких преступлений, что неминуемо может отразиться на повышении уровня доверия населения к эффективности механизма уголовно-правовой защиты интересов граждан.

Как справедливо заключает Р. Н. Боровских, преимущественно авторы базовых методик обосновывают их создание: «1) общественной опасностью деяний, их распространенностью; 2) низкой раскрываемостью, ненадлежащим качеством расследования соответствующих дел; 3) недостаточной, по их мнению, компетентностью правоприменителей по проблеме расследования соответствующих преступлений, и т. д.». При этом в качестве средства обоснования считает необходимым в том числе указание результатов проведенного анкетирования[53].

В данном контексте также поддерживаем позицию Н. В. Полякова об эффективности изучения исследуемой преступной деятельности посредством применения метода экспертных оценок[54].

Итак, проведенное исследование, выразившееся, в том числе, в сочетании указанных авторами методов, указало на катастрофически низкую

[53] Боровских Р. Н. Теоретические основы и прикладные аспекты расследования преступлений в сфере страхования : дис. … д-ра юрид. наук. М., 2018. С. 50.

[54] Поляков Н. В. Указ. соч. С. 43.

раскрываемость рассматриваемого деяния, наличие проблем соответствующей подготовки правоприменителей, а также следующих трудностей, с которыми они сталкивались в ходе выявления, раскрытия, расследования мошенничества в сфере компьютерной информации, в т. ч.: несвоевременное сообщение о преступлении, в результате чего частичная или полная утрата цифровых следов преступления; сложности в установлении схемы совершения преступления и похищенных денежных средств из-за дробления, перенаправления похищенного на различные банковские счета, электронные кошельки, перевода в криптовалюту и т. п.; сложности в установлении места совершения преступления в результате использования VPN-сервисов, программ-«ремейлеров», «анонимайзеров», управляющих серверов, расположенных на территории других государств; совершение преступления из-за пределов РФ, отсутствие должного взаимодействия с правоохранительными структурами других государств; недостаточный объем следовой картины преступления в результате работы вредоносных компьютерных программ; сложности в установлении преступников в результате использования для общения мессенджеров, затрудняющих идентификацию пользователей, содержание разговоров, переписки; отсутствие специальных познаний и должной квалификации лиц, производящих выявление, раскрытие, расследование преступления; отсутствие методических рекомендаций по выявлению, раскрытию и расследованию мошенничества в сфере компьютерной информации; сложности в установлении преступников в результате использования банковских и иных платежных карт, расчетных счетов, электронных кошельков и т. п., как правило, оформленных на подставных лиц; длительный срок проведения экспертиз; длительный срок получения ответов на запросы от кредитно-финансовых организаций, провайдеров и т. п. (Приложение 3); трудности в привлечении специалистов, обладающих соответствующими познаниями (Приложение 1).

Также совершенно согласны с мнением О. А. Науменко, определившей в данной связи следующие проблемы: отсутствие у РФ договоров с некоторыми иностранными государствами об оказании правовой помощи в расследовании

уголовных, в результате чего исполнение запросов на установление реального IP-адреса занимает длительный период времени; длительность получения информации от компаний сотовой связи других регионов; неэффективность использования автоматизированных баз; отсутствие индивидуального подхода к составлению плана согласованных ОРМ и следственных действий; недостаточное количество экспертов, имеющих допуск к производству компьютерно-технических экспертиз, длительность и высокая стоимость их производства[55].

В. О. Давыдовым, И. В. Тищутиной также определяются следующие актуальные проблемы: длительность получения из компаний сотовой связи криминалистически значимой информации; использование для совершения преступлений sim-карт и банковских карт, оформленных на третьих лиц; проблемы, связанные с идентификацией пользователей; отсутствие механизма блокирования ВПО для операционных систем мобильных устройств; необходимость систематизации информации о таких мошенничествах в рамках единой базы данных, а также создания автоматизированных систем мониторинга сети Интернет[56].

Как видим, перечень существующих проблем довольно солидный, одной из них является отсутствие соответствующих методических рекомендаций. Так, как уже отмечалось, на вопрос «Нужна ли отдельная криминалистическая методика расследования мошенничества в сфере компьютерной информации?» 80,2 % респондентов ответили утвердительно (Приложение 1).

Наряду с вышеуказанным проведенное исследование выявило еще одну закономерность, заключающуюся в том, что, как правило, осужденными за совершение мошенничества в сфере компьютерной информации являются лица, занимающие низшие должности в преступной иерархии хакерских преступных объединений. При этом установление высшего и среднего руководящего состава

---

[55] Науменко О. А. Проблемы в расследовании уголовных дел о мошенничестве, совершенном с использованием информационно-телекоммуникационнй среды // Вестник Краснодарского университета МВД России. 2019. № 3 (45). С. 62–63.

[56] Давыдов В. О. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 84-85.

преступных формирований в ходе проведения расследования становится невозможным. Данное обстоятельство позволяет неустановленным лицам продолжать совершать действия по приготовлению, совершению преступлений и сокрытию их следов. Достижение ситуации неизобличаемости организаторов и других членов преступных объединений обеспечивается различными средствами.

Как видим, еще одной из существенных проблем считаем расследование единичных преступных посягательств в условиях неизобличаемости так называемого «организованного» мошенничества в сфере компьютерной информации, в связи с чем об искоренении преступной активности в данной сфере говорить не приходится.

При этом пресечение деятельности исполнителей низшего звена сопоставимо с удалением наземных верхушек сорняков при сохранении их корневой структуры. В результате чего, спустя непродолжительное время, несмотря на проведенные аресты членов преступного формирования, мы являемся свидетелями продолжающегося проявления преступной активности, характерной для данного конкретного объединения.

В этой связи автор совершенно согласен и поддерживает позицию Ю. П. Гармаева, указавшего «на наличие в деятельности правоохранительных органов негативной закономерности, некоего неформального приоритета борьбы с мелкими преступлениями, не представляющими правовой и криминалистической сложности», а также нацеленности множества научных криминалистических разработок, в т. ч. методик расследования, на расследование мелких, несложных преступлений[57].

Данное обстоятельство находит свое подтверждение и в результатах проведенного исследования. Так, 23,1 % правоприменителей указали отсутствие нацеленности на раскрытие «организованного» мошенничества в сфере компьютерной информации как одну из допускаемых ошибок. Также респондентами выделены наиболее актуальные причины низкой раскрываемости

[57] Гармаев Ю. П. Преимущественная борьба с «мелкими» коррупционными преступлениями как проблема практики и криминальной науки // Lexrussica. 2023. № 76 (3). С. 63.

«организованного» мошенничества в сфере компьютерной информации, среди которых отсутствие соответствующих методических рекомендаций. 80,4 % опрошенных сотрудников указали, что более эффективно способствовать борьбе с данного вида преступлениями может криминалистическая методика, ориентированная на расследование «организованного» мошенничества (Приложение 1).

Поэтому, при построении методики расследования мошенничества, исходим из принципа нацеленности на изобличение деятельности всего преступного формирования, что именно и является действенной мерой противодействия данному виду противоправного поведения.

Как ранее нами уже указывалось, одной из особенностей совершения мошенничества в сфере компьютерной информации является факт его преимущественного совершения совместно с другими сопутствующими преступлениями. При этом в качестве еще одной из ошибок проводящихся расследований опрошенные респонденты указали отсутствие нацеленности на раскрытие сопутствующих преступлений (Приложение 1). Поэтому направленность формируемой методики на выявление и расследование всей совокупности преступных проявлений является еще одним избранным нами принципиальным подходом.

Резюмируя вышеуказанное можно отметить, что катастрофически низкая степень раскрываемости исследуемых деяний, высокий уровень латентности, недостаточное количество в настоящее время методик расследования, нацеленных на выявление и раскрытие «организованного» мошенничества в сфере компьютерной информации, а также сопутствующих преступных проявлений, постоянно совершенствующиеся способы совершения преступлений в данной сфере выявляют необходимость создания настоящей методики расследования.

Как уже отмечалось, появление в 2012 г. в УК РФ нового состава – мошенничество в сфере компьютерной информации и отсутствие до 2017 г. каких-либо законодательных регламентаций применения данной нормы породило не единообразную правоприменительную практику, обозначив накопившиеся

проблемные вопросы и необходимость их разрешения, в т. ч. посредством формирования соответствующей методики расследования.

Важным вопросом при формировании методики расследования мошенничества в сфере компьютерной информации является ее определение относительно сформировавшихся в научных работах подходов к их криминалистической классификации.

Так, по степени общности, В. А. Образцов разделил все имеющиеся методики на частные и общие, состоящие из комплекса методик расследований определенных групп криминалистически сходных видов преступлений[58].

Ю. П. Гармаев и А. Ф. Лубин, также по степени общности, выделяли общие и частные методики. Так, под такими методиками авторы понимали комплекс научно обоснованных рекомендаций по расследованию группы (нескольких групп) преступлений и конкретного вида преступления, выделенных по уголовно-правовому или криминалистическому основанию [59] . Также авторами все методические рекомендации по объему подразделяются: на полные (собственно методики) и сокращенные (основы методики, особенности методики, отдельные методические рекомендации [60] . В приведенных классификациях формируемая нами методика относится к частной на основании указанных в первом параграфе критериев, являющаяся не полноструктурной, а содержащая только ее особенности.

Также по степени общности А. В. Шмонин выделяет простые и комплексные криминалистические методики. Простые подразделяются на монородовые, моносоставные, моновидовые, а комплексные – на монообъектные (монородовые, моновидовые, моносоставные) и полиобъектные (полиродовые, поливидовые)[61]. В данном случае формируемая нами методика расследования мошенничества в сфере компьютерной информации является комплексной, полиобъектной методикой.

---

[58] Криминалистика / под ред. В. А. Образцова. М., 1995. С. 374–375.

[59] Гармаев Ю. П. Проблемы создания криминалистических методик расследования преступлений. Теория и практика. СПб., 2006. С. 163.

[60] Там же. С. 184–189.

[61] Шмонин А. В. Методология криминалистической методики : монография. М., 2010. С. 140–141.

Н. П. Яблоков относительно уровня конкретизации методических рекомендаций имеющиеся методики разделил на методики высокой, меньшей, еще меньшей и частной степени общности [62] . Полагаем, что в данной классификации методика расследования мошенничества в сфере компьютерной информации относится к группе еще меньшей степени общности, включающей в себя видовые и подвидовые методики расследования.

В зависимости от используемых научных знаний И. А. Возгрин подразделял методики на собственно криминалистические и комплексные [63]. К последнему виду относится и формируемая нами методика расследования, сочетающая в себе знания не только криминалистики, но и уголовного права, оперативно-розыскной деятельности.

Исследование, проведенное Р. Н. Боровских, позволило сделать вывод, что «некоторые ученые видят возможности дальнейшего развития заключительного раздела криминалистической науки в разработке базовых (укрупненных) методик расследования преступлений»[64].

Хотелось бы прокомментировать данные тезисы применительно к формируемой нами криминалистической методике. Считаем, несмотря на важность создания общих методик расследования, нельзя отрицать научную и прикладную значимость и частных методик, особенно это касается формируемой нами частной методики расследования мошенничества в сфере компьютерной информации. Аргументируем наше мнение. Так, общей методикой расследования в нашем случае может являться методика расследования мошенничеств, основные положения которой должны применяться при расследовании различных его видов. Однако, как уже отмечалось, мошенничество в сфере компьютерной информации является единственным специальным составом мошенничества, в котором отсутствует его ключевой признак – обман или злоупотребление доверием. Напомним, что основными криминалистическими признаками данной

[62] Криминалистика. В 5 т. Т. 5. Методика расследования преступлений : учеб. для вузов / И. В. Александров [и др.]. М., 2023. С. 17.

[63] Возгрин И. А. Введение в криминалистику: история, основы теории, библиография. СПб., 2003. С. 287–294.

[64] Боровских Р. Н. Указ. соч. С. 51.

нормы являются: отсутствие непосредственного контакта между преступником и потерпевшим, совершение преступления в определенном «виртуальном» пространстве, наличие специфических цифровых следов, которые, в большей степени, не свойственны как для основного состава мошенничества, так и его разновидностей. Теперь представим, что при расследовании исследуемого нами вида мошенничества и сопутствующих ему преступлений правоприменителям следовало бы руководствоваться рекомендациями, данными только в общей методике расследования мошенничества. В данном случае, отсутствие частной методики расследования данного вида преступления проявилось бы наличием соответствующих познавательных пробелов в сознаниях правоприменителей (особенно при отсутствии у них соответствующей специальной подготовки) и вызвало бы немало трудностей при распознавании и расследовании таких преступлений. Надо отметить, что свидетелем такой сложившейся ситуации мы с вами и явились. Отрицание целесообразности создания частных криминалистических методик образно представляется отрицанием необходимости существования врачей узких специализаций наряду с наличием врача терапевта. При этом еще раз отмечаем важность и значимость общих криминалистических методик расследования, как содержащих основополагающие знания об определенной группе преступлений и мерах уголовно-правового реагирования на них.

Учитывая специфику подготовки, совершения и расследования исследуемых преступлений, характеризующуюся объемностью и многоаспектностью мошенничества в сфере компьютерной информации, в процессе формирования методики мы избрали включение в ее структуру наиболее актуальных аспектов в виде особенностей методики, освещение которых будет способствовать эффективному процессу расследования. Итак, в качестве таких элементов мы избрали следующие:

– понятие и признаки мошенничества в сфере компьютерной информации;

– данные о типичных способах, обстановке, личности типичного преступника и потерпевшего, типичных следах;

– особенности доследственной проверки и возбуждения уголовного дела;

– типичные следственные ситуации, алгоритм их разрешения, а также выдвигаемые версии расследования;

– тактику производства отдельных следственных действий;

– особенности использования специальных знаний.

Итак, проведенное исследование позволило сформулировать понятия методики расследования мошенничества в сфере компьютерной информации, в общем и более конкретном виде.

Методика расследования мошенничества в сфере компьютерной информации представляет собой систему знаний о противоправном воздействии на соответствующую охраняемую группу общественных отношений и мерах уголовно-правового реагирования на такое воздействие.

При формировании более предметного понятия формируемой методики за основу были взяты соответствующие понятия, выработанные в своих диссертационных исследованиях А. В. Чумаковым[65] и Н. В. Поляковым[66].

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

[65] Чумаков А. В. Указ соч. С. 38.
[66] Поляков Н. В. Указ. соч. С. 51.

Глава 2. ОСОБЕННОСТИ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1. Типичные способы мошенничества в сфере компьютерной информации

Ценность и практическая значимость любой криминалистической характеристики взаимообусловлена полнотой и степенью систематизации информации, содержащейся в ее структурных элементах. Поэтому предельно важно уделить пристальное внимание каждому из ее элементов.

Как известно, способ преступления является системообразующим элементом криминалистической характеристики преступления, поэтому знания о нем являются основой разработки любой криминалистической методики расследования преступления.

В научном сообществе существуют различные подходы к определению понятия способа преступления. Одним из наиболее полных считаем определение, данное Г. Г. Зуйковым, который под способом преступления понимает «систему действий по подготовке, совершению и сокрытию преступлений, детерминированных условиями внешней среды и психофизиологическими свойствами личности, могущих быть связанными с избирательным использованием соответствующих орудий или средств и условий места и времени»[67].

Представляется, что как-либо определить многообразие способов преступлений, как явления в целом, вообще не представляется возможным. Так же как в мире нет двух одинаковых людей, нет и двух зеркально одинаковых способов преступления. Перефразируя всем известную фразу «сколько людей - столько и мнений», можно предположить, что «сколько преступлений - столько и способов».

---

[67] Зуйков Г. Г. Криминалистическое учение о способе совершения преступления : автореф. дис. ... д-ра юрид. наук. М., 1970. С. 10.

Видится, что в данном случае возможно вести речь только об определенной типичности способов преступлений, которые в свою очередь, даже находясь внутри одной группы, будут отличаться исходя из особенностей личности преступника, обстановки, обстоятельств совершения преступления и т. д. Выбор того или иного способа зависит от степени развитости сознания человека, способа его мышления. Как известно, способ мышления человека заложен на генном аппарате, для его развития человек сам, посредством познания, серьезной внутренней работы, должен стремиться к расширению и совершенствованию сознания. Недоразвитость же сознания в той или иной степени проецируется вовне, и, в зависимости от устремленности человека, проявляется в различных жизненных аспектах, в т. ч. и в склонности к антиобщественному, противоправному образу жизни.

Анализируя предрасположенность к противоправному поведению и выбору способов совершения преступлений, видится, что с учетом уровня индивидуальной степени осознанности, устремленности, имеющихся познаний, разные люди по-разному отнесутся к выбору вида, способа проявления противоправной деятельности, а также степени участия в ней. Таким образом, знания о способе совершения преступления, могут содержать сведения о различных психофизиологических особенностях личности преступника.

Очевидно, что существенную роль на выбор и характер способа совершения преступления оказывает обстановка его совершения, а также имеющийся уровень развития научно-технического прогресса. Так, тотальная цифровизация всех сфер жизни общества неминуемо отразилась на состоянии преступности, в частности повлекла возникновение и последующую криминализацию новых составов преступлений, в том числе и в сфере компьютерной информации.

Как мы видим, знания о способе преступления имеют очень важное криминалистическое значение, поскольку проявляют всю совокупность информации о средствах, методах, приемах, орудиях, используемых для подготовки, совершения и сокрытия преступления, информацию о лицах, его подготавливающих и совершающих, их физиологических, психических и

нравственных особенностях, обстановке совершения преступления, а также весь спектр информации о механизме следообразования. Поэтому, обладание такой информацией способствует построению наиболее эффективного процесса раскрытия и расследования преступления. Как справедливо заметил Р. С. Белкин, способ имеет решающее значение для частной криминалистической методики, поскольку является базой для выдвижения как общих, так и частных версий, в этом качестве влияет на определение направлений расследования[68].

Резюмируя вышесказанное, представляется, что способ преступления - это совокупность внешних проявлений внутреннего состояния и устремленности человека, направленных на создание необходимых условий по подготовке, совершению преступления и сокрытию следов преступной деятельности[69].

Еще одной важной особенностью уяснения способа совершения преступления является его способность влиять на оценку квалификации содеянного, а также отграничивать преступные действия от смежных составов. Как уже отмечалось, проведенный анализ практики применения введенного в действие в 2012 г. анализируемого состава преступления, выявил наличие существенных трудностей в квалификации преступных деяний, устраненных только после принятия соответствующего постановления Пленума Верховного Суда РФ № 48 [70] . Данное обстоятельство способствовало правильной распознаваемости преступных действий, результатом чего стало сокращение числа зарегистрированных преступлений по данной статье более чем в десять раз.

Известно, что одним из структурных элементов способа преступления являются действия, направленные на подготовку его совершения. В ходе проведения исследования установлено, что, как правило, совершению мошенничества в сфере компьютерной информации предшествуют различные действия, которые в зависимости от способа преступления, имеют место на

---

[68] Белкин Р. С. Курс криминалистики. В 3 т. Т. 3. Криминалистические средства, приемы и рекомендации. М., 1997. С. 314.

[69] Харина Е. А. К вопросу о криминалистической характеристике мошенничества в сфере компьютерной информации // Российский следователь. 2023. № 11. С. 12.

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

стадии его подготовки в единичном или полном своем проявлении. Так, наиболее характерными из них являются следующие действия:

– разработка плана и механизма преступной деятельности, предусматривающих проработку всех ее этапов. Так, в ОПС Lurk, план включал в себя: четкое и детальное распределение функций и обязанностей между участниками; беспрекословное их соблюдение; тщательную подготовку к совершению каждого преступления и соблюдение мер конспирации; поддержание постоянного непосредственного контакта с участниками[71];

– получение специальных познаний, навыков и умений в сфере компьютерной информации, либо приискание лиц, обладающих такими специальными познаниями. На распространенность данных действий указало 62,4 % респондентов (Приложение 1). На данном этапе возможно изучение и анализ специальной литературы, прохождение обучения как на легальных специализированных курсах с последующей адаптацией полученных знаний в криминальном аспекте, так и прохождение специализированного обучения на каком-либо из веб-сайтов теневого Интернета.

Исходя из способа преступления, специфика требующихся знаний для реализации преступных намерений может быть различной. Так, организаторы преступного формирования Lurk, намереваясь совершать хищения денежных средств посредством несанкционированного доступа в компьютерные сети хозяйствующих субъектов РФ и использования прав администратора, главного бухгалтера либо иных привилегированных пользователей, изучили принцип и особенности работы программного обеспечения «1С Бухгалтерия», системы «Банк-Клиент» и программного комплекса «Автоматизированное рабочее место клиента Банка России» (далее АРМ КБР). Кроме того, на одном из изъятых флеш-накопителей обнаружен файл «хайтек.doc», содержащий руководство и способы обналичивания денежных средств «в зоне RU» на 22 листах. Согласно данной инструкции, обналичивание подразделяется на «классическое», «продвинутое» и «хайтек», указана структура банков, как производить обналичивание, работать с

[71]Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

«дропами». При осмотре проекта Exploits системы Trac, установлены ссылки на обучающие статьи, в т. ч.: «Варианты обхода ASLR», «Использование процессора при палеве», «Чистка палева», «Тест планы» и т. д.[72]

При этом имеющиеся или полученные знания включают в себя не только знания о способах преступления, но и четкое представление о применении необходимых мер конспирации и способов сокрытия следов преступной деятельности, а также противодействия расследованию;

– создание преступной группы, преступного формирования, путем вовлечения новых участников, как из числа уже знакомых, так и незнакомых лиц. На характерность данного действия указало 24,8 % респондентов (Приложение 1). Так, по делу Lurk большинство членов были вовлечены в ОПС путем подачи соответствующих объявлений или отклика на такие объявления на различных ресурсах (портал E1, HeadHunter.ru и др.). После проведенного собеседования предлагалось выполнить тестовое задание, при успешном выполнении которого участник принимался в преступную группу[73]. На данном этапе возможно приискание соучастников, трудоустроенных в кредитных и иных организациях, сотрудники которых могут оказать помощь в осуществлении преступного умысла;

– приобретение в собственность и/или аренда жилых, нежилых помещений. Так, по делу Lurk, организатор преступного сообщества в преступных целях использовал принадлежащую ему на праве собственности квартиру, которую оборудовал необходимой компьютерной техникой. Кроме того, подразделениями «обнальщиков» в качестве офисов использовались четыре помещения в Екатеринбурге и одно в Москве[74];

– регистрация юридических лиц для перевода на их счета похищенных денежных средств с целью последующего обналичивания. Так, по делу Lurk одна из свидетельниц открыла на свое имя пять юридических лиц, за каждое из которых получила по 2000 руб. На счет одного из них – ООО «Промторг» была

[72] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...
[73] Там же.
[74] Там же.

перечислена часть похищенных денежных средств ООО «Стройинвест». Помимо вновь открываемых юридических лиц, в реализации преступных намерений могут использоваться ранее открытые, но фактически не действующие юридические лица. Так, один из свидетелей по тому же делу на сайте «Авито» нашел соответствующее объявление и за вознаграждение в 60 000 руб. передал учредительные документы, сведения по расчетным счетам зарегистрированных на его имя юридических лиц: ООО «Сентябрь», ООО «Протон», ООО «Регионснаб»[75];

– приискание и получение в пользование банковских и иных платежных карт, расчетных счетов в банках, оформленных на подставных лиц (так ответило 64,8 % респондентов) (Приложение 1). Как правило, банковские карты и расчетные счета приобретаются за вознаграждение и используются для обналичивания переведенных на них похищенных денежных средств. Способы приискания данных банковских продуктов могут быть различными: посредством размещения соответствующих объявлений на социальных сайтах, веб-сайтах теневого Интернета и т. д. При этом одни владельцы потенциально догадываются об использовании их банковских карт и расчетных счетов для совершения преступных действий, от других владельцев скрывается истинный мотив приобретения, в качестве обоснования могут высказываться версии о необходимости перечисления денежных средств (заработной платы) лицам, не имеющим гражданства РФ и т. д.

Так, по делу Lurk в конце 2015 – начале 2016 г. за вознаграждение были оформлены около 700 банковских карт на физических лиц, а также SIM-карты, к которым можно привязать мобильный банк. По одному из эпизодов преступной деятельности похищенные у Сибирского филиала Банка «Таатта» АО в сумме 99 705 000 руб. были перечислены на 1 261 банковский счет[76];

– приобретение соответствующих компьютерных и (или) технических средств, использование которых необходимо для исполнения преступного умысла

[75] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1...
[76] Там же.

(так ответило 55,5 % респондентов) (Приложение 1). Так, в ОПС Lurk закупкой соответствующего оборудования и специальных средств занимался гр. П.[77]. При этом обслуживание дорогостоящей сетевой инфраструктуры обходилось в десятки тысяч долларов ежемесячно[78];

– приискание, создание ВПО, предоставляющего возможность несанкционированного доступа к компьютерным устройствам и заведомо предназначенного для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации в целях совершения хищений (так ответило 45,6 % респондентов) (Приложение 1). Таким ВПО являются программы, основным назначением которых, в том числе, является проведение оценки безопасности информационных систем и сетей посредством моделирования различных компьютерных атак, позволяющие получать информацию о состоянии банковских счетов клиентов банка, получать возможность управления денежными средствами, находящимися на данных счетах, получать контроль за работой компьютерных устройств юридических лиц, с целью совершения хищений, получать информацию о состоянии кассет банкомата (наличии и количестве купюр) и управлять его работой, путем отправки команд на выдачу денежных купюр в любом доступном объеме и т. д.[79];

– получение конфиденциальной информации, необходимой для совершения хищений, может осуществляться на специализированных Интернет-форумах, например: darkmoney.cc, wasm.ru, darknet.la, anticarder.cc, carding.ug, carderland.com и др., а также в социальных сетях и программах обмена мгновенными сообщениями, например Telegram-каналах: @putkardera, @cc_word и др. Крупнейшим ресурсом для криминального приобретения объектов, изъятых из гражданского оборота, включая рассматриваемую информацию, являлась международная торговая площадка Hydra, включавшая в себя биржу криптовалют, защищаемый мессенджер, сотни виртуальных «магазинов»,

[77] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1...

[78] Стоянов Р. Охота на Lurk. URL: https://securelist.ru/the-hunt-for-lurk/29220 (дата обращения: 20.12.2022).

[79] Приговор Якутского городского суда Республики Саха (Якутия) от 26 августа 2019 г. № 1-681/2019. URL: https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения: 08.08.2022).

представляющих возможность анонимного приобретения запрещенных объектов, а также средств совершения преступлений[80]. На смену закрытой в 2022 г. указанной площадки пришли, в т. ч. Kraken, Solaris.

В течение 2021 г. по сравнению с 2020 г. количество продаваемых текстовых данных банковских карт (номер, дата истечения, имя владельца, адрес, CVV) увеличилось на 36 % с 28 млн до 38 млн[81].

Кроме того, к получению информации ограниченного распространения может относиться получение сведений о соответствующих логинах и паролях (на что указали 46,6 % опрошенных) (Приложение 1), к примеру, сотрудников кредитной организации (которые могут быть коллегами по работе), необходимые для осуществления входа в информационную банковскую систему;

– поиск и аренда управляющих серверов (как правило, расположенных на территории других государств), предназначенных для размещения программных средств, предоставляющих возможность дистанционного управления ВПО. На типичность данного действия указали 39,4 % респондентов (Приложение 1);

– создание сайтов, имитирующих официальные сайты (так ответили 49,5% опрошенных) (Приложение 1), к примеру, сайт известного платежного сервиса или ДБО. Так, братья П., «заражали компьютеры пользователей вирусом Trojan.Win32.VKhost, который, при переходе к официальному интернет-банкингу одного из крупнейших российских банков, перенаправлял клиента на фишинговую страницу»[82];

– приобретение мобильных телефонов (как правило, под каждый эпизод совершения преступления), а также приискание SIM-карт, оформленных на посторонних лиц (так ответили 59,4 % опрошенных) (Приложение 1). Нередко преступниками используются абонентские номера принадлежащие операторам связи других государств. Как правило, данные средства связи используются только для осуществления преступной деятельности. Так, список контактов

---

[80] Гаспарян Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : дис. .. канд. юрид. наук. М., 2020. С. 47–48.

[81] Экскалация киберугрозы: Group-IB проанализировала ключевые тренды развития киберпреступности. URL: https://www.group-ib.ru/media-center/press-releases/gib-2021-2022-report (дата обращения: 11.12.2022).

[82] Хакеры-близнецы Попелыши сели в тюрьму со второго раза. URL: https://news.rambler.ru/crime/40132145-hakery-bliznetsy-popelyshi-seli-v-tyurmu-so-vtorogo-raza (дата обращения: 28.12.2022).

проходящего по делу Lurk телефона марки Nokia состоял из двух номеров: под именем «я» и «ты». На другом телефоне контакты именовались как «ты», «ты1», «ты2», «ты3»[83].

В этой связи совершенно обоснованна позиция О. А. Науменко, указывающей в качестве одного из направлений реализации криминалистического прогноза верификацию виртуальных номеров телефона или исключение технической возможности подмены телефонных номеров, упрощенный порядок приостановки их обслуживания[84];

– использование в противоправных целях компьютерных сетей, таких как Yggdrasill, cjDNS, Briar, SignalOffline, FireChat, позволяющих организовать доступ к информации, распространение которой в России запрещено. А также, использование компьютерных сетей на основе анонимных защищенных подключений, таких как TOR (от англ. The Onion Router – луковичная маршрутизация), где размещается абсолютное большинство виртуальных торговых площадок по нелегальной продаже запрещенных к свободному обороту объектов[85];

– регистрация электронной почты, установка мессенджеров (WhatsApp, Viber, Telegram, Skype, Jabber, Wechat и т. д.), затрудняющих идентификацию пользователей и обеспечивающих наиболее конспиративное общение между участниками преступного формирования (так ответило 48,1 % респондентов) (Приложение 1). Так, в ОПС Lurk общение между участниками осуществлялось через программу обмена мгновенными сообщениями Jabber. Любое общение вне внутренних ресурсов запрещалось[86];

– регистрация электронных кошельков, к примеру, ЮMoney.Яндекс.Деньги, Webmoney, Qiwi, Bitcoin-кошелька и т. д., как правило, используемых для

[83] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

[84] Науменко О. А. О криминалистическом прогнозировании мошенничеств в сети Интернет // Вестник Краснодарского университета МВД России. 2021. № 4 (54). С. 74.

[85] Гаврилин Ю. В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практ. пособие. М., 2021. С. 45–46.

[86] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

перечисления на них похищенных денежных средств. Так, в ОПС Lurk заработная плата участникам выплачивалась чеками Paymer платежной системы Webmoney[87];

– использование различных программ, направленных на сокрытие следов преступной деятельности, к примеру, программ - «ремейлеров», обеспечивающих переадресацию отправлений электронной почты и подмену информации об электронном адресе отправителя электронным адресом «ремейлера» или иным подменным адресом; а также «анонимайзеров», обеспечивающих подмену используемого абонентом сети Интернет уникального IP-адреса. Особой разновидностью «анонимайзеров» являются VPN-сервисы, обеспечивающие шифрование передаваемых данных и создание защищенного информационного канала с сервером, расположенным, как правило, за рубежом, осуществляющим переадресацию сообщений. VPN-сервисы нередко используются совместно с прокси-серверами – физическими устройствами или специальными программами, обеспечивающими роль посредника между подключаемым к сети Интернет устройством и самой сетью. Учитывая, что к одному прокси-серверу могут подключаться сотни различных устройств, все они для внешних пользователей будут иметь общий IP-адрес – адрес прокси-сервера[88];

Так, в преступном сообществе Lurk была создана частная виртуальная сеть сложной конфигурации, и другие подсети. Доступ во внутреннюю сеть осуществлялся только с использованием анонимной сети TOR или нескольких последовательных соединений через прокси-серверы. Администратор группы проводил мониторинг сетевых ресурсов на предмет выявления подозрительных процессов, свидетельствующих о стороннем вмешательстве[89] .

Также, в зависимости от способа преступления, подготовительные действия могут включать в себя и другие элементы. Так, к примеру, при совершении преступления в отношении юридического лица, могут производиться действия, направленные на изучение организации его работы.

---

[87] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...
[88] Гаврилин Ю. В. Указ. соч. С. 46–48.
[89] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

Кроме того, могут использоваться и другие меры противодействия обнаружения преступной деятельности. Так, известные братья П., имели в квартире электромагнитную пушку, способную размагничивать жесткие диски[90].

В настоящее время, исходя из анализа следственно-судебной практики, мнения Е. А. Русскевича[91], с учетом рекомендаций, данных постановлением Пленума Верховного Суда РФ № 48[92], можно выделить следующие наиболее распространенные способы мошенничества в сфере компьютерной информации.

1. Посредством осуществления неправомерного доступа к информационной инфраструктуре кредитной организации. На данный способ из числа наиболее распространенных указали 46,7 % респондентов (Приложение 1). Преступление, в том числе, может быть совершено работником кредитной организации, который посредством нарушения правил эксплуатации средств хранения компьютерной информации изменяет информацию о состоянии лицевого счета. Так, сотрудники одного из банков переводили на подконтрольные им счета денежные средства клиентов банка[93].

2. Посредством воздействия ВПО на компьютерные устройства клиентов кредитных организаций. О распространенности данного способа указали 66,9 % респондентов (Приложение 1). В данном случае речь идет о хищении денежных средств через систему «Мобильный банк», а также посредством неправомерного доступа к личным кабинетам клиентов банков в сети Интернет. Большая часть хищений осуществляется посредством незаконного воздействия, через заражение соответствующим ВПО, как правило, на мобильные компьютерные устройства, работающие на платформе Android. Специфика работы таких программ заключается в самостоятельном, помимо воли владельца счета, и тайном обращении с запросами о состоянии баланса счета, о переводах денежных средств, получении и отсылке полученных кодов. На само же мобильное

[90] Братья по кибероружию. URL: https://blog.group-ib.ru/brothers (дата обращения: 29.12.2022).

[91] Русскевич Е. А. Мошенничество в сфере компьютерной информации : вопросы квалификации [видеозапись круглого стола Павел Яни, Е. А. Русскевич] // YouTube. 15.02.2021. URL: https://youtu.be/knpXHRh2xQc (дата обращения: 15.08.2022).

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

[93] Уголовное дело № 1-675/2019 // Архив Советского районного суда г. Красноярска.

устройство владельца счета никаких оповестительных сигналов в виде уведомлений или SMS-сообщений не поступает.

Так, Отчет ФинЦЕРТ показывает, «что вектор внимания злоумышленников смещается с атак на непосредственную инфраструктуру кредитно-финансовых организаций на исследование клиент-серверных приложений с целью кражи данных клиентов или получения возможности хищения денежных средств со счетов клиентов»[94].

Согласно Обзору отчетности Банка России об инцидентах информационной безопасности, при переводе денежных средств Банка России за 3 квартал 2022 г. по сравнению с аналогичным периодом прошлого года, объем операций без согласия клиентов кредитных организаций, осуществленных по каналам ДБО физических лиц увеличился с 52 081 до 79 174 случаев на сумму с 1 687 955,5 до 2 722 794,85 тыс. руб. соответственно; для юридических лиц с 411 до 1 037 случаев на сумму с 154 964,76 до 268 303,72 тыс. руб. соответственно[95].

Согласно приговору суда, граждане Х., К. и Ш. использовали приобретенное ВПО для заражения вирусами мобильных устройств, тем самым обеспечивали доступ к ним на правах администратора с правом доступа к расчетным счетам. После чего удаленно отправляли сгенерированные команды посредством SMS-сообщений на перевод денежных средств на подконтрольные им банковские счета. В результате действия вредоносных программ SMS-уведомления о происходящих операциях потерпевшим не приходили, при этом многие из них узнавали о произведенных у них хищениях спустя продолжительное время: после обращений к ним следователей; во время разбирательств о недостаче денежных средств при попытке оплатить кредиты и ипотеку, снять наличные денежные средства в банкоматах. Действия Х., К., Ш. квалифицировались по ч. 2 ст. 159.6 УК РФ[96].

---

[94] Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России. URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения: 11.12.2022).

[95] Обзор отчетности Банка России об инцидентах информационной безопасности при переводе денежных средств. URL: http://www.cbr.ru/analytics/ib/review_3q_2022 (дата обращения: 11.12.2022).

[96] Приговор Центрального районного суда г. Тюмени от 3 сентября 2018 г. № 1-18/2018 1-528/2017. URL: https://sudact.ru/regular/doc/ruiCsHOBEBUQ (дата обращения: 15.07.2022).

3. *Посредством установления контроля за работой компьютерных устройств юридических лиц через предустановленное ВПО.* На распространенность данного способа указали 28,4 % респондентов (Приложение 1). Преступления могут совершаться посредством вмешательства в работу ДБО юридических лиц, а также посредством вмешательства в работу самих кредитных организаций.

Как правило, традиционной технологией осуществления несанкционированного доступа к информационной инфраструктуре юридических лиц, кредитных организаций, а также их клиентов является проникновение на их компьютерные устройства ВПО посредством открытия «фишинговых» писем от различных организаций и органов государственной власти. Впоследствии происходит мониторинг компьютерной сети организации, распространение по другим интересующим преступников компьютерам. Установленное ВПО позволяет производить оценку финансовой активности организации, состояния информационной защиты, определить и создать технические возможности совершения хищения денежных средств.

Спецификой совершения преступлений данным способом является плохая распознаваемость компьютерными средствами вредоносных компьютерных программ, которые в случае возникновения угрозы обнаружения имеют способность к самоуничтожению. Как правило, подобные преступления хорошо спланированы и совершаются организованными преступными формированиями, нередко имеющими международный характер.

В данном контексте нельзя не привести пример создания ОПС, деятельность которого распространялась на города Санкт-Петербург, Новосибирск, Уфу, Алтайский край. Численность преступного формирования насчитывала 29 человек, в материалах уголовного дела фигурировало более шестидесяти эпизодов мошенничества, общий ущерб от преступной деятельности составил более 17 млн руб. Суть мошеннической схемы заключалась в фиктивных возвратах оформленных железнодорожных и авиабилетов, в т. ч. S7 и РЖД. Основателями ОПС являлись находившиеся в федеральном розыске за совершение мошенничеств гр. М. и гр. С. (он же являлся ее лидером), которые

познакомились на одном из интернет-форумов преступной направленности. Еще одним из фигурантов, занимавшем одну из руководящих ролей в ОПС являлся гр. К., разработавший специальную вредоносную программу, с помощью которой взламывались базы данных партнеров указанных компаний – ООО «С7 билет» и «Универсальная финансовая система». На электронные адреса корпоративных клиентов компаний, преимущественно туроператоров, рассылались «зараженные» письма, при открытии которых фигуранты получали доступ к идентификационным данным кассиров, от имени которых оформлялись билеты и производилась оплата. Билеты оформлялись на паспортные данные специально подобранных подставных лиц – «дропов», которые впоследствии и обращались за возвратом билетов (в общем более 5 тыс. билетов) и получением наличных денежных средств. Действия фигурантов квалифицированы по ч. 1 ст. 210, ч. 2 ст. 210, ч. 4 ст. 159.6 УК РФ. Кроме того, необходимо отметить, что 10 октября 2018 г. возле подъезда своего дома была застрелена старший следователь по особо важным делам Евгения Шишкина, которая занималась расследованием данного дела. Заказчиком убийства следствие считает организатора ОПС гр. С. Исполнители убийства в настоящее время осуждены, гр. С. пока свою вину отрицает[97].

4. Посредством неправомерного внесения изменений в платежные поручения юридических лиц. Данный способ был указан в числе наиболее распространенных 29,3 % респондентов (Приложение 1). Так, при помощи предустановленного ВПО происходит внесение изменений в реквизиты платежных поручений, направляемых в банк от имени главного бухгалтера, руководителя организации и других уполномоченных лиц. В результате совершения вмешательства в функционирование сервиса ДБО клиентов перечисление денежных средств происходит на подконтрольные преступникам счета.

В настоящее время совершение преступлений данным способом встречается все реже в силу усовершенствования бухгалтерского программного обеспечения,

[97] Суд дал хакерам от 10 до 13 лет по делу о взломе билетных баз РДЖ и S7. URL: https://www.rbc.ru/society/25/12/2019/5e00c7bf9a794770d60099a0 (дата обращения: 04.08.2022).

а именно в изменении способа экспорта-импорта подготовленных платежных поручений[98].

Совершением хищений подобным образом занималось ОПС Lurk. Так, разработанное ВПО размещалось на компьютерах локальной сети различных организаций, после установления компьютеров определенных пользователей (бухгалтеров, операторов АРМ КБР), получали к ним доступ, изучали принцип работы. Затем, в определенное время незаконно формировались и направлялись электронные файлы с реестром платежей, в результате чего похищенные таким образом денежные средства переводились на подконтрольные преступникам счета юридических и физических лиц. Таким образом, преступниками было похищено более 1,25 млрд руб. Действия преступников квалифицированы по ч. 4 ст. 159.6 УК РФ, ч. 1 ст. 210 УК РФ, ч. 3 ст. 272 УК РФ, ч. 2 ст. 273 УК РФ, позже апелляционным определением обвинения по ч. 3 ст. 272, ч. 2 ст. 273 УК РФ были сняты за истечением срока давности уголовного преследования. Участкам ОПС назначены наказания от 5 лет 2 месяцев до 13 лет 4 месяцев лишения свободы[99].

5. Посредством осуществления несанкционированного управления работой банкомата. Данный способ отнесен к числу наиболее распространенных 15,3 % респондентов (Приложение 1). Хищение денежных средств осуществляется путем получения контроля за компьютерной системой, управляющей работой банкомата посредством внедрения соответствующего ВПО. Способы внедрения таких компьютерных программ могут быть различными: путем механического повреждения защитного корпуса банкомата или путем осуществления доступа к информационной инфраструктуре самой кредитной организации.

Так, гр. Ш. приискал в сети Интернет соответствующее ВПО, предназначенное для получения неправомерного доступа к устройствам самообслуживания банков. В ходе подготовительных действий к совершению преступлений, посредством работы вредоносной программы в различных регионах РФ обнаруживались устройства самообслуживания, оборудованные

[98] Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России …

[99] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

уязвимой операционной системой, принадлежащие ПАО АКБ «Связь-Банк», ООО Банк «Аверс», ООО «Хакасский муниципальный банк». В память данных устройств копировались вредоносные компьютерные программы, обеспечивающие удаленный доступ к управлению функциями купюроприемника и предоставляющие технические каналы безналичного перевода денежных средств. В результате на подконтрольные преступникам счета банковских карт были перечислены денежные средства в размере более 2,5 млн руб. Приговором суда гр. Ш. был признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274, ч. 2 ст. 159.6 УК РФ и осужден к наказанию в виде 2 лет 6 месяцев лишения свободы[100].

Существующая судебно-следственная практика указывает на наличие способов совершения мошенничества в сфере компьютерной информации с неоднозначной оценкой.

Так, в судебно-следственной практике имеются варианты неоднозначной правовой оценки хищений, совершенных *посредством задержки шторки купюроприемника банкомата, либо с использованием приспособлений, позволяющих вернуть вложенные купюры.* На практике такие деяния квалифицировались и по п. г ч. 3 ст. 158 УК РФ и по ст. 159.6 УК РФ, имели место случаи переквалификации деяний на ст. 159.6 УК РФ мотивируя совершением вмешательства в нормальное функционирование штатного оборудования и программного комплекса.

Согласно приговору суда, гр. Г. и гр. А., действуя группой лиц по предварительному сговору, совершали хищения денежных средств посредством манипуляций с платежными терминалами. Так, в купюроприемники платежных терминалов запускали подготовленные купюры, преимущественно достоинством 1000 руб., с приспособлением, позволяющим вытащить их обратно. Данные манипуляции производили многократно, что позволяло зачислять на подконтрольные им абонентские номера и банковские карты денежные суммы от

[100] Приговор Кировградского городского суда Свердловской области от 05 августа 2016 г. № 1-105/2016 ...

6 000 до 29 000 руб., которые в последствии обналичивали. Действия гр. Г. и гр. А. квалифицированы по ч. 2 ст. 159.6 УК РФ[101].

6. Посредством создания и использования «фишинговых» сайтов. 47,8 % опрошенных сотрудников правоохранительных органов отнесли данный способ к числу наиболее распространенных (Приложение 1). Важно отметить, что, несмотря на разъяснения, данные законодателем в п. 21 постановления Пленума Верховного Суда РФ № 48 [102], о необходимости квалификации хищений, совершенных посредством создания поддельных сайтов по ст. 159 УК РФ, многие правоприменители, позиции которых мы также придерживаемся, совершение преступления подобным способом считают целесообразным квалифицировать по ст. 159.6 УК РФ. Следствием неоднозначной оценки подобных деяний явилась не единообразная правоприменительная практика.

Согласно приговору суда, гр. Р., используя разработанное ВПО, создал сайт, имитирующий сайт известного платежного сервиса, который разместил на сервере организации, занимающейся оказанием «хостинг» услуг. При обращении к платежному ресурсу потерпевшие осуществляли ввод пароля и логина своих интернет-кошельков, которые несанкционированно копировались и использовались гр. Р. для доступа к денежным средствам, которые перечислял на ранее приобретенную банковскую карту. Согласно своей роли в преступной группе, обналичиванием денежных средств через терминалы банкоматов за долю в 30 % занимался гр. А. Для сокрытия своей личности гр. А. использовал подложное водительское удостоверение РФ с вклеенной своей фотографией, которое предъявлял при проверке документов. В результате гр. Р. был осужден по ч. 2 ст. 159.6, ч. 2 ст. 273 УК РФ, гр. А. – по ч. 2 ст. 159.6 УК РФ, ч. 3 ст. 327 УК РФ[103].

По сути, совершение указанных хищений осуществляется посредством работы ВПО и заключается в неправомерном перечислении денежных средств со

---

[101] Приговор Кизилюртовского городского суда Республики Дагестан от 11 июня 2014 г. № 1-49/2014. URL: https://sudact.ru/regular/doc/7Mcxk2HXGclB/ (дата обращения: 07.08.2022).

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

[103] Приговор Приволжского районного суда г. Казани Республики Татарстан от 09 ноября 2018 г. № 1-588/18. URL: https://sudact.ru/regular/doc/o3PSlcynw8Lv (дата обращения: 02.08.2022).

счета клиента на подконтрольные преступникам счета. Так, имеются случаи, когда проникновение ВПО произошло в результате посещения якобы легального сайта, содержащего образцы бухгалтерских документов[104].

Учитывая принципиальную схожесть данного способа совершения преступления с большинством вышеуказанных типичных способов, предполагаем целесообразным квалифицировать указанные деяния по ст. 159.6 УК РФ.

Кроме того, наряду с указанием наиболее распространенных способов рассматриваемых преступлений, в рамках настоящего диссертационного исследования, проведена типологизация рассматриваемой преступной деятельности по двум основаниям.

I. В зависимости от степени организованности мошенничества в сфере компьютерной информации: «организованное» и «несложное».

Вначале необходимо отметить определенные нами критерии относимости конкретного деяния к тому или иному типу мошенничества. Так, основным критерием разграничения «организованного» мошенничества от «несложного» является уровень сложности и незаурядности способа его подготовки, совершения и сокрытия следов преступной деятельности. Так, характер проявления соответствующих действий на различных стадиях реализации преступного умысла при «организованном» мошенничестве свидетельствует о высокой организации процесса. Такими действиями могут быть: тщательная спланированность, приискание соответствующих компьютерных устройств, технических средств, написание или приобретение, как правило, высококачественного ВПО, незаурядность способа преступления, приискание соучастников, обеспечение конспиративности общения, тщательная подготовка и изучение объекта преступного посягательства, преимущественная нацеленность на продолжительное и систематическое осуществление преступной деятельности.

При этом совершение преступления в группе лиц не всегда будет свидетельствовать о его относимости к «организованному» типу мошенничества.

[104] Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России …

Так, преступление, хоть и совершенное в группе лиц, при этом несложным, «примитивным» способом, в данном контексте не будет обладать признаками «организанного» типа мошенничества.

1. *«Организованное» мошенничество в сфере компьютерной информации.* Как правило, характеризуется созданием устойчивых организованных преступных групп и ОПС. Во главе или среди заместителей такой структуры, преимущественно, находится лицо, обладающее глубокими специальными познаниями в сфере ИТТ, имеющее хорошие организаторские способности. Ролевые функции участников четко распределены и регламентированы; совершению преступлений предшествует, как правило, не быстрый этап подготовки, включающий в себя приискание или создание, как правило, высококачественного ВПО, приобретение соответствующих компьютерных устройств и технических средств, вовлечение и обучение новых участников, организацию системы общения, построенную на принципах конфиденциальности и т. д. Нередко деятельность таких преступных формирований имеет межрегиональный или международный характер, а доход от преступной деятельности исчисляется миллионами долларов США.

Как уже отмечалось, ярким примером деятельности таких преступных формирований явилось ОПС Lurk.

2. «Несложное» мошенничество в сфере компьютерной информации. Как правило, характеризуются несложными способами совершения преступления, может совершаться одним или несколькими лицами, не обязательно обладающими специальными познаниями в сфере ИТТ.

Так, согласно приговору суда, реализуя умысел на совершение хищений денежных средств, гр. З. на одном из сайтов преступной направленности приобрел доступ к административной панели, позволяющей в течение двух месяцев обнаруживать мобильные устройства, в операционной системе которых уже имеются вредоносные файлы, и путем удаленного доступа управлять

функциями данных устройств, в т. ч. осуществлять переводы денежных средств без ведома владельца. Посредством размещения соответствующего объявления на странице своей супруги одного из социальных сайтов сроком на двое суток за денежное вознаграждение получил в пользование банковские карты ПАО «Сбербанк России». Таким образом, используя приисканное программное обеспечение путем получения информационного доступа к мобильным устройствам и возможности управлять лицевыми счетами банковских карт путем использования автоматизированного SMS-сервиса «Мобильный банк», гр. З. совершил переводы денежных средств на находящиеся в его распоряжении банковские карты. В результате чего был осужден по ч. 2 ст. 159.6 УК РФ[105].

II. В зависимости от уголовно-правовой квалификации совершенного преступления.

1. Посредством совершения основного преступления (предусмотренного ст. 159.6 УК РФ). Характеризуется совершением деяния, признаки которого полностью охватываются объективной стороной мошенничества в сфере компьютерной информации и не требуют дополнительной квалификации по другим нормам уголовно-правового закона.

2. Посредством совершения основного и сопутствующих преступлений. Как уже было указано, такими преступлениями, преимущественно, являются деяния, предусмотренные гл. 28 УК РФ «Преступления в сфере компьютерной информации».

Как мы видим, анализ способов совершения мошенничества в сфере компьютерной информации указывает на наличие уязвимостей средств программно-технической защиты компьютерных средств и обоснованно указывает на необходимость их усовершенствования с целью усиления противодействия возможным противоправным посягательствам.

[105]Приговор Уссурийского районного суда Приморского края от 06 июня 2017 г. № 1-513/2017. URL: https://sudact.ru/regular/doc/P8NIXBB0caLC/ (дата обращения: 13.08.2022).

2.2. Обстановка совершения мошенничества в сфере компьютерной информации

Наряду с другими элементами криминалистической характеристики преступления состояние обстановки является неотъемлемой его частью, проецирующейся на характере подготовки, совершении преступления, сокрытии его следов, а также на поведении лиц, вовлеченных в противоправное деяние.

В целом, в социуме под обстановкой в широком смысле слова принято понимать какую-либо совокупность социальных, политических, эпидемиологических, экологических, экономических, военных и других факторов, имеющегося уровня развития науки и техники, духовного развития и нравственного воспитания, являющуюся определенным макромиром и создающую определенную среду для возможности возникновения предпосылок, импульса и потенции появления и развития определенного направления деятельности.

Как известно, согласно третьему закону Ньютона, «любое действие рождает противодействие». Рассматривая этот закон применительно к данной концепции, можно сформулировать следующее: развитие какой-либо сферы правоотношений порождает появление и развитие различных вариантов деструктивного проявления, выражающихся, в различных формах, в т. ч. преступной направленности. Поэтому появление преступлений, совершаемых в сфере ИТТ и прослеживающаяся тенденция их постоянного роста, были бы невозможны без сложившихся в социуме определенных условий и соответствующей обстановки.

В научном сообществе существуют различные взгляды на формирование понятия «обстановка совершения преступления».

Так, Р. Г. Камнев под обстановкой понимает «совокупность непосредственных объективных особенностей условий и взаимодействующих обстоятельств случайного, ситуативного характера, оказывающих доминирующее

воздействие на создание объективно способствующей совершению отдельного преступления ситуации»[106].

В конструкции данного определения автором указывается на случайный характер взаимодействующих обстоятельств. Однако, как известно, ничего случайного в жизни нет, а возникновение какого-либо события или явления является лишь следствием проявления на физическом плане определенной причины, развитие которой может занимать многие годы.

Н. П. Яблоков указывает, что «под обстановкой совершения преступления в криминалистическом аспекте понимается система различного рода взаимодействующих между собой до и в момент совершения преступления объектов, явлений и процессов, характеризующих место, время, вещественные, природно-климатические, производственные, бытовые и иные условия окружающей среды и другие факторы объективной реальности, определяющие возможность, условия и иные обстоятельства совершения преступления»[107].

Несмотря на данное автором, довольно развернутое, определение, оно все же не является полным, поскольку описывает проявление только внешних обстоятельств. Предложенное Н. П. Яблоковым определение сформулировано по принципу «бытие определяет сознание», но ведь и сознание также определяет бытие. Несомненно, бытие может принуждать к совершению преступлений, но существует немало примеров, когда человек, живущий в прекрасных условиях, не испытывающий никаких неудобств, все же может стать преступником.

В. Н. Кудрявцев, давая оценку данному явлению, считает, что «обстановка совершения преступления не сводится к совокупности непосредственных физических условий, в которых действовал преступник. Это понятие охватывает более широкий круг явлений и включает также общую историческую и социально-политическую обстановку, конкретные условия жизни и деятельности данного коллектива, в которых было совершено преступление»[108].

---

[106] Камнев Р. Г. Соотношение места, времени и обстановки совершения преступления // Вестник Волгоградского государственного университета. 2006. № 8. С. 133.

[107] Яблоков Н. П. Криминалистика : учебник. М., 2009. С. 36.

[108] Кудрявцев В. Н. Объективная сторона преступления : учеб. пособие. М., 1960. С. 23.

Необходимо отметить, что мы являемся сторонниками более системного подхода к освещению каждого из элементов криминалистической характеристики и обстановки совершения преступления в частности. Поэтому, в рамках данного диссертационного исследования, считаем целесообразным более пристальное внимание уделить определению факторов и совокупности различных процессов, способствующих созданию обстановки совершения преступлений в сфере компьютерной информации.

В целом, наиболее существенными факторами (в их широком понимании), влияющими на создание определенной плодородной среды, способствующей созданию благоприятной обстановки совершения преступлений в сфере компьютерной информации, а также способствующей их постоянному количественному росту, являются:

– масштабная популяризация престижности, высокооплачиваемости, востребованности занятием деятельностью в сфере ИТТ. Этот позитивный и актуальный для современного общества процесс положительным образом отразился на стремлении молодежи к получению соответствующего образования. Однако определенная часть лиц, получивших соответствующие знания, как правило, довольно молодого возраста с неокрепшей психикой и детским внутренним возрастом, стремящаяся к социальному доминированию, а в большей степени к скорейшему обогащению любыми способами, свой выбор в реализации в социуме останавливает на действии вне правового поля. Кроме того, бесконтактный способ совершения преступлений вселяет в преступников мнимую уверенность в безнаказанности содеянного.

Так, по одному из уголовных дел организатор преступной группы являлся студентом АНОО ВО «Воронежский институт высоких технологий» [109] . По другому уголовному делу были осуждены четверо студентов факультета информатики одного из вузов[110];

[109] Приговор Октябрьского районного суда г. Барнаула Алтайского края от 20 апреля 2017 г. по уголовному делу № 1-18/2017 // Архив Октябрьского районного суда г. Барнаула Алтайского края.

[110] Приговор Промышленного районного суда г. Самары от 30 августа 2016 г. по делу № 1-478/2016 // URL: https://sudact.ru.

– функционирование на просторах теневого Интернета большого количества веб-сайтов, предоставляющих множество различного рода услуг информационного, обучающего характера, предложений о продажах целых пакетов инструментов, необходимых для совершения преступлений в сфере ИТТ, так и их структурных элементов: ВПО, банковских карт, SIM-карт, необходимой спецтехники и т. д.

Предлагаемые соответствующие обучающие программы и специальные подготовительные курсы предоставляют лицам, даже не имеющим специальных познаний в сфере ИТТ реальную возможность совершения преступлений.

Так, гр. З. на сайте http://darkmoney.cc приобрел у неустановленного следствием лица сроком на два месяца доступ к административной панели Android.bot, позволяющих совершать хищения денежных средств с банковских карт, подключенных к системе «Мобильный банк»[111];

– имеющиеся уязвимости программно-технической защиты компьютерных устройств, в частности мобильных устройств, работающих на платформе Android, а также банкоматов. Доступность разработки ВПО, посредством которого осуществляются хищения с указанных мобильных устройств и преимущественное распространение их на территории РФ породило существование большого объема соответствующей правоприменительной практики. Вышеуказанный пример является иллюстрацией одного из таких случаев. К типам уязвимостей банкоматов относятся: недостатки сетевой безопасности, недостатки защиты периферийных устройств, недостатки конфигурации систем и устройств. При совершении преступлений используются различные вредоносные программы, такие как GreenDispenser, Alice, Ripper, Radpin, Ploutus и др., представленные к продаже на различных сайтах теневого Интернета[112].

---

[111] Приговор Уссурийского районного суда Приморского края от 06 июня 2017 г. № 1-513/2017…

[112] Сценарии логических атак на банкоматы, 2018. URL: https://www.ptsecurity.com/ru-ru/research/analytics/atm-vulnerabilities-2018/ (дата обращения: 08.01.2023).

Так, в результате приобретения и использования соответствующего ВПО для неправомерного доступа к устройствам самообслуживания банков преступником были похищены денежные средства в размере более 2,5 млн руб.[113];

– наличие различных мессенджеров и приложений, предоставляющих возможность конспиративного общения и затрудняющих идентификацию пользователей. Анализ следственно-судебной практики показывает, что самыми распространенными из них являются WhatsApp, Viber, Telegram. При этом на сегодняшний день самым безопасным приложением для обмена сообщениями считается Signal. Преимуществами такого приложения является сквозное шифрование, открытый исходный код, отсутствие записи IP-адреса, самоуничтожающиеся сообщения. Другими, схожими по функциональности и конфиденциальности мессенджерами являются WickrMe, Wire, Threema, Silence, Dust[114];

– утечка персональных данных и информации ограниченного доступа, как правило, систематизированных в базах данных, представленных на просторах теневого Интернета и используемых, в том числе, для совершения различного рода преступлений. Так, согласно соответствующему отчету экспертно-аналитического центра InfoWatch, количество утечек информации в России в первом полугодии 2022 г. по сравнению с аналогичным периодом прошлого года выросло в 1,5 раза, более 80 % утечек спровоцированы хакерскими атаками. Так, в первом полугодии 2022 г., объем «утекшей» информации составил 187,6 млн записей. Такие утечки произошли в РЖД, авиакомпании «Победа», телекоммуникационных компаниях «Ростелеком» и «ВымпелКом», сервисах «Мир Тесен», Fotostrana, сервисах доставки «Яндекс.Еда», DeliveryClub и т. д.. Так, за первые шесть месяцев 2022 г. в ДаркВебе обнаружены сведения о 2036 утечках[115].

---

[113] Приговор Кировградского городского суда Свердловской области от 05 августа 2016 г. № 1-105/2016...

[114] ТОП-5 самых защищенных и безопасных мессенджеров 2023 года. URL: https://trashexpert.ru/software/security/ -secure-and-encrypted-messaging-apps (дата обращения: 08.01.2023).

[115] Отчет об утечке данных за 1-е полугодие 2022 года. URL: https://www.infowatch.ru/sites/default/files/analytics/ files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pd f (дата обращения: 08.01.2023).

Так, 21 февраля 2022 г. на официальном сайте МВД России сообщено, что сотрудниками Управления «К» МВД России пресечена деятельность группировки, создавшей в сети Интернет площадки, на которых осуществлялась покупка и продажа персональных данных пользователей систем ДБО, банковских карт, номеров социального страхования граждан, проживающих за рубежом, а также доступов к серверам по протоколу удаленного рабочего стола[116].

7 февраля 2022 г. специалисты Управления «К» МВД РФ заблокировали работу двух популярных «кардерских» ресуров. Полностью были закрыты доступ к «Ferumshop» (fe-acc18.ru) и «Skyfraud» (sky-fraud.ru)[117];

– возможность регистрации серверов, используемых для совершения преступлений на территории других государств, что является мощным инструментом противодействия расследованию. Особый способ совершения преступлений в ИТТ посредством использования киберпространства позволяет нивелировать какие-либо государственные границы и независимо от места нахождения совершать хищения на территории различных государств. К примеру, серверы хакерской группировки Cobalt размещались в Германии, Литве, Панаме, а хищения были совершены в 40 странах мира[118];

– массовое распространение вредоносных компьютерных программ на компьютерные устройства граждан. Довольно часто, распространение таких программ осуществляется посредством рассылки «фишинговых» сообщений, ссылок, при открытии и переходе по которым происходит установка на устройство соответствующих вредоносных компьютерных программ. Впоследствии базы данных с зараженными устройствами предлагаются к реализации на форумах теневого Интернета.

---

[116] Фигурантам уголовного дела о неправомерном обороте средств платежей предъявлены обвинения. URL: https://мвд.рф/mvd/structure1/Upravlenija/убк/Publikacii_i_vistuplenija/item/28647999 (дата обращения: 24.01.2023).

[117] Управление «К» МВД РФ заблокировало два популярных «кардерских» ресурса. URL: https://habr.com/ru/news/ 650321 (дата обращения: 24.01.2023).

[118] Cobalt (хакерская группа). URL: https://ru.wikipedia.org/wiki/Cobalt_(хакерская_группа) (дата обращения: 01.10.2022).

По данным Лаборатории Касперского доля спама в 2022 г. оставалась на уровне 50 % от общего объема входящих сообщений в электронной почте[119].

Анализ судебно-следственной практики показывает, что результатами проведения компьютерных экспертиз становятся обнаруженные на компьютерных устройствах потерпевших различные вредоносные приложения, например Whatsapp-1.apk, Odnoklassniki_203.apk, Odnoklassniki.apk, 2GIS.apk, Play_Market.apk, Instagram.apk[120];

– возможность совершения хищения денежных средств с использованием служебного положения. В данном случае имеется в виду наличие такой возможности у сотрудников, прежде всего, кредитных организаций. Наличие денежных средств на банковских счетах граждан и обладание, в силу должностных обязанностей, возможностью доступа в компьютерную банковскую систему, повлекли за собой реальность совершения хищений посредством перечисления денежных средств на подконтрольные преступникам счета. Нередко, для сокрытия своих действий преступники для входа в банковскую систему используют ставшие им известными логины и пароли коллег по работе. Примером совершения подобного преступления являются материалы такого уголовного дела в отношении ПАО КБ «Восточный»[121];

– пренебрежение требованиями компьютерной безопасности, в т. ч.: неиспользование или использование устаревшего антивирусного программного обеспечения, использование простых логинов и паролей.

Специалистами информационной безопасности Банка России в качестве соответствующих потенциальных угроз также выделяются: отсутствие установленных актуальных обновлений на основные продукты, как правило, используемые в кредитных организациях; отсутствие сегментирования сети; отсутствие или неправильная настройка систем управления событиями

---

[119] Корпоративный фишинг и спам в 2022 году: все чаще атакуют HR-специалистов и бухгалтеров. URL: https://www.kaspersky.ru/about/press-releases/2022_korporativnyj-fishing-i-spam-v-2022-godu-vsyo-chashe-atakuyut-hr-specialistov-i-buhgalterov (дата обращения: 22.01.2023).

[120] Приговор Октябрьского районного суда г. Барнаула от 20 апреля 2017 г. № 1-18/2017...

[121] Уголовное дело № 1-675/2019 // Архив Советского районного суда г. Красноярска.

информационной безопасности, что позволяет атакующему скрытно долгое время находиться в сети; неправильная настройка межсетевого экранирования[122];

– низкий уровень прикладного программного обеспечения по защите информации в корпоративных сетях, концентрация компьютерной информации различного назначения в незащищенных базах данных, наличие возможности несанкционированного доступа к компьютерной информации посторонних лиц, широкий круг пользователей[123];

– использование в противоправных целях компьютерных сетей, таких, как Yggdrasill, cjDNS, Briar, SignalOffline, FireChat, позволяющих организовать доступ к информации, распространение которой в России запрещено[124];

– возможность использования электронных платежных систем, электронных кошельков, перевода похищенных денежных средств в цифровую валюту, криптовалюту, являются дополнительными мерами сокрытия преступной деятельности и облегчения способов ее совершения. Так, по делу Lurk, один из руководителей структурных подразделений из обналиченных денежных средств часть оставлял себе, остальные переводил в биткоины[125].

Одной из особенностей совершения преступлений в сфере компьютерной информации, является то, что преступники весьма внимательно относятся к его подготовке. В первую очередь это относится к специалистам высокого уровня. Данное обстоятельство является следствием влияния сложившейся обстановки на выбор способов совершения преступления и поведения его участников.

Так, к примеру, уже обладая всеми необходимыми познаниями в сфере совершения хищений посредством компьютерных технологий, а также располагая всеми необходимыми инструментами для его совершения, у участников группировки Cobalt на изучение инфраструктуры одного банка уходило по нескольку недель[126].

---

[122] Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России …

[123] Поляков В. В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. № 2-1 (78). С. 115.

[124] Гаврилин Ю. В. Указ. соч. С. 45.

[125] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1...

[126] Group-IB: несмотря на арест лидера, группа Cobalt продолжает атаки на банки. URL: https://www.group-ib.ru/media-center/press-releases/gib-cobalt-activity/ (дата обращения: 04.01.2023).

Также, еще на этапе подготовки к совершению деяния, преступниками предпринимаются меры к созданию благоприятных условий по изменению обстановки после совершения преступления. Как правило, в большей степени, это относится к удалению следовой картины преступной деятельности: использование самоуничтожающихся компьютерных программ, удаление из компьютерных систем различных файлов, регистрационных записей и т. д.

Все это позволяет преступникам создать для себя наиболее благоприятные условия реализации противоправного деяния и приблизиться, в их мечтах и грезах, к аспекту безнаказанности. Таким образом, с учетом оценки реальной действительности, преступники прилагают все усилия к изменению обстановки совершения преступления в свою пользу.

В свою очередь, неблагоприятными факторами, с точки зрения преступников, влияющими на состояние обстановки совершения преступления являются наличие высокой степени программно-технической защиты компьютерных средств посредством незаконного доступа к которым осуществляется совершение преступления, соблюдение правил обращения с компьютерной информацией и доступа к ней и т. д.

Как известно, структурными элементами обстановки совершения преступления являются время и место его совершения. Данные элементы неразрывно связаны с обстановкой, а точнее, определяют ее. Именно пространство и время, являясь ключевыми общеобязательными характеристиками существования материи, в свою очередь определяют характер формирования и существования определенной среды - обстановки.

Одним из ключевых элементов обстановки является место совершения преступления, оказывающее «влияние на весь процесс формирования следовой картины и, соответственно, является носителем как материальных, так и идеальных следов, а значит, обладает существенной информативностью» [127] . Правильное определение и установление места совершения преступления во

[127] Коломинов В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. … канд. юрид. наук. Иркутск, 2017. С. 39.

многом предопределяет успешность получения криминалистически значимой информации по делу и способствует раскрытию преступления.

В связи с имеющимися специфическими особенностями совершения преступлений в сфере компьютерных технологий, в научном сообществе существуют различные подходы к определению места их совершения.

Так, Л. В. Иванова, Г. В. Пережогина резюмируют, что местом совершения преступления «следует считать место ввода информации и выхода в информационно-телекоммуникационную сеть с последующей реализацией из этого места преступного деяния, независимо от места, где наступили последствия»[128].

По мнению В. В. Коломинова, «кроме телекоммуникационной сети, местом совершения мошенничества являются места обналичивания денежных средств, полученных путем обмана»[129].

Отсутствие единого подхода в данном вопросе породило не единообразную следственно-судебную практику, анализ которой показывает, что преимущественно местом совершения преступления признается конкретное место совершения преступления, а также место наступления общественно-опасных последствий. Так, в ходе расследования одного из уголовных дел по факту совершения мошенничества в сфере компьютерной информации сотрудницами ПАО КБ «Восточный», местом совершения преступления были признаны их рабочие места, где размещались компьютерные средства, посредством которых они входили в банковскую систему и совершали хищения денежных средств[130].

При существовании не единообразной судебно-следственной практики, с учетом специфики рассматриваемой категории преступлений (включающей как основное, так и сопутствующие преступления), своевременно уместными стали следующие разъяснения: согласно п. 19 постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной

[128]Иванова Л. В., Пережогина Г. В. Указ. соч. С. 166.

[129] Коломинов В. В. Установление места совершения преступления в процессе расследования мошенничества в сфере компьютерной информации // Криминалистические чтения на Байкале – 2015 : мат-лы Междунар.-науч. практ. конф. (Иркутск, 18–19 июня 2015 г.). Иркутск, 2015. С. 267.

[130] Уголовное дело № 1-675/2019 // Архив Советского районного суда г. Красноярска.

практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»), «местом совершения такого преступления является место совершения лицом действий, входящих в объективную сторону состава преступления»[131]; согласно изменениям от 15.12.2022 в постановлении Пленума Верховного Суда РФ № 48 «местом совершения мошенничества, состоящего в хищении безналичных денежных средств, исходя из особенностей предмета и способа данного преступления, является, как правило, место совершения лицом действий, связанных с обманом или злоупотреблением доверием и направленных на незаконное изъятие денежных средств»[132].

Одним из определяющих моментов в установлении места совершения преступления является способ его совершения. Так, при совершении мошенничества в сфере компьютерной информации посредством установления контроля за работой банкомата при непосредственном механическом воздействии на него и последующим заражением его компьютерной системы управления вредоносной программой, местом совершения преступления будет являться место расположения конкретного банкомата. Однако при совершении хищения из того же банкомата посредством установления удаленного доступа к компьютерной системе соответствующей кредитной организации и генерации команды на автоматическую выдачу денежных средств, местом совершения преступления будет место расположения компьютерных устройств преступника. А при осуществлении преступных действий с использованием различных компьютерных устройств, расположенных на значительном удалении друг от друга, таких мест может быть несколько.

---

[131] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37. URL: https://www.consultant.ru/document/cons_ doc_LAW_434573 (дата обращения: 20.12.2023).

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

Необходимо отметить, что кроме мест совершения преступления в процессе расследования преступлений устанавливаются также места, обладающие значимой криминалистической информацией.

Так, места обналичивания, снятия со счетов денежных средств, добытых преступным путем, могут обладать значительной информативностью, в частности большой объем такой информации может содержаться в видеозаписях с камер видеонаблюдения. Места создания, модификации вредоносных компьютерных программ могут обладать информацией об элементах их конфигурации, других различных материальных и виртуальных следах и т. д.

Кроме того, при совершении преступления посредством удаленного доступа, немаловажное криминалистическое значение имеет место нахождения компьютерных устройств потерпевшего, поскольку детальный анализ их содержимого позволяет получить значимую часть следовой картины преступной деятельности, необходимой для успешного расследования преступления и изобличения виновных лиц. Так, при совершении хищений посредством установления контроля за работой информационной инфраструктуры банковских организаций на компьютерных устройствах в последствии обнаруживаются следы работы ВПО.

Кроме того, «на первоначальных стадиях, когда лицо не установлено, местом совершения преступления на момент возбуждения уголовного дела необходимо считать место проживания потерпевшего»[133].

Отличительной особенностью совершения рассматриваемого вида преступлений является отсутствие привычного контакта между потерпевшим и преступником. При этом компьютерные устройства потерпевших и преступников могут территориально находиться на значительном удалении друг от друга и даже размещаться на территории различных государств, что существенным образом затрудняет процесс расследования. Как уже отмечалось, одним из преступных сообществ преступления совершались на территории более 40 стран мира. Все это

[133] Белова Н. В., Белов А. В. Место совершения дистанционных хищений (проблемы практики применения) // Судебная власть и уголовный процесс. 2021. № 2. С. 72.

стало возможным благодаря использованию в преступной деятельности возможностей своеобразного компьютерного пространства, многие авторы данное пространство выделяют как одно из мест совершения рассматриваемой группы преступлений.

Следует отметить, что в научном сообществе существуют различные мнения по поводу наименования данного вида пространства: «киберпространство», «виртуальное пространство», «цифровое пространство». Приведем некоторые из них.

Так, Е. П. Ищенко, характеризуя «виртуальное» пространство совершенно верно указывает, что «взаимодействующие в нем объекты (файлы данных и программ), которые участвуют в процессе образования возникающих при этом следов, не имеют внешнего строения. Весь арсенал средств и методов работы с материальными следами, накопленный трасологией, здесь оказывается практически бесполезным»[134].

К примеру, Л. В. Иванова, Г. В. Пережогина, предлагая именовать данное пространство «цифровым», определяют его как часть информационного, объединяющего посредством телекоммуникационных технологий информационные ресурсы, средства взаимодействия субъектов информационной сферы, в т. ч. информационные системы и сайты в сети Интернет и сети связи[135].

Видится, что данное определение является довольно сложно сконструированным, затрудняющим понимание, уяснение сути и правоприменительную идентификацию явления.

И. М. Рассолов, давая определение «киберпространству», указывает, что «это сфера социальной деятельности, связанная с оборотом информации во Всемирной информационной паутине, а также в других информационно-

[134] Ищенко Е. П. Виртуальное пространство как объект криминалистического познания // Криминалистика и судебно-экспертная деятельность в условиях современности : мат-лы Междунар. науч.-практ. конф. (26 апреля 2013 г.) : в 2 т. / Краснодарский университет МВД России. Т. 1. Краснодар, 2013. С. 20.

[135] Иванова Л. В., Пережогина Г. В. Указ. соч. С. 160.

коммуникационных сетях (региональных, опорных, ведомственных, корпоративных)»[136].

Применительно к данному определению необходимо отметить, что в указанной формулировке акцент сделан на соответствующих сетях, при этом не уделено должного внимания самому объекту (компьютерным устройствам и т. д.), посредством которого и происходит формирование данных сетей и осуществляется взаимодействие в данном пространстве.

Наряду с этим, в п. «д» ст. 4 Стратегии развития информационного общества Российской Федерации на 2017–2030 годы, применительно к данному вопросу, приводится еще одно понятие – информационное пространство, под которым понимается «совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры»[137].

Необходимо отметить, что анализ данного определения информационного пространства позволяет констатировать, что оно является наиболее полным, отражающим его суть, структуру и соответствующие характеристики исследуемой среды.

Не вдаваясь в подробности терминологического различия данного пространства, необходимо отметить, что, исходя из имеющихся условий внешней обстановки (наличие соответствующих компьютерных устройств и их уровня, имеющиеся навыки компьютерной грамотности и т. д.), преступник самостоятельно создает своего рода условия, обстановку, в рамках и по сценарию которой и будет происходить действие в этом киберпространстве. Так, наметив для совершения преступления определенную цель, например, совершение хищения в одном из банков, преступник, в зависимости от уровня квалификации пишет или приобретает соответствующее ВПО, в случае необходимости производит его модификацию, изучает имеющиеся в организации меры информационной защиты, предпринимает усилия по их техническому

[136] Рассолов И. М. Указ. соч. С. 13.
[137] О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы …

устранению и т. д. Таким образом правонарушитель совершает действия, обеспечивающие, по его мнению, обстановку нераспознаваемого, беспрепятственного, результативного, безнаказанного протекания действия в киберпространстве.

Другим взаимообуславливающим элементом обстановки совершения преступлений в сфере компьютерной информации является время его совершения. Согласно ч. 2 ст. 9 УК РФ, временем совершения преступления признается время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий.

Учитывая способность компьютерных устройств к фиксации времени совершения различных действий, в т. ч. с компьютерной информацией, определение времени совершения преступления не вызывает значительных трудностей. В данном случае большего внимания может потребовать вопрос определения точности его установки на соответствующем компьютерном устройстве, не исключая возможности его умышленного изменения с целью сокрытия преступной деятельности.

При этом в зависимости от способа совершения мошенничества в сфере компьютерной информации можно выделить свои характерные особенности времени его совершения.

Так, в случае совершения преступления посредством неправомерного доступа к информационной инфраструктуре кредитной организации можно отметить, что такие хищения требуют длительной подготовки (с момента проникновения в компьютерную систему организации до совершения преступления может пройти несколько недель) и преимущественно совершаются в вечернее время пятницы, в выходные или праздничные дни. Тем самым преступниками предпринимаются дополнительные меры по созданию наиболее благоприятной обстановки совершения преступления, в т. ч. по противодействию обнаружения и пресечения преступной деятельности. Так, по делу Lurk преступления совершались 30 декабря, 20 февраля – перед праздничными днями. Денежные средства с банковских карт снимали в ночное время, в связи с

установленным суточным лимитом для снятия наличных[138]. Такие преступления, как правило, хорошо спланированы и относятся к «организованному» типу мошенничества в сфере компьютерной информации, рассмотренному в предыдущем параграфе.

Совершение преступлений посредством установления контроля за работой банкоматов, как правило, совершается в вечернее или ночное время, позволяющее исключить, или минимизировать, возможность наблюдения за действиями преступников.

Совершение мошенничества в сфере компьютерной информации с использованием служебного положения, например, сотрудниками банков, напротив, совершается в рабочее дневное время.

Проведенные исследования рассматриваемой группы преступлений, а также детальный анализ обстановки как элемента криминалистической характеристики преступлений позволяют полагать о возможности включения в ее структуру дополнительных элементов, рассмотрение которых будет способствовать более всеобъемлющему и всестороннему определению явления.

Возможность включения в обстановку совершения преступления дополнительных элементов поддерживается многими учеными. Так, Р. Г. Камнев, указывает, что обстановка «вполне может включать и некоторые другие объективные условия в виде особенных, юридически значимых обстоятельств, ситуаций и факторов, происходящих из природы возникновения и стечения различных социальных отношений и окружающей среды»[139].

М. В. Кардашевская, Ю. В. Гаврилин, считают что электронная платежная система («Яндекс.Деньги», WebMoney, PayPal, QIWI и др.) в криминалистической характеристике хищений должна рассматриваться как обстановка совершения преступления[140].

---

[138] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

[139] Камнев Р. Г. Указ. соч. С. 133.

[140] Кардашевская М. В., Гаврилин Ю. В. Электронная платежная система как элемент обстановки преступления // Академическая мысль. 2020. № 2 (11). С. 22–23.

Характер рассматриваемых преступлений позволил сделать вывод о возможности включения в обстановку их совершения наличие соответствующих компьютерных устройств, программно-аппаратных и других технических средств, с помощью и посредством которых совершаются данные преступления. В ходе проведенного анкетирования 75,3 % респондентов указали на верность данной позиции (Приложение 1).

Данное обстоятельство является отличительной чертой совершения преступлений рассматриваемой категории. Обладание соответствующими инструментами определяет способ совершения преступления и сокрытия следов преступной деятельности, является важным фактором благоприятного или неблагоприятного стечения для преступника обстоятельств. Так, обладание дорогостоящим компьютерным оборудованием и высококвалифицированными вредоносными компьютерными программами, обладающими признаками слабой распознаваемости, способными к самоуничтожению и т. д., способствует созданию условий, при которых преступным киберформированиям длительное время удается безнаказанно заниматься осуществлением преступной деятельности. Стоимость таких компьютерных устройств и компьютерных программ может быть как незначительной, так и требовать серьезных финансовых вложений. Как правило, организация преступления на таком уровне свидетельствует об его отнесении к «организованному» типу мошенничества.

При этом в случае совершения преступлений посредством осуществления доступа к соответствующим базам данных кредитных или иных организаций, а также в других случаях совершения преступления (к примеру, посредством использования соответствующей банкноты, позволяющей извлечь ее из банкомата), где характер преступной деятельности не предусматривает обладание такими компьютерными устройствами, речь может идти только о наличии доступа к ним.

В целом, оценивая значимость данного структурного элемента криминалистической характеристики, необходимо отметить, что обладая возможностью оценки обстановки совершения преступления, как правило, уже после его окончания, сотрудники правоохранительных органов, при должном

внимании, могут восстановить ее полную картину до и во время совершения преступления, получив тем самым знания относительно способа, типа, уровня организации преступления, способствующие еще на первоначальном этапе расследования выдвижению определенных криминалистических версий и более эффективному выстраиванию процесса расследования.

2.3. Личность типичных преступника и потерпевшего и их криминалистическое значение

В силу наличия довольно тонкой квалификационной грани между различными составами компьютерных преступлений, рассуждая о типичных свойствах личности преступника, занимающегося совершением мошенничества в сфере компьютерной информации, а также с учетом того обстоятельства, что данное преступление, как правило, совершается в совокупности с рядом других сопутствующих составов, на наш взгляд, целесообразно вести речь о характерных особенностях личности таких преступников в едином аспекте[141].

Изучению личности преступника в научном сообществе всегда уделялось должное внимание. Данное обстоятельство породило существование различных формулировок понятия данного явления.

Так, В. В. Лунеев под личностью преступника понимает «человека, виновно совершившего уголовно наказуемое деяние, обладающего совокупностью социальных криминологически значимых свойств, которые во взаимодействии с криминогенными факторами внешней среды обусловили преступное поведение»[142].

По мнению Ю. М. Антоняна, «личность преступника выступает в качестве совокупности социально значимых негативных свойств, образовавшихся в

[141] Харина Е. А. Личность типичного преступника, совершившего мошенничество в сфере компьютерной информации // Российский следователь. 2023. № 9. С. 54.

[142] Лунеев В. В. Курс мировой и российской криминологии. В 2 т. Т. 1. Общая часть. В 3 кн. Кн. 3 : учеб. для вузов. М., 2023. С. 24.

процессе многообразных и систематических взаимодействий с другими людьми»[143].

О. В. Старков под личностью преступника понимает «личность человека как социального существа, обладающего системой криминогенных свойств, приведших его непосредственно к совершению преступления»[144].

Рассуждая о личности, как явлении, необходимо отметить, что способ мышления человека заложен на генном аппарате и в дальнейшем совершенствуется в процессе жизни человека. Становление личности начинается с детства, где сознание ребенка формируется посредством копирования поведения родителей и окружающих его людей, исходя из уровня морально-нравственных принципов совершаемых ими поступков.

Анализируя способность к противоправному поведению, как к явлению в целом, видится, что практически каждый человек способен на совершение правонарушения, однако с учетом уровня индивидуальной степени осознанности разные люди по-разному отнесутся к одному и тому же проявлению противоправной деятельности или возможности ее проявления. Так, один человек, образно представив для себя возможность совершения того или иного правонарушения или преступления, исходя из своего внутреннего цензора, подобные действия сочтет неприемлемыми ни при каких обстоятельствах. Другой может допустить возможность противоправного поступка, однако не решится на его совершение под страхом наказания. Третий же, совершив однажды противоправный поступок и будучи подвергнутым наказанию, правильно осознав полученный жизненный урок, раз и навсегда откажется от совершения подобного в будущем. А четвертый, наоборот, уловив даже еле просматриваемую перспективу возможности совершения правонарушения или преступления, с инициативой и даже с азартом приступит к реализации задуманного.

Степень вовлеченности лиц, переступивших грань правовой дозволенности также различна: одни преступники с опаской решатся на совершение

---

[143] Антонян Ю. М. Криминология : учеб. для вузов. М., 2024. С. 80.
[144] Старков О. В. Криминология. Теория и практика : учеб. для вузов. М., 2021. С. 232.

эпизодичного преступления, после которого будут испытывать чувство вины и страх быть подвергнутым наказанию, другие будут считать нормой систематическое совершение преступлений небольшой или средней тяжести, третьи же будут желать и стремиться к совершению тяжких и особо тяжких преступлений, характеризующихся наибольшей степенью опасности.

Занимаясь подготовкой и совершением преступления, организм преступника находится в своеобразном стрессовом состоянии, а после успешного совершения деяния фигурант получает своего рода наслаждение и адреналин. Неправильно осознанное внутреннее движение, работая на нейронном уровне, набирает силу, проявляясь зависимостью и необходимостью совершения повторных деяний, действуя по принципу наркозависимости.

Видится, что суть преступника как явления в целом заключается в осуществлении какого-либо воздействия на другую структуру посредством подчинения своей воле.

Наряду с единым образом личности преступника, в зависимости от конкретного вида преступной направленности, существуют свои характерные отличительные свойства личности преступника.

Рассматривая личность преступника, занимающегося совершением рассматриваемых деяний, видится, что его специфической, отличительной чертой является то, что преступник, как правило, с жертвой не знаком и его не интересует его личностная характеристика, определяющим моментом является обладание соответствующим имуществом, организация доступа к которому и является главной задачей преступника.

В целом, в социуме принято выделять следующие характерные отрицательные черты внешнего отображения социального поведения специалистов в сфере компьютерных технологий, в большей степени имеющие отношение к лицам преступной направленности:

– пренебрежительное отношение к физическому труду, в частности к осуществлению трудовой деятельности, требующей серьезных физических усилий, и в целом к лицам, имеющим рабочие специальности. Как правило,

будучи сами недостаточно физически развитыми, считают обратное уделом людей с недостаточным уровнем умственных способностей;

– низкий уровень либо отсутствие патриотизма. Как правило, относится к молодым специалистам в сфере ИТТ, обладающим слабыми познаниями в области истории и русской культуры, воспитанным на компьютерных играх, подмене истинных ценностей, навязывании чуждых для России западных ориентиров. Как известно, немалая часть таких специалистов покинули РФ, живут и работают за рубежом, считая родину отсталым, недоразвитым государством;

– ограниченный круг общения, невысокий уровень социального взаимодействия и адаптации, основной причиной которых являются частичная виртуализация жизнедеятельности человека, подмена ценности человеческого общения на виртуальное;

– низкий уровень моральных принципов, отсутствие каких-либо сожалений о характере и размере причиняемого вреда;

– уверенность в своей исключительности и безнаказанности, стремление к интеллектуальному доминированию. В результате профессионального взросления, совершения ряда безнаказанных преступлений, усовершенствованием применяемых средств защиты и методов конспирации, самооценка таких специалистов неминуемо возрастает[145].

Большинство из вышеуказанных качеств действительно характерны именно для компьютерных преступников, однако, некоторые из них, применимы как к субъектам других видов преступной направленности, так и к проявлениям социального поведения законопослушных граждан. К примеру, отнесение характеристики о низком уровне патриотизма не обязательно присуще компьютерным преступникам. Так, объявленная в 2022 г. в РФ частичная мобилизация для участия в специальной военной операции сподвигла тысячи мужчин призывного возраста к стремлению покинуть территорию государства.

[145] Харина Е. А. Личность типичного преступника ... С. 54.

В научной среде существуют различные взгляды на классификацию преступников в сфере компьютерной информации. Так, Н. П. Яблоков выделяет следующие группы таких преступников:

– профессиональные взломщики компьютерных сетей и программ, занимающиеся созданием и распространением вредоносных программ-вирусов;

– лица, имеющие разного рода психические отклонения, страдающие компьютерными фобиями (своеобразным профессиональным компьютерным заболеванием);

– профессиональные взломщики компьютерных сетей и программ – члены ОПГ, занимающихся преступным бизнесом в сфере компьютерной информации[146].

М. В. Жижиной и Д. В. Завьяловой субъекты рассматриваемой преступной деятельности подразделены на следующие подгруппы:

– «лица с разным уровнем развития навыков в сфере информационных технологий, не ведущие систематической преступной деятельности;

– без развитых навыков в сфере информационных технологий или со средним их уровнем, ведущие систематическую преступную деятельность, зачастую состоящие в преступных группировках;

– с высоким уровнем навыков в сфере информационных технологий, ведущие систематическую преступную деятельность»[147].

В. В. Коломинов таких преступников предлагает разделять:

1) на профессиональных субъектов преступной деятельности («хакеров», «компьютерных злоумышленников»), которые являются программистами высшего класса (IT-специалистами) и работают либо с уже реализованными программами, либо придумывают уникальные программы самостоятельно;

[146] Яблоков Н. П. Криминалистика : учебник. М., 2009. С. 360.

[147] Жижина М. В., Завьялова Д. В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) // Актуальные проблемы российского права. 2022. Т.17, № 5 (138). С. 154.

2) непрофессиональных субъектов преступной деятельности (могут иметь специальное образование или относятся к «самоучкам»). Они в свою очередь делятся:

а) на продвинутых пользователей (могут создавать несложные компьютерные программы, сайты, понимают всю механику действия и работы на технически сложных устройствах и ПК);

б) уверенных пользователей (знают, как работают компьютерные системы, могут сами устанавливать компьютерные программы)[148].

Полученный в ходе диссертационного исследования опыт изучения личности преступников в сфере компьютерной информации, посредством обращения к судебно-следственной практике рассматриваемой категории преступлений, а также к опыту и знаниям различных экспертов (Приложение 2), посредством анализа и обобщения их мнений (Приложение 3), позволили прийти к выводу о наличии существенных, отличительных черт личности между компьютерными специалистами различного уровня профессионализма. Для определения наиболее точной криминалистической характеристики нами выделены определенные уровни профессионального мастерства таких преступников, с присущими им характерными особенностями личности[149]. Данная гипотеза нашла свое подтверждение в ходе проведенного анкетирования, когда 76,2 % (945 человек) опрошенных правоприменителей подтвердили правдивость данных выводов (Приложение 1).

1. **Специалисты высокого уровня**, своего рода эксперты в сфере ИТТ. Лица, входящие в данную категорию обладают незаурядными, обширными и глубокими познаниями в области компьютерной грамотности, сами являются разработчиками различных компьютерных программ, генераторами идей по преодолению средств программно-технической защиты. Деятельность в сфере информационных технологий, как правило, является единственным профессиональным направлением жизнедеятельности таких людей, становится

[148] Коломинов В. В. Расследование мошенничества в сфере компьютерной информации... С. 69.
[149] Харина Е. А. Личность типичного преступника... С. 54–55.

образом их жизни. Компьютерная среда является для них местом приложения, реализации и развития имеющегося творческого потенциала. Для такого рода специалистов преступная деятельность выступает в роли компьютерной игры, разработчиком правил и принципов которой являются они сами[150].

Как правило, предрасположенность к подобной деятельности проявляется в довольно юном возрасте. Так, гр. К., организатор ОПС Lurk, интерес к разработкам в сфере информационных технологий проявлял с детства, еще в 2000 г., будучи школьником, стал победителем конкурса персональных веб-страниц[151].

Являясь обладателями большого опыта совершения хищений посредством преступной реализации высоких компьютерных знаний, такие преступники обладают большой степенью уверенности, а порой и самоуверенностью, в возможности успешной реализации преступного умысла в отношении любого объекта посягательства[152]. При этом выбор объекта преступного посягательства, как правило, носит избирательный характер и зависит от степени развитости эго профессионала. Так, по делу Lurk хищения совершались у хозяйствующих субъектов РФ, обладающих серьезным финансовым состоянием, и, как следствие, соответствующим уровнем организации защиты информационной инфраструктуры. Только по двум из эпизодов деятельности ОПС было похищено: у ПАО АКБ «Металлинвестбанк» 677 594 317 руб. 70 коп., у КБ «Гарант-Инвест» (АО) 467 415 000 руб.[153]

Несомненно, преступления, организованные и совершенные специалистами такого уровня, относятся к «организованному» типу мошенничества в сфере компьютерной информации, описанному нами в параграфе 2.1. настоящего диссертационного исследования.

Особенностями личности таких преступников является полное отсутствие каких-либо сожалений относительно степени наступления общественно-опасных

---

[150] Харина Е. А. Личность типичного преступника ... С. 55.

[151] Антоненков Д. «Идет невидимая война. Мы стали ее участниками». Обвиняемые рассказывают историю группы хакеров Lurk. URL: https://66.ru/news/internet/24829 (дата обращения: 28.09.2023).

[152] Харина Е. А. Личность типичного преступника ... С. 55.

[153] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

последствий их преступной деятельности. При этом главной отличительной чертой психологического состояния таких преступников, отличающей представителей данной категории от других, менее компетентных компьютерных преступников, является подготовка и совершение преступлений с высокой степенью азарта, граничащей с ажиотажем[154].

Как уже отмечалось ранее, после успешного совершения очередного преступления организм фигуранта получает огромное наслаждение и очередную дозу адреналина. Аналогично с ситуацией наркозависимых людей, когда с увеличением стажа употребления изменяется объем и качество принимаемых соответствующих средств, в ситуации с компьютерными преступниками, с получением все бóльших соответствующих знаний и навыков, опыта преодоления средств программно-технической защиты, у таких преступников возникает потребность в поиске и выборе специфических, труднодосягаемых объектов преступного посягательства и их количестве[155].

Специалист такого уровня имеет высокий статус в «своих кругах», пользуется неподдельным уважением. В силу обладания очень низкими моральными принципами характеризуется отсутствием каких-либо угрызений совести в результате наступления общественно-опасных последствий посредством реализации преступной деятельности.

Жертвы для таких преступников являются даже не целью, а смыслом жизни, формой и средством реализации их жизненных потребностей в социальной реализации творческого потенциала. При этом к самой жертве испытывают пренебрежительное, надменное отношение. Такое же поведение может просматриваться и в социальных взаимодействиях данной категории преступников.

Достижение внутренней профессиональной зрелости преступников такого уровня проецируется вовне соответствующим уровнем мышления, способом изложения мыслей и манерой поведения в социуме. Достигнув зрелости,

---

[154] Харина Е. А. Личность типичного преступника... С. 55.
[155] Там же.

изменить свой характер, склад ума, сферу сознания и способ мышления, специалисты такого уровня уже не могут и не стремятся.

Особенностью образа мышления компьютерного специалиста высокого уровня является построение мышления по принципу четкой структуры, шаблона, полное понимание и восприятие которого обладает очень мощной внутренней силой. Имеющийся уровень знаний и опыта, способность анализировать, сопоставлять, прогнозировать возможные исходы различных ситуаций, способность к образному видению отдельных элементов и ситуации в целом, позволяют специалистам такого уровня производить удары точно в цель и добиваться поставленной цели. Без учета ориентированности их противоправной деятельности, направленной на разрушение гармонии и целостности определенных областей общественных отношений, такого специалиста можно было бы без преувеличения назвать гением своего дела.

Ярким примером создания, «успешного» функционирования и «заката» деятельности «непобедимой» хакерской группировки, на протяжении нескольких лет являвшейся лидером киберпреступного пространства Российской Федерации является ОПС Lurk.

14 февраля 2022 г. Кировским районным судом Екатеринбурга был вынесен приговор двадцати одному участнику данного преступного сообщества, в т. ч. его лидеру гр. К.[156].

Группа Lurk носила чуть ли не легендарный статус. Прежде всего, из-за своей закрытости: многие мелкие и средние группировки изъявляли желание «поработать» с ними, но те всегда предпочитали действовать без посторонних. Поэтому, когда группа Lurk предоставила доступ к одной из своих программ Angler, она получила большую популярность – «продукт» от абсолютных авторитетов «киберандерграунда» не нуждался в обширной рекламе и в конце 2013 г. стал одним из ключевых подобных инструментов на criminal2criminal-рынке[157].

Из проведенного компанией «Бифит» исследования следует, что из всех реализованных в системе iBank 2 средств защиты против Lurk эффективен только

[156] Харина Е. А. Личность типичного преступника ... С. 55.
[157] Стоянов Р. Охота на Lurk …

контроль на стороне сервера банка, остальные меры противодействия, были успешно преодолены авторами Lurk, что говорит об их профессионализме. По мнению экспертов «Лаборатории Касперского», в целом Lurk оставляет впечатление сложной и мощной системы. Упорство и сосредоточенность, с которыми авторы работают над своим троянцем, говорит о высокой степени их мотивации[158].

Другим примером работы высококвалифицированных компьютерных специалистов является деятельность группы Cobalt (Carbanak), жертвами которой стали финансовые организации более чем в 40 странах мира, ущерб составил более чем 1 млрд евро.

На совершение хищений у одного банка уходило до нескольких недель. Изученные материалы о деятельности финансовых организаций позволяли производить точные удары и похищать крупные суммы денежных средств. Длительное время факторами успешного функционирования преступной организации также являлось постоянное тестирование новых инструментов и схем, частая смена локации проведения атак, хорошая осведомленность о работе банковских структур[159].

2. Опытные преступники в сфере ИТТ. В отличие от специалистов высокого уровня опытные преступники, как правило, не являются сами разработчиками соответствующих компьютерных программ, однако с большой степенью активности и профессионализма занимаются их использованием. При этом в процессе эксплуатации в зависимости от схемы и механизма осуществления преступной деятельности могут вносить свои коррективы, адаптируя работу компьютерных средств и устройств соответствующим образом[160].

---

[158] Шульмин А., Прохоренко М. Банковский троянец Lurk: специально для России. URL: https://securelist.ru/ bankovskij-troyanec-lurk-specialno-dlya-rossii/28708 (дата обращения: 20.12.2022).

[159] Group-IB: несмотря на арест лидера, группа Cobalt продолжает атаки на банки. URL: https://www.group-ib.ru/media-center/press-releases/gib-cobalt-activity (дата обращения: 04.01.2023).

[160] Харина Е. А. Личность типичного преступника ... С. 56.

Так, опубликованный исходный код троянской программы ZeuS спровоцировал появление множества модификаций этой программы, разрабатываемых небольшими группами киберпреступников[161].

Другим примером является осуществление, а вернее продолжение, преступной деятельности братьями-близнецами П.. Будучи осужденными к шести годам лишения свободы условно за совершение хищений с использованием системы ДБО, братья продолжили заниматься преступной деятельностью. При этом стали действовать еще осторожнее: «они взяли на вооружение новые вредоносные программы QHost и Patched.IB, автоматизировали процесс хищения и постоянно модернизировали сами вирусы, чтобы их не обнаруживали антивирусы»[162].

Относительно профессиональной деятельности таких специалистов можно отметить, что они не всецело погружены в данную сферу отношений и вполне могут иметь и основную легальную работу, как правило, имеющую отношение к информационным технологиям[163].

В отличие от психологического состояния высококвалифицированных преступников в сфере компьютерных технологий, главной отличительной чертой которых является наличие азарта и стремления совершения подобных преступлений, особенностью психологического состояния опытных преступников является обладание высокой степенью неподдельного интереса к совершению компьютерных преступлений, который в последствии, в случае продолжения осуществления преступной деятельности и совершенствования своего мастерства, может перейти в азарт[164].

Избирательность в объектах преступного посягательства для таких специалистов не имеет особого значения, как правило, жертвами преступлений становятся «полуслучайные» лица, к которым преступники относятся как к шестеренкам в большом наборе своего преступного механизма. По сравнению со

---

[161] Стоянов Р. Охота на Lurk …
[162] Братья по кибероружию …
[163] Харина Е. А. Личность типичного преступника ... С. 56.
[164] Там же.

специалистами низших уровней, опытные преступники в стремлении профессионального роста научились не быть ленивыми и проявляют стремление к совершенствованию своего мастерства. Жадность уже не является преобладающим и побуждающим фактором к совершению преступлений. По мере совершенствования своего профессионального мастерства у специалистов такого уровня все чаще возникают идеи по способам реализации преступного умысла, запуску и функционированию механизма преступления, отысканию и использованию различного рода уязвимостей программно-технической защиты, минимизации оставления следов преступной деятельности[165].

Отношения в социуме специалисты такого уровня выстраивают так, чтобы можно было управлять психикой оппонента. В социальной среде опытных преступников можно определить как психологов, политиков в поведении, умело подстраивающихся под возможные варианты социального общения.

В отличие от специалиста высокого уровня сознание опытного компьютерного преступника не может образно охватить всю необходимую работу по подготовке, совершению и сокрытию преступления в целом, в связи с чем ему требуется больше времени на осознание его отдельных структурных элементов, отдельные случаи могут потребовать обращения к новым знаниям и получению необходимого опыта. В социальном плане особенность такого способа мышления может проявляться невозможностью одномоментной оценки ситуации и необходимостью затраты определенного количества времени на представление, анализ всех возможных аспектов ситуации, оценку всех возможных рисков и т. д.

Как правило, преступления, спланированные и совершенные специалистами такого уровня, относятся к «организованному» типу мошенничества в сфере компьютерной информации, при этом нечастые случаи совершения преступлений, относящихся к «несложному», «бытовому» типу мошенничества, носят несистемный характер.

3. Специалисты среднего уровня в сфере ИТТ. Характеризуются обладанием соответствующих познаний на уровне уверенных пользователей.

---

[165] Харина Е. А. Личность типичного преступника ... С. 56.

Относительно степени вовлеченности в осуществление противоправной деятельности преступников данной категории можно отметить ее несистемный характер. Как правило, отношение к подобному роду преступной деятельности характеризуется устойчивой увлеченностью, она может являться своего рода хобби.

Отличительной особенностью психологического состояния таких преступников является мечтательное, иллюзорное представление о достижении грядущих возможных уровнях специалиста высокого класса, способного на совершение громких, резонансных, безнаказанных преступлений[166].

Особенностями характера специалистов такого уровня является ворчливость, недовольство собой и окружающими, чем вызывает к себе подобную зеркальную реакцию социума. Проявлением теневых сторон личности таких людей является жадность и лень, отсутствие должного усердия, что и является препятствием на пути его профессионального роста и затрудняет переход на уровень опытного компьютерного преступника.

В связи с отсутствием достаточных знаний и опыта, характерной особенностью степени развитости сознания специалистов среднего уровня является фрагментарное видение ситуации. Специалист такого уровня уделяет внимание лишь отдельным аспектам, которые способно охватить его сознание. При этом полное видение всей ситуации или схемы события отсутствует.

Специалист такого уровня уделяет внимание лишь отдельным аспектам, привлекшим его внимание, охватить которые способно его сознание, при этом единомоментное видение всей ситуации или схемы события отсутствует.

Преимущественно, специалистами среднего уровня, в силу невысокого уровня организации и несложного способа, совершаются преступления, относящиеся к «несложному», «бытовому» типу мошенничества в сфере компьютерной информации.

4. «Бытовые», «случайные» компьютерные преступники. Характеризуются невысоким, обывательским уровнем компьютерных знаний.

[166] Харина Е. А. Личность типичного преступника ... С. 56.

Осуществление преступной деятельности может начаться с внезапно возникшего преступного умысла или совершения преступления, не требующего особых специальных познаний. К примеру, для совершения работником кредитной организации действий по изменению состояния своего или подконтрольного ему банковского счета требует только обладания возможностью осуществлять доступ к системе банковского обслуживания клиентов[167].

Так, двое мужчин, являющихся уроженцами Республики Армения, используя билеты Банка России номиналом 1000 и 5000 руб., оснащенные специальными приспособлениями (краями из полимерной пленки и приклеенными полимерными полосками), позволяющими вынуть их из купюроприемных механизмов информационно-платежных терминалов, совершали хищения денежных средств, вызывая сбой нормального функционирования программно-технического обеспечения данных устройств[168].

Успешное и безнаказанное совершение преступлений подобного уровня может спровоцировать человека на совершенствование навыков и умений, подвигнуть на получение новых знаний в сфере компьютерных технологий и к повышению своего потенциала в данной преступной сфере.

Особенностями характера преступников такого уровня является неуверенность в своих действиях и их результате, наличие страха быть изобличенными. Такое поведение является результатом отсутствия необходимых навыков и знаний. В общении с собой и окружающими довольно эмоциональны, преобладает хвастовство, амбициозность, детский психологический уровень развития, нежелание прилагать дополнительные усилия для профессионального роста, что затрудняет совершенствование и дальнейший переход на более высокий профессиональный уровень[169].

Преступления, совершаемые специалистами такого уровня, в силу примитивности их способа относятся к «несложному», «бытовому» типу мошенничества в сфере компьютерной информации.

---

[167] Харина Е. А. Личность типичного преступника ... С. 56.
[168] Уголовное дело № 1-414/15 // Архив Индустриального районного суда г. Барнаула.
[169] Харина Е. А. Личность типичного преступника ... С. 56.

Необходимо отметить, что развитие профессионального мастерства и модернизация особенностей личности на каждом из уровней не носит статичный характер. На каждом из них существуют свои стадии профессионального роста, поэтапное прохождение которых переводит преступника и осуществляемую им преступную деятельность на следующий качественный уровень, характеризующийся более квалифицированными способами совершения преступлений и более сложными в преодолении имеющейся степени защиты объектами преступных посягательств[170].

При этом видится, что единым принципом для всех стадий профессионального роста компьютерных специалистов, как направляющих свой потенциал на осуществление противоправной деятельности, так и занимающихся его реализацией в правовом поле, является получение новых знаний, совершенствование имеющихся навыков и умений.

Необходимо отметить, что преступления в сфере ИТТ указанными специалистами довольно часто совершаются в группе лиц, при этом, естественно, особую общественную опасность имеют преступления, совершаемые организованными преступными группами (далее ОПГ) и ОПС. Таким преступным формированиям присуща высокая степень конспиративности, устойчивости, распределение ролевых функций, возможность организации совершения преступлений, находясь за пределами Российской Федерации. Преимущественно такие преступные формирования создаются для совершения преступлений, относящихся к «организованному» типу мошенничества.

Как справедливо отмечает А. П. Осипенко, «сложность совершения высокотехнологичных преступлений, обеспечивающих высокую доходность, заставляет преступников объединяться, применяя «разделение труда». При этом «высочайшие скорости передачи данных по компьютерным сетям на любые

[170] Харина Е. А. Личность типичного преступника ... С. 56.

расстояния приводят к тому, что координация преступной деятельности перестает зависеть от удаленности участников криминальных формирований»[171].

Выполнение определенной ролевой функции в таких преступных объединениях, как правило, свидетельствует об обладании такими участниками характерными специфическими личностными особенностями, идентифицирующими их относительно других членов преступных объединений. Поэтому для представления наиболее полной криминалистической характеристики личностей преступников рассматриваемой категории считаем необходимым осветить наиболее характерные черты участников преступных объединений в зависимости от осуществляемой ими ролевой функции.

Лидер. Как известно, довольно часто руководителями хакерских преступных объединений являются выходцы из стран бывшего СССР, преимущественно проживающие за пределами Российской Федерации, на территории Европейских стран или ближнего зарубежья.

Деятельность преступного формирования преимущественно устроена таким образом, что действительными сведениями о личности лидера, в целях недопущения возможности обнаружения и изобличения, либо не располагает никто, либо располагает очень узкий круг особо приближенных лиц, его заместителей. Подобная организация имеет свои положительные для лидера аспекты. Так, довольно часто осужденными за совершение мошенничества в сфере компьютерной информации являются исполнители, занимающие низшие преступные роли в преступном объединении, при этом установить самого руководителя, а также его заместителей, как правило, в ходе предварительного расследования не представляется возможным.

Так, наряду с поэтапным осуждением участников одной из самых известных хакерских группировок Cobalt (Carbanak, Anunak), ее лидер оставался на свободе. Только после проведения совместной соответствующей работы правоохранительных структур нескольких стран, в т. ч. Европейского союза,

[171] Осипенко А. Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие // Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 183–184.

США, Румынии, Белоруссии, Тайваня, лидер сообщества был задержан в Испании[172].

Нередко причиной проблематичности расследования рассматриваемых преступлений и задержания подозреваемых является их территориальная разобщенность и применяемые меры конспирации в общении друг с другом. Так, к примеру, лидер, программисты и «дропы» вышеуказанного преступного сообщества находились в разных странах[173].

Итак, характеризуя личность лидера преступного объединения рассматриваемой категории преступлений, следует отметить, что им, как правило, является специалист высокого уровня, который либо сам является разработчиком соответствующих вредоносных компьютерных программ, либо имеет такого специалиста в числе своих заместителей. Главной психологической особенностью такого руководителя, наряду с обладанием сильными лидерскими качествами, является способность генерировать различные идеи по осуществлению преступной деятельности и проецировать их, с присущим ему азартом, на других членов объединения, заражая их соответствующей идеологией, как, впрочем, это и происходит в случае с компьютерным вирусом.

Главная особенность характера лидера заключается в проецировании своей идеи на других членов объединения, вдохновение на совершение задуманного. При этом лидер требует беспрекословного подчинения своей воле, не приемлет проявления своеволия и идей других членов группы.

Так, гр. К., лидер преступного сообщества Lurk, вовлек в его состав иных лиц, сплотил их и объединил вокруг себя для совершения преступлений, распределив роли каждого участника. Преступному сообществу была присуща строгая дисциплина, безусловное подчинение лидерам структурных подразделений и самому организатору. Тщательное планирование общей деятельности преступного сообщества, а также каждого отдельного преступного

[172] В Испании задержан лидер «самой успешной» хакерской группировки Carbanak. URL: https://www.vedomosti.ru/technology/articles/2018/03/26/754928-ispanii-hakerskoi (дата обращения: 03.02.2023)

[173] Нефедова М. Арестован лидер хакерской группы Cobalt (она же Carbanak). URL: https://xakep.ru/2018/03/27/cobalt-arrests (дата обращения: 04.01.2023)

посягательства, позволяло длительное время совершать систематические преступления, не попадая при этом в поле зрения правоохранительных органов[174].

Лидерами преступного формирования, как правило, становятся специалисты высокого уровня в сфере ИТТ, однако это правило не носит системный характер. Характерны случаи, когда лидером такого объединения становится сильная личность с высокими организаторскими способностями, являющаяся генератором идей, но имеющая пробелы знаний и опыта в одной или нескольких областях противоправной деятельности в сфере компьютерных технологий, например, в области разработки вредоносных компьютерных программ. Для устранения таких пробелов в преступной деятельности, подыскиваются соответствующие специалисты, которые в зависимости от важности и весомости компетенции его направления, как правило, становятся заместителями лидера.

В зависимости от характера порученной деятельности руководитель преступного объединения может иметь одного или нескольких своих **заместителей.** Так, в преступном сообществе Lurk существовали финансовый и технический директор, а также руководители различных структурных подразделений. Одной из функций таких заместителей являлся подбор как соответствующих специалистов, знания и навыки которых необходимы для реализации преступного умысла, так и простых исполнителей, к примеру, подставных лиц, на имена которых оформлялись банковские карты. Согласно переписке из телефонных мессенджеров, в преступном сообществе проводилась работа по проверке большого количества лиц на предмет непогашенных кредитов, привлечения к уголовной, административной ответственности, наличия исполнительных производств. В случае прохождения проверки делалась отметка «Чист. Вариант». Конечно, основной мотивацией вовлечения в совершение преступной деятельности является получение материальной выгоды и обещание ее получения. Так, гр. К., мотивируя группу участников, сообщает им, что они

[174] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1...

должны «пахать», и как выйдут на самоокупаемость, он им поднимет зарплату до 70, а потом еще больше[175].

Одной из психологических особенностей заместителей лидера, является то, что, как правило, они не испытывают дискомфорта в том, что не являются лидерами и даже наоборот, получают удовольствие от возможности наделения материальными благами исполнителей, чувствуя себя своего рода благодетелями. Довольствуются отведенной им ролевой функцией, так как отсутствует возможность проявления своих идей и творчества. За проявление своеволия, как правило, в группе следует наказание.

Отличительной чертой мышления заместителей является несение ответственности за определенное направление деятельности, умение поставить задачи и контролировать их исполнение. В социальном плане такие люди обычно отличаются хозяйственностью и упорядочением, не терпят своеволия и неисполнительности.

Ролевые функции **исполнителей** могут быть различны. Образно исполнителей и осуществляемые ими функции можно представить в виде воинов, исполняющих все поступающие от руководства приказы. Одной из психологических особенностей лиц, осуществляющих исполнительские функции является мнимое осознание собственной значимости и действительной силы в реализации преступной деятельности.

Характерной особенностью таких людей является, в силу различных причин, отсутствие чувства опасности и самосохранения. Так, как правило, именно исполнители являются основными лицами, привлекаемыми к уголовной ответственности за совершение преступлений в сфере компьютерной информации.

В зависимости от направленности и масштабности умысла преступного объединения, в его структуру могут входить исполнители, специализирующиеся на выполнении определенных функций.

---

[175] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 …

Так, в преступном сообществе Lurk были созданы и функционировали следующие структурные подразделения, каждое из которых имело своего руководителя:

– «разработчики» – занимались непосредственным созданием ВПО, нейтрализацией средств защиты компьютерной информации;

– «системные администраторы» – занимались администрированием сетевой инфраструктуры: серверов, сетевых узлов и сторонних сервисов (в т. ч. почтовый сервер и сервер Jabber);

– «тестировщики» – занимались тестированием ВПО, поиском ошибок, сбоев в работе, взаимодействием с «разработчиками» для устранения выявленных недостатков;

– «взломщики» – занимались неправомерным доступом в локальные вычислительные сети объектов преступного посягательства, их анализом, использованием прав привилегированных пользователей;

– «заливщики» – занимались изменением логина и пароля входа в систему ДБО Банк-Клиент, подменой реквизитов получателей денежных средств. Руководителем «заливщиков» являлся сам гр. К.;

– «скриптописатели» – занимались разработкой банковских «скриптов», основное назначение которых заключалось в подмене платежных реквизитов в системе дистанционного банковского обслуживания;

– «обнальщики» – занимались подготовкой промежуточных банковских счетов «фирм-однодневок», поиском лиц («дропов»), которые открывали на свои имена банковские счета, оформляли банковские карты, с помощью которых выводились и обналичивались похищенные денежные средства; занимались снятием денежных средств через банкоматы, переводом на различные электронные платежные системы. «Дропером» может быть как зарегистрированное на подставное лицо или приобретенное юридическое лицо, либо физическое лицо, на имя которого зарегистрирована банковская карта;

– также существовали отдельные участники, выполнявшие следующие функции: оператор «бот-нета» – занимался оценкой качества «бота»

(инфицированного ПК), поиском сведений о наиболее обеспеченных, крупных предприятиях; несколько лиц занималось «эксплойтами», один их участников являлся «чистильщиком». Каждое из структурных подразделений имело своего руководителя[176].

В зависимости от функциональной нагрузки, участники рассматриваемых преступных формирований могут именоваться: «денежные мулы» (занимаются получением денежных средств со счетов в банках, банкоматов), программисты (занимаются созданием ВПО), «верстальщики» и «веб-программисты» (занимаются созданием «фишинговых» страниц и сайтов, поддельных интерфейсов приложений), распространители (занимаются распространением ВПО)[177].

В свою очередь «дропы» могут подразделяться на «разводных» (имеют мнимое представление о характере предоставляемых ими услуг), «неразводных» (привлеченные к осуществлению преступной деятельности открыто, без обмана), «частично разводных». «Дропы» также могут быть «выцепляемыми» (находящимися на связи) и «невыцепляемыми», «ручными» (выполняющие все поступающие указания) и «неручными»[178].

Участники преступного объединения, осуществляющие функции по поиску «дропов», координации их деятельности, называют «дроповоды».

Как уже отмечалось, структура и состав исполнителей преступного объединения могут быть различными. Так, к примеру, в преступную группу братьев П. входили: «трафферы» (занимались распространением вредоносных компьютерных программ), «крипторы» (занимались обновлением (изменением) кода вредоносных программ), «дропы» (занимались обналичиванием денежных средств)[179].

---

[176] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

[177] Стоянов Р. Русскоязычная финансовая киберпреступность: как это работает. URL: https://securelist.ru/russkoyazychnaya-finansovaya-kiberprestupnost-kak-eto-rabotaet/27338 (дата обращения: 04.02.2023).

[178] Дропология. Как вербуют дропов, чему обучают и как используют. URL: https://teletype.in/@osintology/dropologiya.

[179] Братья по кибероружию...

Наряду с традиционной структурой ОПГ, в ряде объединений, специализирующихся на совершении определенного вида преступлений, в зависимости от количества участников и разграничении их функций, существуют свои организационные особенности. Так, к примеру, по мнению специалистов «Лаборатории Касперского» состав типичной организованной киберпреступной группы, может быть следующим: организатор, руководитель «дроп-сервиса», «дроповод», «дропы», «заливщик», распространители («трафогон», спам, загрузки), разработчик, «крипто-сервис», настройщики сервера (админ, настройщик)[180].

В свою очередь, по оценкам специалистов «Лаборатории Касперского», деятельность, направленная на совершение преступлений в сфере компьютерной информации, в зависимости от количества участвующих в ней лиц, может быть условно реализована в следующих формах:

– партнерские программы – схема, в результате которой организаторы, предоставляют «партнерам» практически весь необходимый набор инструментов для осуществления как можно большего распространения ВПО, за что получают часть полученного преступным путем дохода;

– одиночные преступники, мелкие и средние группы. В данном случае, преступник или преступники самостоятельно организуют совершение преступления, при этом, как правило, не обладая высокими познаниями в сфере компьютерных технологий, необходимые для осуществления преступления инструменты, вынуждены приобретать на «черном» рынке;

– крупные организованные группировки – как правило, численность таких групп насчитывает более десяти человек и отличается масштабностью деятельности и организации по совершению преступлений. Такими группировками в частности являются Carberp, Carbanak, Lurk[181].

[180] Стоянов Р. Охота на Lurk …
[181] Стоянов Р. Русскоязычная финансовая киберпреступность ...

В целом, резюмируя вышесказанное, в качестве причин низкой раскрываемости «организованного» мошенничества, опрошенные респонденты отметили высокий уровень организации преступления, в результате чего оставление незначительной следовой картины (56 %); отсутствие у «низовых» исполнителей и подставных лиц информации об организаторах преступного объединения и/или других его членах в силу соблюдения конспиративности, использования в процессе общения друг с другом технических средств связи, исключающих или затрудняющих идентификацию (34,1 %); использование в преступной деятельности высокотехнологичных компьютерных устройств (35,6 %); использование в преступной деятельности высококачественного ВПО (41 %) (Приложение 1).

В рамках данного исследования нельзя не упомянуть о проведенном анализе социально-демографических признаков типичных преступников в сфере компьютерной информации.

Так, согласно сведениям, размещенным на официальном сайте Судебного департамента при Верховном суде РФ [182] , преимущественно лицами, осужденными за совершение рассматриваемой категории преступлений, являются мужчины в возрасте 18–35 лет, имеющие высшее или среднее профессиональное образование.

Обращаясь к рассмотрению вопроса о лицах, являющихся типичными потерпевшими по делам о совершении преступлений в сфере компьютерной информации необходимо отметить, что ими являются как физические, так и юридические лица всех форм собственности.

Отличительной особенностью совершения данного вида преступлений является отсутствие непосредственного контакта между преступником и потерпевшим. Как отмечалось ранее, специфической чертой личности преступника является его не нацеленность на личностные ориентиры и качества

[182] Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL: https:// http://www.cdep.ru (дата обращения: 19.02.2023).

потерпевшего. При этом преступник, как правило, с жертвой не знаком и его не интересует его личностная характеристика, определяющим моментом является обладание соответствующим имуществом, организация доступа к которому и является главной задачей преступника.

К примеру, при совершении хищений посредством установления контроля за работой системы ДБО, единственным критерием выбора жертвы является наличие на его счетах денежных средств.

В случае с ОПС Lurk, нацеленность их преступной деятельности заключалась, как правило, в хищении денежных средств крупных финансовых организаций. В частности были атакованы большинство крупных российских банков, в числе которых четыре крупнейших. Для создания новых перевалочных серверов, через которые идет трафик серверам злоумышленников, а также для заражения большого числа компьютеров, жертвами данного сообщества становились IT-организации в сфере «телеком», средства массовой информации и новостные «агрегаторы»[183].

Итак, первым существенным признаком жертв преступлений в ИТТ является обладание соответствующими материальными благами, доступ к которым возможно осуществить посредством преодоления соответствующих средств программно-технической защиты.

Второй характерной чертой является обладание определенной степенью самонадеянности и пренебрежение соблюдением мер безопасности, позволяющим повысить степень защищенности компьютерной информации, а равно и отсутствие знаний о необходимости применения таких мер безопасности.

Д. С. Шурыгина, В. В. Поляков в этой связи отмечают, что легкомысленное, небрежное или халатное отношение к информационной безопасности со стороны потерпевших способствует совершению преступлений,

[183]Шульмин А., Прохоренко М. Указ. соч.

выступая в качестве причины и благоприятных условий, при которых оно становится возможным[184].

Лицами, потенциально обладающими наибольшей степенью опасности быть подверженными таким преступлениям, являются активные пользователи сети Интернет, в т. ч. совершающие с его использованием различные покупки и производящие различные платежные операции, пользователи систем ДБО и т. д.

Еще одной особенностью жертв компьютерных преступлений, как правило, имеющей отношение к категории юридических лиц, является обладание соответствующими программно-техническими средствами компьютерной защиты с некоторыми уязвимостями, позволяющими преступникам получить реальную возможность совершения преступления, а также уделение недостаточного внимания соблюдению имеющимся мерам противодействия противоправной деятельности.

2.4. Типичные следы мошенничества в сфере компьютерной информации

Как уже отмечалось, одним из основных элементов криминалистической характеристики мошенничества в сфере компьютерной информации, являются знания о способе его совершения, которые определяют и/или позволяют скоординировать дальнейшее направление расследования преступления. В свою очередь, обладание информацией о способе совершения преступления взаимообусловлено между собой с другим важным элементом криминалистической характеристики преступления – следами противоправной деятельности.

В целом, след – это отображение характерных свойств и качеств одного объекта, спроецированных на другом объекте в результате какого-либо взаимодействия. Как известно, следы преступной деятельности в зависимости от их специфики могут содержать информацию не только о форме объекта

[184] Шурыгина Д. С., Поляков В. В. Особенности криминалистической характеристики потерпевших по компьютерным преступлениям // Проблемы правовой и технической защиты информации. 2018. № 6. С. 162–166.

взаимодействия, но и о части его макромира, содержащего сведения о его характерных свойствах, подготовке, способе совершения и сокрытия преступления, используемых орудиях и средствах, мотивах, поводах и обстановке, характеристике и численности задействованных в преступлении лиц и т. д.

В этой связи В. Б. Вехов отмечает: «следовоспринимающий объект несет информацию не только об отражающем объекте. Он является также носителем информации о механизме следообразования, т. е. действиях с отражаемым объектом или самого отражаемого объекта. В данном случае отражаемый объект является средством передачи информации о способе, а через него и о субъекте действия»[185].

Итак, проведенное исследование позволило выделить следующие типичные следы рассматриваемой категории преступлений.

I. Материальные следы.

1. Следы-предметы.

а) различного рода документы:

– банковские документы: банкноты Банка России; договоры, справки об открытии счетов и вкладов в кредитных организациях; заявления о предоставлении банковских услуг; выписки по счетам; договоры кредитования, договоры банковского обслуживания и оказания услуг, в т. ч. договоры на обслуживание клиентов банка с использованием системы Банк-Клиент; выписки по операциям на банковских счетах; карточки с образцами подписей и оттисков печатей; документы о переводе денежных средств; платежные поручения, распоряжения, извещения по счетам и вкладам; квитанции, кассовые чеки; копии инкассационных чеков; чеки о снятии денежных средств; приходно-кассовые ордера; заявки на изготовление платежных карт; анкеты держателей банковских карт, сведения об операциях, произведенных по счетам, документы по операциям с платежными картами, выписки из мониторинга платежей через терминалы и т. д.;

– иные документы: документы о государственной регистрации юридического лица и индивидуального предпринимателя; учредительные документы; выписки из ЕГРИП, ЕГРЮЛ; документы, удостоверяющие личность;

[185] Цифровая криминалистика ... С. 96.

трудовые договоры; должностные инструкции; договоры возмездного оказания услуг по обслуживанию платежных терминалов; паспорта терминалов по приему платежей; договоры аренды транспортных средств, движимого, недвижимого имущества; выписки мониторинга терминала из раздела «проблемные платежи», выписки инкассации терминалов, детализации соединений абонентских номеров, проездные билеты на железнодорожный транспорт, авиабилеты, посадочные талоны, билеты Банка России со специальными приспособлениями и т. д.;

б) различного рода предметы: компьютерные устройства, технические средства (мобильные телефоны, смартфоны, планшеты, ноутбуки, нетбуки, персональные компьютеры, оргтехника, жесткие диски, флеш-карты, sim-карты, видеорегистраторы, CD и DVD диски, Wi-Fi-роутеры, серверы, различные закладные устройства, устройства для уничтожения, дистанционного съема компьютерной информации, фото- и видеокамеры, поглотители частотных сигналов и т. д.), банковские карты, различного рода устройства, в т. ч. предназначенные для взлома банкоматов и т. д.

Так, при расследовании уголовного дела в ходе обыска только у одного из обвиняемых было изъято 2 ноутбука, 3 системных блока, 7 мобильных телефонов, более 500 SIM-карт, более тридцати банковских карт, 4 флеш-модема, адаптер, 2 Wi-Fi-роутера, 2 флеш-карты, 6 записных книжек, 4 тетради с рукописным текстом, незаполненные бланки договоров об оказании услуг связи, три мобильных платежных терминала, папка с документами, печать юридического лица[186].

2. Следы-отображения: следы пальцев рук; следы обуви; микрочастицы, запаховые следы, оставленные от взаимодействия с компьютерными устройствами, документами и другими предметами, следы орудий взлома, следы транспортных средств и т. д.

II. Идеальные следы.

Типичными идеальными следами мошенничества в сфере компьютерной информации и сопутствующих преступлений являются показания

[186] Приговор Октябрьского районного суда г. Барнаула от 20 апреля 2017 г. № 1-18/2017 ...

подозреваемого, обвиняемого, свидетелей, экспертов и специалистов. Свидетелями в зависимости от ситуации могут являться следующие лица: сотрудники кредитных организаций, кассиры банков, лица, на имена которых оформлены расчетные счета, банковские карты, открыты электронные кошельки, собственники арендуемых квартир и автомобилей, сотрудники отделов безопасности, сотрудники гостиниц. При совершении преступлений с использованием служебного положения, свидетелями могут быть также сослуживцы, руководители подозреваемых, обвиняемых.

Особенность исследуемой разновидности преступлений, совершенных с использованием различных компьютерных устройств, алгоритм действия которых недоступен обыденному сознанию, неминуемым образом отразился на специфичности общей следовой картины преступной деятельности.

Учитывая специфику способов рассматриваемых преступлений, особую роль в общем объеме следов имеют следы, образованные в результате взаимодействия с компьютерной информацией.

Данную группу следов невозможно безоговорочно отнести как к категории материальных, так и идеальных следов, так как они образуют свою отдельную, характерную категорию следов. В связи со стремительной компьютеризацией и цифровизацией всех сфер жизни общества, в настоящее время наибольшую актуальность приобретает потребность в развитии соответствующего раздела криминалистической техники. Пока же в научном сообществе, несмотря на существенные продвижения в данном вопросе, отсутствует единообразное понимание относительно наименования данной категории следов преступной деятельности.

Так, В. А. Мещеряков предлагает такие следы именовать «виртуальными следами». Ими он предлагает определять следы, сохраняющиеся «в памяти технических устройств, в электромагнитном поле, на носителях машиночитаемой

информации, занимающей промежуточное положение между материальными и идеальными»[187].

В. А. Милашев, рассматривая данную категорию следов, сформулировал понятие «бинарные следы», под которыми понимает «результаты логических и математических операций с двоичным кодом»[188]. Относительно данного понятия можно отметить, что не соответствует состоянию современного научно-технического прогресса, так как вместо двоичного кода уже давно используется шестнадцатеричный и более (32, 64 и 86) разрядные коды.

В. В. Борисов ввел термин «информационный след», под которым он понимает «некоторую информационную запись, сделанную на компьютерной технике подозреваемых в преступлении лиц с помощью специального программного средства и произведенную субъектом уголовно-процессуальной системы»[189]. Считаем, что данное автором определение является неполным, осколочным, поскольку отражает наличие соответствующей информационной записи только на компьютерной технике подозреваемых, без учета наличия таких следов на компьютерных устройствах потерпевшего, свидетелей и т. д.

Несколько иной позиции придерживается В. Б. Вехов, по мнению которого рассматриваемую группу следов следует именовать «цифровыми», «являющимися материальными невидимыми следами», представляющими из себя «любую криминалистически значимую компьютерную информацию, т. е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[190]. Полагаем, что понятием, наиболее полно отображающим и проявляющим суть рассматриваемых следов, является понятие «цифровые следы».

Несмотря на отсутствие единообразного понимания в вопросе формирования соответствующего определения следов данной категории, одной из их характерных особенностей является наличие неразрывной связи с объектами

---

[187] Мещеряков В. А. Указ. соч. С. 112.
[188] Милашев В. А. Указ. соч. С. 17.
[189] Борисов В. В. Указ. соч. С. 164.
[190] Цифровая криминалистика ... С. 97.

материального мира (компьютерами, планшетами, мобильными телефонами, смартфонами и другими компьютерными устройствами), которые в свою очередь могут являться следами-предметами.

В. О. Давыдовым, В. Д. Малахвей выделяются следующие стадии следообразования таких следов: стадия физического проявления свойств следообразующих объектов, стадия преобразования исходной физической формы проявления следообразующего объекта в цифровую форму, стадия предварительной обработки, передачи и хранения полученной информации[191].

Итак, наиболее полный перечень следообразующих и следовоспринимающих объектов в механизме образования цифровых следов приведен В. Б. Веховым: электромагнитный сигнал; файл; сетевой адрес (например, IP-адрес (Internet Protocol – протокол передачи данных в сети Интернет), MAC – адрес (Media Accees Control – управление доступом к среде), IMEI (International Mobile Equipment Identity – международный идентификатор мобильного оборудования); доменное имя; электронное сообщение (SMS – сообщение (Short Message Service – службы коротких сообщений), MMS – сообщение (Multimedia Messaging Service – служба передачи мультимедийных сообщений), сообщения электронной почты и др.; электронные денежные средства; цифровая валюта; электронная подпись; электронный документ; электронный журнал; база данных; программа для ЭВМ; вредоносная компьютерная программа; сайт; страница сайта[192].

Таким образом, цифровые следы, оставленные в результате взаимодействия с указанными следообразующими и следовоспринимающими объектами, обладающие оперативно значимой информацией и будут являться одной из разновидностей следов преступной деятельности рассматриваемой категории и

---

[191] Давыдов В. О. О некоторых аспектах практики реализации криминалистического предупреждения преступлений экстремистской направленности в информационно-телекоммуникационном пространстве // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности : сб. науч. ст. по мат-лам междунар. науч.-практ. конф. (Москва, 26 мая 2023 г.) / Академия управления МВД России. Ч. 1. М., 2023. С. 198.

[192] Цифровая криминалистика ... С. 97–103.

могут быть использованы в процессе расследования и доказывания по уголовному делу.

В ходе совершения мошенничества в сфере компьютерной информации с использованием ВПО могут быть оставлены следующие разновидности цифровых следов:

– файлы (исполняемые и различные скрипы, файлы динамически загружаемых библиотек, лог-файлы, архивы, файлы электронной почты);

– программы, предназначенные для удаленного или локального управления системой, для удаления системных данных, а также для кражи пользовательских данных и сбора сведений о системе;

– записи журналов системных событий и событий информационной безопасности;

– список запущенных процессов и служб;

– список действующих и недавно установленных сетевых соединений;

– информация о событиях информационной безопасности антивирусного программного обеспечения, экрана SIEM-систем;

– список локальных и доменных пользователей;

– ключи реестра автозагрузки программ;

– данные планировщика заданий;

– артефакты и метаданные запуска программ (Prefetch, Amcache, Shimcache)[193].

В результате изучения судебно-следственной практики наиболее типичными цифровыми следами в результате совершения исследуемых преступлений являются следующие: записи с камер видеонаблюдения; переписка посредством сотовой, мобильной связи, различных мессенджеров и приложений, электронной почты, социальных сетей, блогов; сведения о номерах телефонов, адресах сайтов, IP-адресах, серверах, сведения о соединениях и телефонных переговорах, результаты прослушивания телефонных переговоров; сведения о

[193]Бердникова О. П. Особенности расследования мошенничества в сфере компьютерной информации : учеб. пособие. Екатеринбург, 2021. С. 17–18.

контактах и другая информация, содержащаяся в памяти мобильных телефонов, смартфонов; сведения, содержащиеся на сайтах, в социальных сетях, блогах, форумах; сведения о персональных данных, учетные записи, имена пользователей, логины, пароли; электронные документы, файлы, содержащие различного рода сведения, касающиеся подготовки, совершения преступления и сокрытия его следов; фото- и видео файлы; сведения, содержащиеся в памяти компьютерных устройств; следы создания, использования, приобретения различных компьютерных и вредоносных программ; сведения об открытии, закрытии банковских и расчетных счетов, о движении денежных средств по счетам и т. д.

Так, при расследовании уголовного дела № 1-414/15 по факту совершения серии хищений денежных средств из платежных терминалов в Барнауле сотрудники правоохранительных органов, после просмотра записей с камер видеонаблюдения, установили, что к совершению преступления причастны лица неславянской национальности. В ходе выезда в г. Новосибирск (место предполагаемого следования фигурантов), были просмотрены записи видеокамер, установленных в аэропорту «Толмачево». В результате просмотра были установлены лица, схожие с лицами, совершившими преступление, при проверке сведений о прохождении ими регистрации были установлены их анкетные данные. Причастность выявленных лиц также подтверждалась тем обстоятельством, что похищенные денежные средства с одного из терминалов были переведены на карту одного из преступников. Вещественными доказательствами по делу являлись изъятые семь сотовых телефонов и 25 банковских карт[194].

Переоценить значимость цифровых следов для процесса расследования невозможно, так, отличительной чертой значительной части цифровых следов является обладание отображением структурированного алгоритма взаимодействия компьютерной информации (в частности ВПО), распознание сущности которого возможно с помощью специальных познаний и

[194] Уголовное дело № 1-414/15 // Архив Индустриального районного суда г. Барнаула Алтайского края.

соответствующих программных средств. Полученные знания способны привнести в процесс расследования по уголовному делу значительный объем криминалистически важной информации, способствующей проявлению более полной картины совершенного преступления, а в ряде случаев в корне изменить ход расследования.

Совершенно верно утверждение О. В. Флерова относительно значимости данного вида следов – «цифровой след фактически выступает «отпечатком жизни и личности человека»: в нем явно видны интенции человека, его интересы, потребности, социальный и интеллектуальный уровень развития, уровень культуры человека; коммуникация человека в Интернете также позволяет судить о его психологических свойствах»[195].

Принципиально согласны и с убеждением А. Б. Смушкина, что при совершении компьютерных преступлений «могут использоваться программы различного уровня сложности: «стандартные» – которые составлены максимально просто и которые легко найти в сети Интернет или нелегальной продаже; «приспособленные» программы – переделанные самим злоумышленником; самостоятельно написанные злоумышленником программы. В зависимости от сложности и распространенности программ они могут оставить в памяти устройства различные виртуальные следы, позволяющие идентифицировать программу, способ взлома и сокрытия. Обладая подобной информацией, можно сделать вывод о профессиональном уровне злоумышленника»[196].

Приведенный в предыдущем параграфе перечень типичных способов мошенничества в сфере компьютерной информации, указывает на то, что одним из основных его орудий является ВПО. Анализ судебно-следственной практики, а также мнений экспертов в сфере информационных технологий, позволили прийти к выводу о наличии специфических особенностей в характере оставляемых цифровых следов в зависимости от квалификации лица (лиц), явившегося автором

[195] Флеров О. В. Цифровой след человека в Интернете: основные гуманитарные подходы // Образовательные ресурсы и технологии. 2018. № 4 (25). С. 80.

[196] Смушкин А. Б. Виртуальные следы в криминалистике // Законность. 2012. № 8 (934). С. 45.

использованного ВПО, а также организовавшего и совершившего преступление. Знания таких особенностей позволяют получить ориентирующие сведения относительно личности преступника, способе и средствах совершения преступления, что благотворным образом отразится на ходе, качестве и сроках расследования в целом.

Итак, приведем характерные особенности следовой картины преступной деятельности, оставляемой преступниками, имеющими различного уровня квалификацию в сфере компьютерных технологий.

Особенность следовой картины преступной **деятельности высококвалифицированных специалистов в сфере ИТТ** заключается в том, что в результате использования имеющихся у такого уровня преступников специальных знаний и навыков в области компьютерных технологий, созданные и внедренные ими высококвалифицированные компьютерные программы работают довольно скрытно, изощренно и лояльно, в связи с чем оставляют в компьютерных устройствах потерпевших незначительные следы и повреждения. Специфика таких программ заключается в нахождении узких, уязвимых мест системы защиты и получении доступа к информационной системе потерпевшего (как правило, кредитной организации), при этом работа уже внедренной компьютерной программы существенным образом не отражается на работоспособности всей компьютерной системы организации. Кроме того, в случае возникновения угрозы своего обнаружения, компьютерная программа способна к самоизъятию, самоуничтожению и нейтрализации следов своего присутствия, что существенным образом затрудняет ход расследования или вообще делает установление истины по делу практически невозможным. Немаловажную роль в сокрытии следов преступления имеет использование такими преступниками высококачественных специальных компьютерных устройств, как правило, дорогостоящих, что также может указывать на серьезный уровень организации преступления.

Примером действия такого ВПО являются разработанное и модифицированное ОПС Lurk ВПО, которое условно обозначалось как «HBS»,

клиентские приложения (боты) которого классифицированы АО «Лаборатория Касперского» как ВПО Trojan-Spy.Win32.Lurk и Trojan-Spy.Win64.Lurk, а также с условным обозначением и наименованием Angler EK, Angler, Loader, «Лоадер XXX», Exploit Kit, используемые для эксплуатации уязвимостей в другом ПО, классифицированные АО «Лаборатория Касперского» как ВПО семейства Exploit. Используемое ВПО обладало следующим функционалом: перезагружать и выключать компьютер; собирать логины и пароли; подключаться в режиме наблюдения, управления, записи всего, что происходит на рабочем столе; перехватывать все, что набирает пользователь; удаляться с компьютера (при направлении сервисной команды uninstall_bot экстренно стирались следы пребывания на компьютере, программа самоудаляла себя и все свои файлы); «убивать» компьютер пользователя (при направлении сервисной команды kill_pc бот сначала удалял себя, потом «убивал» файловую систему на диске, компьютер перезагружался и больше не включался. Так, созданное ВПО Lurk, проникнув в компьютерную сеть юридического лица, более месяца неоднократно модифицировалось участниками ОПС, чтобы работа ВПО не обнаруживалась средствами антивирусной защиты. Кроме того, обладало модульным строением и широкой функциональностью, что позволяло длительное время изучать компьютеры потенциальных жертв, исследовать действия определенных пользователей, получать информацию, хранящуюся на их компьютерах и при этом оставаться незамеченным[197].

В техническом плане вредоносная программа была необычной: в отличие от большинства других, она не оставляла на жестком диске атакованной системы никаких следов, а работала только в оперативной памяти машины[198]. Если по результатам анализа компьютер признан непригодным для атаки ВПО, завершала свою работу и самоудалялась[199].

---

[197] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1...
[198] Стоянов Р. Охота на Lurk …
[199] Шульмин А., Прохоренко М. Указ. соч.

Таким образом, реализованные в данной компьютерной программе технические решения позволяли длительное время ОПС безнаказанно заниматься совершением хищений денежных средств.

Следовая картина преступной **деятельности опытных компьютерных** преступников отличается от предыдущего случая наличием больших повреждений и разрушений системы защиты потерпевшего. Данный факт объясняется отсутствием у данной категории преступников достаточных знаний для создания высокопрофессиональной компьютерной программы, работа которой была бы неуловима. Такие программы вбрасывают больший объем разрушительной информации, который и приводит к более разрушительным последствиям. При этом информационное поле компьютерной системы потерпевшего (как правило, кредитной организации) начинает ощущать некорректную работу системы защиты, что может выражаться в сбоях и заторможенности работы компьютерных систем и насторожить пользователей о возможных проблемах системы защиты информационной безопасности.

Следовая картина преступной **деятельности компьютерного специалиста среднего уровня** имеет еще более явный разрушительный характер. Специфика действия внедренных вредоносных компьютерных программ специалистов такого уровня заключается во взломе защитной системы потерпевшего и подменой ее на свою. При загрузке такая программа подкачивает на себя защитную программу потерпевшего и начинает работать по ее принципу. Распознать возможность действия такой программы довольно не трудно, так как работа компьютерных средств, пораженных такой программой, может приостанавливаться, блокироваться.

Следы преступной деятельности «**случайных» или «бытовых» компьютерных преступников носят еще более** распознаваемый, подчас примитивный характер. Довольно часто преступления, совершаемые преступниками такого уровня, характеризуются преимущественно совершением механических манипуляций и носят явный обозримый характер. Так, к примеру, совершаются преступления, связанные со вводом информации по изменению

баланса своего или подконтрольного преступнику счета, преступления, совершенные посредством задержки шторки купюроприемника банкомата, посредством механического воздействия на корпус банкомата и т. д.

Так, согласно материалам уголовного дела, гр. Л., имея умысел на хищение денежных средств из банкоматов, заранее приобрел у неустановленного лица инструкцию по взлому банкомата, программное обеспечение для несанкционированного управления банкоматом, а так же коды доступа для автоматической выгрузки денежных средств из банкомата. Реализуя свой преступный умысел гр. Л. приобрел аккумуляторный шуруповерт, подыскал подходящий по техническим характеристикам банкомат, после чего в ночное время проделал в корпусе банкомата два отверстия, извлек необходимый провод с разъемом, подключил имевшийся при себе удлинитель с клавиатурой и запустил с флеш-накопителя имевшуюся вредоносную программу. Получив информацию о количестве имеющихся в банкомате денежных средств, ввел необходимый код, после чего банкомат начал автоматическую выдачу денежных средств, всего на общую сумму более 4 млн руб. В результате совершения действий, заключавшихся в неправомерном доступе к охраняемой законом компьютерной информации, вмешательстве в функционирование средств хранения, обработки компьютерной информации, модификации компьютерной информации и нейтрализации средств защиты компьютерной информации, содержащейся на накопителе (жестких магнитных дисках) системного блока банкоматов с использованием вредоносных компьютерных программ, гр. Л. был признан виновным в совершении преступлений, предусмотренных ч. 3 ст. 159.6, ч. 2 ст. 272, ч. 2 ст. 273, ч.1 ст. 30, ч. 3 ст. 159.6 УК РФ[200].

Как уже отмечалось, особое место в перечне средств совершения рассматриваемой категории преступлений занимает ВПО, посредством которого зачастую и совершаются компьютерные преступления. На сегодняшний день однозначно определить круг имеющихся вредоносных компьютерных программ

[200] Приговор Октябрьского районного суда г. Владимира от 04 июня 2019 г. № 1-95/2019. URL: https://sudact.ru/regular/doc/v59eyhN7lzJq (дата обращения: 25.07.2022).

не представляется возможным, так как ежедневно в мире создаются новые вредоносные программы, а уже имеющиеся модернизируются и совершенствуются.

Как правило, распространение ВПО осуществляется посредством рассылки зараженных сообщений или ссылок на поддельные сайты или приложения. Так, по одному из эпизодов дела Lurk, согласно заключению компании GroupIB, заражение произошло с сайта «Ведомости.ру»[201].

Также, с целью распространения ВПО и сбора информации могут проводится массированные атаки. К примеру, таким атакам подвергались сайты крупнейших российских информационных агентств, таких как «РИА Новости», Gazeta.ru, через которые, используя уязвимость в системе обмена рекламными баннерами, распространялись вредоносные программы, основной функцией которых был сбор информации об атакованном компьютере, передача ее на сервер преступников[202].

Так, по одному из уголовных дел, согласно экспертным заключениям, на изъятых оптических дисках обнаружено большое количество вредоносных приложений, в т. ч.: приложения 8504.apk, 5444.apk, 8503.apk, com.tyjtry.wetpihkmre-2apk, которые являются вредоносными. К примеру, приложение 8504.apk соединяется с удаленными серверами pay.fastmopay.com, api.kfkx.net, rs.kfkx.net, rs.2010010.com, rs.wo-da.com, rs.zhiqupk.comи подчиняется их командам. Злоумышленники способны управлять устройством, отправлять SMS-сообщения и перехватывать входящие сообщения, скачивать персональные данные со смартфона[203].

По делу Lurk, согласно заключениям экспертов, на изъятых компьютерах обнаружены:

– вредоносное программное обеспечение, в т. ч. Trojan-Spy. Win32.Lurk.voh; RemoteAdmin.Win32.Agent.dx; Win32/TrojanDownloader.Sougle.A; Win32.Dropper. mc.,Trojan-Spy.Win32.Lurk.vny;

---

[201] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...
[202] Стоянов Р. Охота на Lurk …
[203] Приговор Октябрьского районного суда г. Барнаула от 20 апреля 2017 г. № 1-18/2017 ...

– переписка в системе Jabber и посредством электронной почты;

– рабочие снимки экрана в процессе тестирования программного обеспечения;

– журналы работы отладчика в процессе работы программного обеспечения, детектируемого как Lurk;

– реквизиты банковских счетов, различные платежные документы;

– виртуальные машины, используемые для тестирования ВПО и совершения хищений путем подмены реквизитов;

– наборы утилит, в частности программа для подмены реквизитов платежных документов Banktools[204].

По заключению специалистов АО «Лаборатория Касперского», при совершении преступлений фигуранты стремятся к оставлению как можно меньшего количества следов, в частности в сокращении времени использования вредоносной инфраструктуры. Так, некоторые из них «жили» всего несколько часов, в течение проведения той фазы операции, для которой они предназначались. Еще одной попыткой сокрытия следов преступной деятельности является, к примеру, получение доступа из инфраструктуры скомпрометированного объекта к другим организациям[205].

Уровень сложности используемых вредоносных программ различен и варьируется от довольно простых, написанных начинающими программистами, до достаточно сложных, плохо распознаваемых, постоянно совершенствующихся программ, авторами которых являются специалисты высокого уровня компьютерной грамотности, гении своего дела.

Создание и функционирование высокоорганизованных преступных объединений, использующих ВПО, созданное специалистами высокого уровня занимает не высокий процент от числа существующих групп и лиц, занимающихся совершением преступлений в сфере компьютерной информации. Большинством из них являются преступники и группы, имеющие более простую

[204] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

[205] Киберугрозы для АСУ и промышленных предприятий в 2022 году. URL: https://securelist.ru/threats-to-ics-and-industrial-enterprises-in-2022/103980 (дата обращения: 08.11.2022).

организацию и использующие в преступной деятельности программные продукты низкого или среднего качества.

Одним из примеров вредоносной высококачественной программы является банковский троянец Emotet, которая считается «королем» ВПО и является одной из самых разрушительных, сложных и опасных троянских программ. Нанесенный ею ущерб исчисляется миллионами долларов. Программа способна без распознавания обманывать базовые антивирусы, она полиморфна, т. е. при каждом обращении немного меняет свой код[206].

Так, бэкдор Carbanak (основанный на коде Carberp), позволил одноименной преступной группировке совершить атаки на более 100 банков и совершить хищения более чем на 1 млрд руб.[207]

Примером ВПО невысокого качества, специализирующегося на совершении хищений из банкоматов кредитных организаций, является программный комплекс – Cutlet Maker, состоящий из трех программ: Cutlet Maker – обеспечивает выдачу денежных средств (по одной или по 50 купюр), Stimulator – для проверки количества банкнот в диспенсере и их номинала и c0decalc – программа для генерации кодов, используемых Cutlet Maker. В конце 2017 г. данная программа была выложена неизвестными лицами на открытые специализированные форумы сети Интернет и распространялась в Телеграм-чатах в полном объеме, что указывает на ее эффективность ниже ожидаемого авторами программы уровня[208].

Так же, к примеру, в случае совершения мошенничества в сфере компьютерной информации посредством воздействия вредоносных компьютерных программ на компьютерные устройства клиентов кредитных организаций (речь идет о хищении денежных средств через систему «Мобильный банк») используются одни из многочисленных довольно простых типов ВПО.

---

[206] Что такое Emolet и как от него защититься. URL: https://www.kaspersky.ru/resource-center/threats/emotet (дата обращения: 12.12.2022).

[207] Большое банковское ограбление: APT-кампания Carbanak. URL: https://securelist.ru/bolshoe-bankovskoe-ograblenie-apt-kampaniya-carbanak/25106 (дата обращения: 04.01.2023).

[208] Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России …

Программы такого типа широко представлены на пространствах «теневого» Интернета, приобретение которых не вызывает серьезных трудностей.

В целом полученные в процессе расследования преступления знания, относительно типа и сложности использованного программного обеспечения, содержат в себе информацию об уровне квалификации его создателя, а характерные особенности таких программ могут указывать как на группу таких лиц, так и на конкретного лица.

Как и в случае совершения преимущественного большинства преступлений, уже на стадии его подготовки преступники осуществляют меры по сокрытию следов преступной деятельности. Наряду с общераспространенными способами сокрытия следов преступной деятельности, одним из основных способов сокрытия следов при совершении компьютерных преступлений является выбор и использование в совершении преступления ВПО соответствующего профессионального уровня, где в зависимости от повышения ее классности повышается степень нераспознаваемости и неопределяемости. Так, ряд компьютерных программ обладают способностью самоуничтожения следов вмешательства после достижения целей их использования. Дополнительными мерами сокрытия следов преступной деятельности рассматриваемой категории преступлений является использование серверов, расположенных на территории других государств, VPN, TOR, Proxy, использование чужой электронной подписи, чужих логин и паролей, использование компьютерных средств посторонних лиц и т. д.

В целом, обладая сведениями о способе совершения преступления, характере оставленной следовой картины, уровне сложности используемого ВПО, лица, занимающиеся раскрытием, расследованием преступления могут выдвигать версии относительно того, к какому типу мошенничества в сфере компьютерной информации («организованному или «несложному», «бытовому») относится данное преступление, а также о том, к какой категории преступников относительно обладания специальными познаниями (высококвалифицированным, опытным, специалистам среднего уровня или «бытовым», «случайным»)

относится лицо, совершившее преступление. Обладание такими сведениями позволит получить ориентирующую информацию относительно имеющегося объема познаний в сфере ИТТ, образа мышления, психологических особенностях потенциального преступника и, с учетом имеющихся оперативно-справочных учетов, способствовать выдвижению версий о причастности к совершению преступления конкретного человека или преступного формирования.

Глава 3. ОСОБЕННОСТИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

3.1. Особенности доследственной проверки и возбуждения уголовного дела

Приступая к рассмотрению вопросов, непосредственно связанных с уголовно-правовой реакцией государства на преступные проявления, необходимо отметить, что доследственная проверка и возбуждение уголовного дела являются принципиально важными этапами всего процесса расследования. Именно на данном этапе уполномоченным лицом принимается решение о дальнейшей судьбе имеющейся информации о готовящемся, совершаемом или совершенном преступлении.

Как уже отмечалось, анализ судебно-следственной практики указал на наличие у правоприменителей трудностей определения места совершения исследуемого преступления, и, как следствие, определения места проведения расследования. В этой связи, в параграфе 2.2. настоящего исследования приведены некоторые коррективы, внесенные в решение данного вопроса разъяснениями, данными постановлением Пленума Верховного Суда РФ № 37[209] и постановлением Пленума Верховного Суда РФ № 48[210].

Однако, учитывая то обстоятельство, что преступление, как правило, совершается удаленно и место совершения преступником действий, охватываемых объективной стороной преступления, неизвестно, на практике возникают трудности определения подразделения органа внутренних дел, в котором будет производиться предварительное расследование, что естественным образом отражается на сохранности следовой картины преступной деятельности.

---

[209] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 …

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

Проведенное анкетирование подтвердило актуальность данного вопроса. Так, 55,2 % респондентов указали несвоевременное сообщение о преступлении в результате чего частичная или полная утрата цифровых следов, а также сложности в установлении места совершения преступления (57,6 %) в качестве одних из трудностей раскрытия исследуемых деяний (Приложение 1).

В данном случае следует руководствоваться приказом МВД России «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» от 03.04.2018 № 196, предписывающим при поступлении сообщения о преступлении, предусмотренном ст. 159.6 УК РФ, незамедлительно принимать исчерпывающие меры к раскрытию преступлений и установлению лиц, их совершивших; вопрос о возбуждении уголовного дела принимать в ОВД РФ, в которое поступило сообщение о преступлении[211].

Итак, в соответствии с ч. 1 ст. 140 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) поводами для возбуждения уголовного дела являются: заявление о преступлении, явка с повинной, сообщение о совершенном или готовящемся преступлении, полученное из иных источников, постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании[212].

В ходе проведенного исследования, в качестве наиболее распространенных источников получения информации о мошенничестве в сфере компьютерной информации, 91 % респондентов отметили потерпевших физических лиц, 46,6 % указали потерпевших юридических лиц, 30,5 % отметили сведения, полученные в результате проведения ОРМ, 23,8 % – сведения, полученные в результате расследования других преступлений, 15,6 % – в результате инициативного выявления рассматриваемой группы преступлений (Приложение 1).

---

[211] О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений : приказ МВД России от 03.04.2018 № 196 // Доступ из справ.-правовой системы «КонсультантПлюс».

[212] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ : ред. от 25.12.2023 // Доступ из справ.-правовой системы «КонсультантПлюс».

Как видим, в преимущественном большинстве случаев поводами для возбуждения уголовных дел рассматриваемой категории явились заявления потерпевших – физических лиц. Гораздо меньшее количество заявлений, поступающих от уполномоченных представителей юридических лиц, легко объясняется спецификой способов совершения преступлений. Так, к примеру, работа одного ВПО может одновременно совершать хищения у большого количества лиц, чьи мобильные устройства подключены к системе ДБО, а организация, подготовка и совершение хищения в кредитной организации может занять у преступников несколько месяцев.

Специфика способов рассматриваемой категории преступлений, характер оставляемой неявной следовой картины указывают на необходимость до возбуждения уголовного дела проведения предварительной проверки, что и подтверждается анализом судебно-следственной практики. Продолжительность такой проверки может быть как совсем небольшой (к примеру, при задержании лица на месте преступления), так и занять довольно продолжительное время.

Так, В. В. Коломинов указывает, что в 27 % случаев предварительная проверка по делам рассматриваемой категории продолжалась до 30 суток и более[213].

Проведенное анкетирование сотрудников позволило определить следующие наиболее распространенные действия, осуществляемые при проверке сообщений: 76,5 % респондентов указали получение объяснений; 80,5 % – направление запросов, получение необходимых выписок, истребование документов; 59 % – проведение осмотра места происшествия; 51,4 % – проведение ОРМ; 35,6 % – назначение и производство судебных экспертиз; 41,9 % – исследование документов и предметов (Приложение 1).

Рассмотрим специфику проведения указанных действий подробнее.

Получение объяснений от заявителей (физических, юридических) и других лиц. Необходимо отметить, что, согласно ч. 1.2 ст. 144 УПК РФ, такие

[213]Коломинов В. В. Расследование мошенничества в сфере компьютерной информации ... С. 84.

объяснения, полученные до возбуждения уголовного дела, могут быть использованы в качестве доказательств.

В зависимости от категории потерпевшего, а также от способа совершения хищения, круг опрашиваемых лиц, а также спектр освещаемых вопросов, является различным. Так, при совершении преступления в отношении физического лица, соответствующие объяснения, как правило, получаются от самого заявителя и касаются выяснения обстоятельств совершения хищения денежных средств, а также возможных событий, действий, способствующих его совершению. Такими действиями, к примеру, могут быть: скачивание и установка на мобильное устройство нового приложения или обновление имеющегося, в результате чего происходит заражение устройства ВПО; получение электронных писем, сообщений как от незнакомых, так и внешне знакомых отправителей, в т. ч. содержащих различные ссылки, при переходе по которым, возможно, и произошло заражение. В связи с тем, что мошенничество в сфере компьютерной информации, как правило, совершается в отношении безналичных и электронных денежных средств, у заявителя выясняются сведения об открытых счетах, вкладах, электронных кошельках, подключенных услугах ДБО и т. д.

Процедура получения объяснений в случае совершения хищения денежных средств юридического лица отличается от предыдущего случая по кругу опрашиваемых субъектов и объему выясняемой информации.

Нередко факты совершения хищений в финансовых, а также других учреждениях, подтверждаются результатами проведенных внутренних проверок, служебных расследований, ревизиями и т. д. В ряде случаев, в рамках таких проверок, выдвигаются версии о вероятности совершения деяния кем-либо из определенной группы лиц, или высказываются обоснованные предположения относительно конкретного лица или группы лиц.

Так, по делу Lurk в результате такой проверки установлено, что хищение совершено в результате несанкционированного доступа в информационную компьютерную сеть, а сотрудники банка к произошедшему не причастны [214].

[214] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 …

В подобных, а также в случаях совершения хищения посредством внешнего вредоносного воздействия на информационную инфраструктуру юридического лица, производятся опросы лиц, выявивших признаки совершенного преступления, проводивших внутренние проверки, возможных свидетелей, сотрудников, отвечающих за обеспечение технической, компьютерной безопасности организации и других лиц о ставших им известными обстоятельствах произошедшего.

Выясняются вопросы о признаках неправомерного воздействия: изменение файловой структуры (переименование, появление новых файлов и папок, изменение размеров и содержимого файлов); изменение в заданных ранее настройках компьютера; необычные проявления в работе компьютерных устройств, свидетельствующие о работе вредоносных компьютерных программ, в т. ч. замедление или неправильная загрузка операционной системы, замедление работы и т. д.[215]

Проведение осмотра места происшествия, обнаружение, осмотр и изъятие следов преступления. Основной целью проведения осмотра места происшествия, конечно, является получение криминалистически важной информации посредством установления следовой картины преступления.

Тактика проведения указанных действий, возможности используемых при этом специальных технических средств, подробно будут рассмотрены в следующих параграфах. Кратко отметим лишь то, что спецификой их проведения является обязательное участие специалиста, нацеленность на установление и изъятие компьютерных устройств, электронных носителей информации, как обладателей значительного объема доказательственной базы, а также различного рода документов и предметов, имеющих отношение к расследуемому преступлению. Такими документами, к примеру, могут быть документы, свидетельствующие об оказании услуг подключения к сети провайдером, открытии банковского счета, электронного кошелька, расходные накладные,

[215] Бердникова О. П. Особенности первоначального и последующего этапов расследования мошенничества в сфере компьютерной информации : учеб. пособие. Екатеринбург, 2019. С. 8–9.

платежные поручения и другие документы, содержащие следы совершенного преступления.

При этом в ходе проведения указанных действий целесообразно использование различной криминалистической техники, в частности UFED, XRY, MOBILedit, «Мобильный криминалист», Тарантула и др., способных к извлечению, систематизации данных и построению отчетов, в т. ч. на основе удаленной информации[216].

К примеру, информационно-аналитический комплекс «Мобильный криминалист» предназначен, в том числе, для извлечения персональных данных из мобильных устройств, облачных сервисов, дронов и персональных компьютеров, для установления связи между владельцами устройств и их контактами, объединять контакты из разных источников, строить маршруты передвижения, выявлять самые посещаемые места конкретным субъектом[217].

Установленные и изъятые в ходе проведения осмотра следы преступления являются объектами назначения различных видов *экспертиз*. Особенностью расследования исследуемой группы преступлений является назначение и проведение различных подвидов компьютерно-технических экспертиз (которые подробно будут рассмотрены в параграфе 3.4.), заключения по которым являются одним из основных источников доказательственной и изобличающей преступную деятельность информации. Несмотря на предусмотренную законодателем возможность назначения такой судебной экспертизы уже на этапе предварительной проверки, на практике, ввиду ее высокой стоимости и длительности производства (на что также указали 17,4 % опрошенных респондентов (Приложение 1), ее назначение, как правило, не осуществляется. При этом проведение исследований носителей компьютерной информации в ходе проведения предварительной проверки рассматриваемой категории преступлений, имеет очень важное, а порой, решающее значение при решении вопроса о

[216]Скобелин С. Ю. Использование специальных знаний при работе с электронными следами // Российский следователь. 2014. № 20. С. 31–33.

[217] Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник университета имени О.Е. Кутафина (МГЮА). 2019. № 3 (55). С. 48–49.

возбуждении уголовного дела. Результаты проведения доследственных исследований, как правило, оформляются соответствующими актами, справками, отчетами; вопросы, в случае назначения судебных экспертиз и доследственных исследований, обычно ставятся одинаковые[218].

Как правило, совершение хищений у крупных хозяйствующих субъектов хорошо спланировано и относится к «организованному» типу мошенничества, что указывает на причастность к преступлению высоквалифицированных, опытных специалистов в сфере ИТТ.

В подобных случаях, когда, к примеру, суммы похищенного исчисляются сотнями миллионов рублей, представители таких организаций самостоятельно инициируют проведение соответствующих экспертиз и результаты исследования представляют правоохранительным органам. Так, по делу Lurk, после совершения хищения, ООО «Стройинвест» еще до возбуждения уголовного дела обратилось в компанию GroupIB для проведения соответствующей экспертной оценки. По результатам проведенного исследования следовало, что компьютер подвергся заражению ВПО[219].

Успешность установления, собирания и фиксации криминалистически важной информации, общий спектр которой станет будущим доказательственным базисом изобличения преступной деятельности, а также получение такой информации в процессе расследования, во многом зависит от плодотворности взаимодействия следователя, оперативных подразделений, а также специализированных структур.

Особое место в такой работе занимает взаимодействие со специалистами Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД РФ (ранее – Управление «К» МВД России) и его территориальными подразделениями – отделами на региональном уровне (далее – подразделения по борьбе с киберпреступлениями). Так, в ходе проведения проверки по одному из эпизодов хищения, сотрудниками

[218] Выявление и раскрытие хищений денежных средства с лицевых счетов банковских карт граждан : отчет о НИР / Т. В. Попова, А. А. Васильченко, А. В. Котяжов, М. В. Дульцев. М., 2017. С. 72–76.

[219] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

данного подразделения установлено, что денежные средства были переведены на счет ООО «Промторг», а в дальнейшем – на счета физических лиц и обналичены. Впоследствии установлены банкоматы и лица, занимавшиеся обналичиванием денежных средств. В ходе проведения ПТП зафиксированы разговоры об обналичивании денежных средств. Запрошены записи с камер видеонаблюдения, установлены приметы внешности. Так, в новогоднюю ночь гр. Р. с сестрой обналичивали денежные средства на протяжении 10–12 часов с перерывами[220].

Как уже отмечалось, важную роль в раскрытии, расследовании рассматриваемых преступлений имеет взаимодействие со специалистами АО «Лаборатория Касперского», компании F.A.C.C.T., и другими специализированными организациями.

Нельзя не отметить, что в практической деятельности нередко имеют место случаи неэффективного взаимодействия оперативных и следственных подразделений, на что указывают 19 % опрошенных в ходе проведения анкетирования респондентов. И. М. Комаров относительно уровня такого взаимодействия при расследовании «скримминговых» преступлений указывает, что оно «практически отсутствует или настолько слабо, что преимущественно связано с задержанием преступника и проведением вербальных следственных действий с его участием»[221].

Помимо сообщений от потерпевших физических и юридических лиц, наиболее распространенным источником получения информации о рассматриваемых преступлениях является проведение ОРМ. Результаты проведения данных мероприятий, как на этапе предварительной проверки, так и других последующих этапах расследования, являются источником принципиально важных, а порой и решающих, доказательств по делу.

Как уже отмечалось, характерной особенностью рассматриваемой группы преступлений, отличающей ее от преимущественного большинства других

---

[220] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

[221] Комаров И. М. Правовые и криминалистические проблемы расследования мошенничества в сфере компьютерной информации // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сб. мат-лов Всерос. науч.-практ. конф.. Воронеж, 2015. С. 13.

противоправных деяний, является отсутствие непосредственного контакта между преступником и потерпевшим и осуществление действий, охватываемых объективной стороной в особом информационном пространстве. Алгоритм манипуляций в данной среде, кроме внешних проявлений, не подвластен обыденному сознанию, в связи с чем отсутствует возможность визуального определения и фиксирования криминалистически значимой информации. В этой связи особую актуальность приобретает целесообразность проведения ОРМ, преимущественно имеющих негласный характер, позволяющих с использованием специальных технических средств установить и зафиксировать преступную деятельность. Так, 47,2 % опрошенных респондентов указали проведение не всего необходимого комплекса ОРМ, а также недостаточное акцентирование внимания на проведении негласных ОРМ (17,3 %) в качестве типичных ошибок, допускаемых при выявлении и раскрытии исследуемых преступлений (Приложение 1).

Итак, обращаясь к рассмотрению вопроса проведения предварительной проверки, а также пресечения преступной деятельности и раскрытия исследуемых преступлений, с позиции ОРД, можно отметить следующие ОРМ, целесообразность проведения которых способствует наиболее всестороннему, плодотворному и рациональному проведению расследования.

Наведение справок. 59,2 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). Применительно к рассматриваемой категории преступлений, преимущественно заключается в получении ответов на соответствующие запросы, направляемые в различные организации, к примеру, финансовые, кредитные структуры, операторам сотовой связи, провайдерам и т. д.

Так, от кредитных организаций и операторов платежных систем возможно получение сведений о проведенных финансовых операциях: времени осуществления трансакции, сумме операции, сведения о сервисе, через который совершена операция, о владельцах счетов, на которые были перечислены похищенные денежные средства, возможные сведения об указанных адресах

электронной почты, сведения об IP-адресах устройств, с помощью которых был произведен доступ к сервису ДБО и т. д.

От оператора сотовой связи возможно получение сведений о владельцах соответствующих номеров, номере IMSI и его заменах, IMEI телефонного аппарата, сведения о других телефонных аппаратах, в которых использовались данные SIM-карты и SIM-картах, используемых в данных телефонных аппаратах, сведения о поступлении и снятии со счета владельца номера денежных средств, сведения о детализации телефонных звонков и сообщений, сведениях о расположении базовых станций оператора во время оказания услуг сотовой связи. От оператора организации, предоставляющей услуги доступа к сети Интернет, возможно получение сведений о журналах доступа к сети Интернет, журналах использования IP-адресов[222].

При этом 46,9 % опрошенных респондентов указали на длительный срок получения ответов на запросы от кредитно-финансовых организаций, провайдеров и т. д. (Приложение 1), что является одним из проблематичных вопросов в процессе раскрытия, расследования рассматриваемой категории преступлений.

Поэтому на этапе проведения предварительной проверки, в некоторых случаях, в целях оптимизации процесса и исключения времени ожидания ответов на соответствующие запросы, целесообразно предложение заявителям возможности самостоятельного получения и предоставления соответствующих документов, получение которых не вызывает каких-либо трудностей. Например, справки (выписки) о наличии и состоянии своего банковского счета, электронного кошелька, истории проведенных операций, движении денежных средств по счетам, детализации своих телефонных переговоров.

Получение компьютерной информации (ПКИ). 65,2 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). ПКИ является относительно новым

[222] Гаспарян Г. З. Указ. соч. С. 128.

ОРМ, введенным в действие в 2016 г.[223], появление которого неоднозначно воспринято научным сообществом. Так, к примеру, А. С. Дубинин, А. В. Серов считают необходимым исключение его из перечня ОРМ, в связи с тем, что получение такой информации должно происходить в рамках следующих мероприятий: снятие информации с технических каналов связи, наблюдение, исследование предметов и документов, обследование помещений, зданий, сооружений, участков местности и транспортных средств[224]. Не рассматривая целесообразность самостоятельного существования данного ОРМ, необходимо отметить, что оно позволяет получить информацию, содержащуюся в компьютерных устройствах.

Получение наиболее оперативно значимой информации предполагается посредством негласного проведения мероприятия и может осуществляться путем: непосредственного подключения к телекоммуникационному оборудованию компьютера или компьютерной сети; электромагнитного перехвата излучений мониторов компьютера и считывания информации; аудиоперехвата с использованием акустических вибрационных датчиков; видеоперехвата с помощью специальных оптических приборов и др.[225].

В целом, способами доступа к информационным источникам с целью получения оперативно значимой информации могут быть:

– негласное применение специального программного обеспечения и оборудования для съема данных с компьютерных устройств, потенциально содержащих оперативно значимую информацию, включая скрытый дистанционный доступ к компьютерам, имеющим сетевое подключение;

---

[223] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : федер. закон от 06.07.2016 № 374-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

[224] Дубинин А. С., Серов А. В. Получение компьютерной информации как самостоятельное оперативно розыскное мероприятие // Вестник Воронежского института МВД России. 2018. № 3. С. 174.

[225] Дубоносов Е. С. Оперативно-розыскное мероприятия «Получение компьютерной информации»: содержание и проблемы проведения // Известия Тульского государственного университета. Экономические и юридические науки. 2017. № 2-2. С. 27.

– негласная установка в компьютерные устройства специального программного обеспечения, позволяющего фиксировать содержание осуществляемых с этих компьютеров сеансов связи;

– применение аналитического программного обеспечения для выявления оперативно значимой информации в базах данных различного назначения.

– проведение вербовочных мероприятий в отношении администраторов форумов, где злоумышленники обманом получают доступ к форумам, скрывая сведения об их действительных IP адресах;

– вербовка обменных сервисов Биткойн (Криптографическая валюта, а также электронная наличность), через которые преступники обналичивают денежные средства»[226];

– оперативно-розыскной мониторинг представляющих оперативный интерес сетевых информационных ресурсов, реализуемый через автоматизированный поиск ресурсов, содержащих запрещенную к распространению информацию; оперативно-розыскное изучение материалов выявленных ресурсов, связанных с деятельностью преступных сообществ; наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности[227].

Прослушивание телефонных переговоров (ПТП). 40,5 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). Данный вид ОРМ, как правило, является одним из наиболее информативных и позволяет получить сведения о содержании разговоров фигуранта, об абонентах этих переговоров, их установочных данных. Получаемая таким образом информация может содержать различного рода сведения о совершенном или готовящемся преступлении, его соучастниках, что способствует реализации поставленной цели изобличения всего преступного объединения. Так, по делу Lurk в отношении членов преступного

[226] Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации, предусмотренных статьей 159.6 Уголовного кодекса Российской Федерации : метод. рекомендации / С. Н. Миронов [и др.]. Казань, 2017. С. 57–58.

[227] Осипенко А. Л. Оперативно-розыскная деятельность в киберпространстве: ответы на новые вызовы // Научный вестник Омской академии МВД России. 2010. № 2 (37). С. 38–43.

сообщества неоднократно проводились ОРМ ПТП, в результате которых получалась и подтверждалась информация об осуществлении преступной деятельности[228].

Снятие информации с технических каналов связи (СИТКС). 59,6 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). ОРМ, «проводимое на основании судебного решения и заключающееся в перехвате с помощью специальных технических средств открытой (незашифрованной) информации, передаваемой проверяемыми лицами по техническим каналам связи»[229]. Проведение мероприятия преследует те же цели, что ПТП, и, как правило, проводится с ним в комплексе. Необходимо отметить, что на практике, получение такой информации, содержащейся, в т. ч. на электронных ящиках, в мессенджерах и социальных сетях, затрудняется в связи с использованием фигурантами различных средств «анонимизации» (VPN, PROXY, TOR, I2P). Как уже отмечалось, данный вид мероприятия схож с ОРМ получение компьютерной информации. Так, в ходе опроса 48 оперуполномоченных, проведенного Е. И. Куликовой, 21 из них указали на проведение СИТКС при необходимости получения информации, содержащейся в мессенджерах (WhatsApp, Viber, Telegram), а 27 о целесообразности проведения в таком случае ПКИ[230].

По делу Lurk, в соответствии с актом ОРМ СИТКС произведено удаленное копирование данных с серверов. Впоследствии установлено, что сервер используется, в том числе, для доступа к командным центрам управления ВПО, с помощью которого осуществляется неправомерный доступ[231].

Опрос. 55,1 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). Данный вид ОРМ направлен на получение (как гласное, так и негласное) какой-либо

---

[228] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

[229] Дубоносов Е. С. Оперативно-розыскная деятельность : учебник и практикум для вузов. М., 2023. С. 257.

[230] Куликова И. Е. Особенности проведения некоторых оперативно-разыскных мероприятий при раскрытии мошенничеств, совершаемых с использованием средств мобильной связи и методов социальной инженерии // Российский следователь. 2022. № 7. С. 70–74.

[231] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

оперативно значимой информации, способствующей раскрытию преступного деяния. Необходимо отметить, что проведение данного вида ОРМ в электронном виде не противоречит действующему законодательству. Изучение мест сетевого общения (чатов, форумов, конференций и т. д.), посещаемых разрабатываемым лицом, позволяет устанавливать контакт с субъектами, которым известны сведения о криминальной активности такого лица. При проведении опроса оперативный сотрудник может использовать инструменты обеспечения анонимности сетевого общения, скрывать свои истинные цели и профессиональную принадлежность. При этом возможно использование легендированной формы проведения опроса, при которой оперативный сотрудник легендирует истинные цели и ведомственную принадлежность[232].

Наблюдение. 16,1 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). Наблюдение осуществляется негласно и заключается в физическом, электронном или комплексном наблюдении как за лицами, так и за другими объектами. Такими объектами, к примеру, могут быть места хранения похищенного имущества[233]. К примеру, такими объектами могут быть установленные по IP-адресам места расположения компьютерных средств, с помощью которых было совершено или готовится к совершению преступление. Так, по делу Lurk, наблюдение было установлено за офисным помещением, использовавшимся для осуществления преступной деятельности. В ходе мероприятия фиксировались все посещавшие офис лица[234].

Сбор образцов для сравнительного исследования. 11 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). Учитывая специфику рассматриваемых преступлений, особую важность данный вид ОРМ имеет при обнаружении и изъятии объектов, содержащих цифровые следы преступления.

---

[232] Алескеров В. И., Колокольчикова О. Н. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации : учеб.-практ. пособие. Домодедово, 2016. С. 38.

[233] Дубоносов Е. С. Оперативно-розыскная деятельность. С. 242–243.

[234] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

Исследование предметов и документов. 47,9 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). Это «проводимое с применением специалистов непроцессуальное криминалистическое исследование объектов, сохранивших следы преступной деятельности или явившихся орудием совершения преступления» [235] . Как правило, такому исследованию подвергаются компьютерные устройства, технические средства, средства связи и т. п. Так, по делу Lurk,в соответствии с актом ОРМ было изучено содержимое скопированной на диск информации, в результате чего получены сведения о зараженных компьютерных устройствах[236].

Обследование помещений, зданий, сооружений, участков местности и транспортных средств. 23,5 % опрошенных респондентов указали данный вид ОРМ в числе наиболее распространенных по делам данной категории (Приложение 1). Заключается в гласном, зашифрованном или негласном обследовании указанных объектов с целью получения оперативно значимой информации, необходимой для раскрытия преступления. Так, могут обследоваться места расположения используемых преступниками компьютерных устройств и технических средств. По делу Lurk, в соответствии с протоколом, проведено обследование кабинета ВЧ-11 аэропорта «Кольцово», в результате обнаружены два ПК, у которых отсоединены и изъяты жесткие диски[237].

В правоприменительной практике известны примеры проведения ОРМ *Оперативный эксперимент.* В ходе его проведения в сетевом пространстве создавались негласно контролируемые объекты, представляющие интерес для лиц, осуществляющих противоправную деятельность (например, сайтов-ловушек, сайтов экстремистского содержания, сетей по обеспечению продажи наркотических средств и т. д.) [238] . При этом только 5,6 % опрошенных

[235] Дубоносов Е. С. Оперативно-розыскная деятельность. С. 236.
[236] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...
[237] Там же.
[238] Алескеров В. И., Колокольчикова О. Н. Указ. соч. С. 39.

респондентов указали на распространенность его проведения по делам данной категории (Приложение 1).

Учитывая количество предложений на различных сайтах теневого Интернета по предоставлению множества инструментов осуществления преступной деятельности в сфере ИТТ, а также предложений по найму лиц для осуществления различных услуг в данной сфере правоотношений (явно имеющих преступный контекст), целесообразной является возможность инициативного выявления преступлений рассматриваемой категории, на возможность чего указали 57,2 % опрошенных респондентов (Приложение 1).

В диссертации уже отмечалась избранная нами принципиальная позиция нацеленности ухода от преимущественной борьбы с «мелкими» преступлениями, при этом видится, что выявление, раскрытие и расследование «организованного» мошенничества в сфере компьютерной информации требует соответствующего высококвалифицированного уровня организации уголовно-правового реагирования, для чего может потребоваться объединение усилий нескольких правоохранительных структур. Полагаем, что системообразующим видом ОРМ при таком подходе должно быть *оперативное внедрение*. Только 8,6 % опрошенных респондентов указали данный вид ОРМ из числа наиболее распространенных в борьбе с рассматриваемой преступной деятельностью. Данное обстоятельство, вероятно, объясняется сложностью его организации, необходимостью консолидации для его проведения различных видов ресурсов: финансовых, трудовых, организационных, правовых и т. д. В итоге, к сожалению, одним из результатов отсутствия нацеленности на выявление организованных форм мошенничества является мнимая борьба по искоренению преступной деятельности данной направленности.

В данном контексте, исходя из сведений, полученных в результате использования метода экспертных оценок, анализа расследования преступлений, совершенных организованными преступными формированиями, предложен один из алгоритмов борьбы с «организованным» мошенничеством в сфере компьютерной информации.

Итак, направление работы в данной ситуации может включать в себя проведение следующих действий: поиск информации о запросе на осуществление явно противоправных действий в сфере компьютерной информации и отклик на данное предложение; далее, как правило, потребуется прохождение соответствующего отбора на наличие специальных навыков и познаний посредством выполнения определенного задания; после успешного выполнения задания и прохождения собеседования, получение доступа к средствам общения, используемым в преступном формировании.

Так, в преступном формировании Lurk, процедура ввода новых членов после прохождения проверки включала в себя: выбор псевдонима; создание пользовательских профилей: электронной почты, чат-клиента Jabber; получение ключей доступа для подключения к VPN; создание пользовательских профилей в панели администрирования и на локальном веб-сервисе[239] .

Далее, в процессе работы, в ходе проведения различных видов ОРМ, сбор и фиксация информации об используемом ВПО, структуре, членах и организаторах преступного формирования, объектах преступного посягательства; возможен ввод в группу других участников, желательно, в финансовую группу, к примеру, для выполнения функции «обнальщиков» или лиц, предоставляющих, принадлежащие им юридические лица, для перевода на их счета похищенных денежных средств. При успешном проведении оперативной разработки мероприятие может быть окончено при наличии достаточных оснований полагать, что собранной доказательственной информации достаточно для установления и задержания всех или большинства членов преступного формирования, а также предъявления им обвинения.

Возможным идеальным сценарием окончания оперативной разработки может явиться перенаправление во время совершения очередного преступления похищенных денежных средств на подконтрольные правоохранительным органам счета либо обналичивание и получение похищенных денежных средств внедренным сотрудником.

[239] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

Необходимо отметить, что, уделяя внимание применению комплекса различных ОРМ, существует вероятность ухода от опасности установления не всех членов преступного формирования, на типичность чего указывают 22,8 % опрошенных (Приложение 1) и изобличения преступной деятельности преимущественно «низовых» исполнителей, тенденции чего мы, как правило, и наблюдаем.

Одним из важных условий является получение данных в результате проведения ОРМ и их представление в соответствии с действующим законодательством.

На практике нередко имеют место случаи, когда наличие процессуальных ошибок в данных стратегически важных вопросах приводит к признанию, полученных таким образом доказательств недопустимыми, что может привести к потере принципиально важных, а может и центральных, доказательственных фактов совершения преступной деятельности.

Проведенное анкетирование, кроме уже указанных, также выявило следующие наиболее типичные ошибки, допускаемые оперативными сотрудниками при выявлении и раскрытии исследуемых преступлений: ошибки в ходе проведения ОРМ (22,6 %), отсутствие нацеленности раскрытии «организованного» мошенничества (23,1 %), ошибки в ходе обнаружения, изъятия, осмотра электронных носителей информации (19,8 %), ошибки в ходе оформления результатов ОРД (11,7 %), нераскрытие сопутствующих преступлений (16,9 %) (Приложение 1).

Таким образом, использование предоставляемых ОРД инструментов получения необходимой информации, в совокупности с проводимыми следственными действиями, способствует повышению вероятности изобличения преступной деятельности не только «низовых» исполнителей, но и всего преступного объединения.

В целом, весь комплекс оперативно-розыскных и следственных действий направлен на установление и доказывание следующих обстоятельств:

– факта совершения преступления;

– способа совершения преступления;

– времени и места его совершения;

– факта использования в совершении преступления соответствующего ВПО, соответствующих компьютерных устройств, технических средств, других орудий преступления;

– факта совершения сопутствующих преступлений, к примеру, создания, использования, распространения вредоносных компьютерных программ, а также лиц, участвующих в их создании, использовании, распространении;

– лиц, виновных в совершении преступления, их роль в преступном объединении и характеристика;

– лиц, потерпевших от преступного воздействия, размер и характер причиненного ущерба;

– местонахождение похищенных денежных средств: места возможного обналичивания, перенаправления на подконтрольные преступникам счета, карты и т. п.

Итак, логическим итогом окончания проведения предварительной проверки является рассмотрение вопроса о возбуждении уголовного дела. При этом автор совершенно согласен и поддерживает позицию Ю. П. Гармаева о необходимости при оценке собранной в результате доследственной проверки информации и решении вопроса о возбуждении уголовного дела исходить из позиции судебной перспективы по делу. Ученым сформулировано определение судебной перспективы – это субъективная оценка правоприменителя по поводу вероятности вынесения обвинительного приговора лицу, в отношении которого начато или планируется уголовное преследование. Автором выделены следующие варианты существования данной категории:

– хорошая судебная перспектива. Характеризуется уверенностью в наличии состава преступления, в наличии достаточных доказательств и в том, что противодействие не сможет помешать вступлению в силу обвинительного приговора суда;

– неясная судебная перспектива. Характеризуется наличием спорного вопроса о наличии состава преступления, отсутствием минимальной и необходимой совокупности обвинительных доказательств, наличием интенсивного, профессионального противодействия уголовному преследованию, которое может помешать вступлению в силу обвинительного приговора суда;

– судебная перспектива отсутствует. Характеризуется отсутствием или маловероятностью наличия состава преступления, отсутствием минимальной совокупности допустимых доказательств, наличием интенсивного, профессионального противодействия уголовному преследованию, которое наверняка может помешать вступлению в силу обвинительного приговора суда[240].

Конечно, наиболее приемлемым результатом проведенной предварительной проверки является наличие оснований полагать, что собранные данные достаточны для возбуждения уголовного дела и наличия у него хорошей судебной перспективы. Совокупность таких аргументирующих оснований могут составлять следующие факты:

– в ходе проведения осмотра места происшествия обнаружены и изъяты компьютерные средства, устройства и другие электронные носители информации, осмотр которых указал на наличие явных следов неправомерного воздействия на компьютерную информацию, следствием чего явилось хищение денежных средств;

– результаты проведенных экспертиз подтверждают наличие неправомерного воздействия на компьютерную информацию, свидетельствуют о наличии следов работы вредоносных компьютерных программ. Тип используемой вредоносной программы предполагает причастность к совершению преступления определенного лица или преступного объединения;

– проведенные юридическим лицом служебные проверки свидетельствуют о совершении хищения и его следовой картине, либо о наличии обоснованного предположения совершения деяния конкретным лицом;

---

[240] Гармаев Ю. П. Концепция «судебная перспектива по уголовному делу» и криминалистическая ситуалогия // Вестник Бурятского государственного университета. 2013. № 2. С. 177–181.

– установление и изъятие записей с камер видеонаблюдения, свидетельствующих о совершении преступления конкретными лицами, как установленными, так и неустановленными;

– в ходе проведения ОРМ получены неопровержимые данные о совершении хищения и лицах его подготавливающих, совершающих или совершивших. Наиболее ценным в такой ситуации является получение сведений о причастности к совершению преступления не только конкретных исполнителей, но и других членов преступного объединения;

– собранные доказательства соответствуют требованиям законодательства. К примеру, при изъятии соответствующих носителей электронной информации, соблюдены предъявляемые к данному процессу требования; получение данных в результате проведения ОРМ и их представление соответствует уголовно-процессуальному законодательству об ОРД, в т. ч. Инструкции по материалам проверки сообщений о преступлениях, Инструкции о порядке предоставления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд[241];

– полученные сведения о перемещении по счетам похищенных денежных средств свидетельствуют об их владельцах;

– противодействие стороны защиты не такое активное, как предполагалось изначально. Заявляются стандартные ходатайства, результаты проведенных ОРМ не обжалуются в суде[242].

В случаях с неясной судебной перспективой, а также когда судебная перспектива отсутствует, лицу, принимающему решение о возбуждении уголовного дела следует максимально взвешенно подходить к реальной оценке объема и качества собранных материалов, а также перспективе дальнейшего возможного их получения.

---

[241] Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд : приложение к приказу МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27.09.2013 № 776/703/509/507/1820/42/535/398/68 // Доступ из справ.-правовой системы «КонсультантПлюс».

[242] Поляков Н. В. Указ. соч. С. 161.

3.2. Типичные следственные ситуации и версии расследования мошенничества в сфере компьютерной информации

Одним из наиболее значимых структурных элементов создаваемой криминалистической методики является направление, определяющее ситуацию, сложившуюся к определенному моменту процесса уголовно-правового реагирования в отношении совершенного или готовящегося преступного деяния, а также указывающее на возможные пути и перспективы разрешения данных ситуаций.

Наиболее существенный вклад в развитие теории следственных ситуаций привнесли О. Я. Баев, Р. С. Белкин, Т. С. Волчецкая, В. К. Гавло, И. М. Лузгин, В. Е. Корноухов, А. Н. Колесниченко, А. В. Шмонин, Н. П. Яблоков и др. ученые.

Из имеющихся в криминалистике подходов к характеристике и классификации следственных ситуаций приведем предложенный авторами учебника по криминалистике (Т. В. Аверьяновой, Р. С. Белкиным, Ю. Г. Коруховым, Е. Р. Россинской), которые следственную ситуацию оценивают как динамическую систему, постоянно изменяющуюся под воздействием объективных (независящих от участников) и субъективных (порождаемых действиями и поведением участников) факторов. Такая система условий состоит из компонентов психологического, информационного, процессуального и тактического, а также материального и организационно-технического характера[243].

С. А. Куемжиева указывает, что содержание следственной ситуации в значительной степени определяется характеристикой следственных действий и оперативно-розыскных мероприятий, необходимых для расследования отдельного вида преступлений[244].

Среди наиболее практически значимых элементов классификаций следственных ситуаций авторы указывают: начальные, промежуточные и

---

[243] Криминалистика : учебник / Т. В. Аверьянова [и др.]. М., 2010. С. 486–487.

[244] Куемжиева С. А. Понятие следственной ситуации и ее роль в определении средств и методов отдельного расследования // Вестник Краснодарского университета МВД России. 2015. № 4(30). С. 194.

конечные ситуации; конфликтные и бесконфликтные ситуации; благоприятные и неблагоприятные ситуации. При этом отмечается, что в силу индивидуализации каждой конкретной следственной ситуации, полностью типизировать их содержание невозможно. Авторы указывают, что типизировать следственные ситуации можно лишь по одному из образующих ее элементов и, как правило, им является компонент информационного характера[245].

Считаем, что именно имеющийся объем информации о событии совершенного или готовящегося преступления во многом определяет дальнейшее направление и вариантность всего процесса расследования.

Несмотря на наличие индивидуальных особенностей каждого из преступных деяний, идентификация складывающейся в отношении него ситуации с одной из определенных методикой расследования типичных следственных ситуаций, и использование предложенного алгоритма ее разрешения, позволяет определить и скоординировать дальнейшее направление всего процесса расследования, оптимизировать использование различных видов ресурсов для эффективного раскрытия и расследования преступления.

По этому поводу совершенно справедливо заключает Т. С. Волчецкая, указывая, что анализ и оценка следственной ситуации имеют весьма существенное прикладное значение, поскольку способствуют:

– выдвижению обоснованных следственных версий, определению дальнейших путей расследования;

– выбору оптимального сочетания и последовательности проведения следственных действий и ОРМ;

– использованию наиболее целесообразных направлений взаимодействия следователя с органами дознания, иными службами;

– выбору наиболее эффективных тактических приемов, комбинаций и операций;

---

[245] Криминалистика. М., 2010. С. 487–488.

– выявлению причин и условий, способствующих совершению преступлений[246].

Предложенный для разрешения ситуаций алгоритм действий не носит императивный характер и в зависимости от конкретной ситуации предполагает вариантность и инициативность принятия субъектом расследования самостоятельных, наиболее целесообразных при данных обстоятельствах решений.

В научном сообществе существуют различные подходы к констатации типовых следственных ситуаций, складывающихся в процессе расследования рассматриваемых преступлений.

Так, С. М. Голятина относительно расследования преступлений, совершаемых в отношении электронных денежных средств, указывает на наличие следующих следственных ситуаций:

– «сложная ситуация, в которой нет достаточной информации о событии преступления, необходимо установить лицо, совершившее его, а также обстоятельства по данному делу;

– простая ситуация, в которой известно событие преступления и лицо, совершившее его, и нужно установить обстоятельства по данному делу»[247].

По мнению Н. М. Малыхиной, С. В. Кузьминой, такими следственными ситуациями являются ситуации, при которых:

– «установлены способ совершения интернет-мошенничества, потерпевшие и свидетели, выявлены отдельные цифровые следы, данные о лице, совершившем преступление, отсутствуют;

– установлены способ совершения интернет-мошенничества, потерпевшие и свидетели, цифровые следы не выявлены, данные о лице, совершившем преступление отсутствуют;

---

[246]Волчецкая Т. С. Криминальные и криминалистические ситуации // Криминалистика : учебник / под ред. Н. П. Яблокова. М., 2016. С. 80-81.

[247] Голятина С. М. Методика расследования хищений электронных денежных средств : дис. … канд. юрид. наук. Волгоград, 2022. С. 91.

– установлены способ совершения интернет-мошенничества, потерпевшие и свидетели, выявлены цифровые следы, известны некоторые данные о лице, совершившем преступление, но его местонахождение неизвестно»[248].

Принимая во внимание мнения различных ученых, а также исходя из анализа судебно-следственной практики относительно объема информации, имеющейся на первоначальном этапе расследования мошенничества в сфере компьютерной информации, нами выделены следующие типичные следственные ситуации[249]:

1) имеется информация о способе совершения преступления, выявлены следы преступления, при этом сведения о личности преступника отсутствуют;

2) имеется информация о способе совершения преступления, при этом объем выявленных следов незначительный, сведения о личности преступника отсутствуют;

3) имеется информация о способе совершения преступления, личности преступника, а также выявлены следы преступления:

– заявитель (физическое или юридическое лицо) самостоятельно выявил признаки совершения преступления, а также личность преступника;

– признаки преступления, а также личность преступника выявлены в результате осуществления оперативно-розыскной деятельности или в результате расследования других преступлений;

– виновное лицо задержано на месте совершения преступления;

4) имеется информация о способе совершения преступления, выявлены следы преступления, имеются сведения о личности преступника, однако его местонахождение неизвестно.

Рассмотрим указанные ситуации подробнее.

Имеется информация о способе совершения преступления, выявлены следы преступления, при этом сведения о личности преступника отсутствуют.

---

[248] Малыхина Н. И., Кузьмина С. В. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети Интернет // Вестник Томского государственного университета. 2021. № 462. С. 240–242.

[249] Харина Е. А. Типовые следственные ситуации первоначального этапа расследования мошенничества в сфере компьютерной информации // Закон и право. 2023. № 11. С. 274–276.

Как правило, данная ситуация является наиболее распространенной при расследовании преступлений данной категории. Так, 53,1 % опрошенных респондентов выделили данную ситуацию из числа наиболее типичных (Приложение 1). В связи с отсутствием ключевых сведений о личности преступника раскрытие таких преступлений может занимать довольно продолжительный период времени, а в случае совершения «организованного» мошенничества может длиться годами. К примеру, деятельность ОПС Lurk, как установлено следствием, началась в 2013 г., а задержание его ключевых участников состоялось только в 2016 г.[250]

Как уже отмечалось, в таких случаях имеющийся объем информации может свидетельствовать о типе совершенного мошенничества, уровне специальных познаний преступника, отличительных чертах его личности (ранее рассмотренных во второй главе диссертации), что будет способствовать выдвижению версий о причастности к совершению преступления конкретного лица или преступного формирования.

В зависимости от способа совершения преступления, наиболее характерными действиями в такой следственной ситуации являются следующие:

– проведение осмотра места происшествия;

– обнаружение, изъятие следов преступления, в т. ч. цифровых следов, компьютерных устройств, носителей компьютерной информации; получение образцов для сравнительного исследования;

– направление соответствующих запросов, получение выписок о владельцах банковских счетов, расходных накладных и других финансовых документов;

– получение заключений о проведенных внутренних проверках, ревизиях организации;

– истребование должностных инструкций, трудового договора (в случае совершения преступления сотрудником организации), правил внутреннего трудового распорядка и т. д.;

– получение информации о движении денежных средств со счета заявителя.

[250]Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

С этой целью необходимо направить запросы на установление владельца счета, на который были переведены похищенные денежные средства, сведений о движение по нему денежных средств, а также данные об IP-адресах при подключении для управления счетом. Одной из особенностей совершения большинства преступлений рассматриваемой категории является использование особого механизма сокрытия следов преступления, заключающегося в перенаправлении перед обналичиванием похищенных денежных средств на несколько других счетов, электронных кошельков и т. д. Так, 49 % респондентов указали данные действия как затрудняющие процесс расследования (Приложение 1). В таких ситуациях необходимо получение выписок о владельцах данных счетов и о проводимым по ним операциям. В случае их наличия, предпринять меры к наложению ареста на имущество[251].

Так, по делу Lurk, одним из банков были представлены анкетные данные 67 держателей банковских карт, а также информация об IP-подключениях данных карт к интернет банкингу[252];

– проверка имеющихся данных об использованных в ходе совершения преступления банковских счетах, абонентских номерах, сайтах в подсистеме «Дистанционное мошенничество» ИБД-Ф (интегрированный банк данных федерального уровня) на предмет их использования в совершении других преступлений. Так, в ходе проведения расследования, по делу Lurk, похищенные денежные средства зачислялись на счета одних и тех же физических лиц[253];

– осуществление взаимодействия с компаниями, оказывающими услуги Интернет-провайдера[254], операторами сотовой связи, а также регистраторами доменного имени с целью получения необходимой информации. В частности такими сведениями могут быть данные о владельцах абонентских номеров, доменного имени сайта, сведения о дате и времени добавления записи по

[251] Особенности квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей: методические рекомендации / А. Ю. Ушаков [и др.]. Н. Новгород, 2020. С. 40.

[252] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1...

[253] Там же.

[254] Сидорова К. С. Алгоритм действий следователя при расследовании мошенничеств, совершаемых дистанционным способом // Закон и право. 2020. № 12. С. 232.

системному времени сервера соединений; IP-адрес маршрутизатора, обслуживающего данную сессию, логин пользователя, наименование линии, вид соединения, тип записи (start, stop, update и дополнительные параметры)[255];

– особое внимание в данном случае уделяется проведению ОРМ (подробно рассмотрены в предыдущем параграфе) и их результатам. Так, по делу Lurk были предоставлены материалы ОРД, проводимые с октября 2014 г. в отношении лиц, причастных к созданию и использованию ВПО Lurk, в т. ч.: справка в отношении членов преступного сообщества на 297 листах, CD-диски с записями с камер видеонаблюдения, с детализацией соединений абонентов сотовой связи, схема телефонных соединений, фотографии участников, данные сайта «Вконтакте»[256].

При этом во исполнение наиболее целесообразного для борьбы с преступностью и избранного нами принципа изобличения всей преступной иерархии, наряду с уже обозначенными действиями, эффективной видится целесообразность проведения комплекса ОРМ, позволяющего выявить других участников преступного объединения;

– организация взаимодействия со специалистами подразделений по борьбе с киберпреступлениями. К примеру, одним из способов такого взаимодействия может быть проведение ОРМ с целью получения сведений об активности мобильных телефонов в определенном месте и в определенное время. Так, использование одного из самых распространенных способов сокрытия следов преступления – использование преступниками SIM-карт, оформленных на посторонних лиц, либо на вымышленные установочные данные, получение информации об IMEI телефонных аппаратов, а далее и сведений о работавших в данном устройстве в разное время SIM-картах, при условии их систематизации и анализа, может явиться источником оперативно значимой информации о самом преступнике, либо о лицах, могущих располагать о нем необходимой информацией. Источником криминалистически важной информации относительно истинных владельцев таких SIM-карт могут быть сведения об

[255] Малыхина Н. И., Кузьмина С. В. Указ. соч. С. 240.
[256] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

установочных данных лица, со счета или абонентского номера которого осуществлялось пополнение баланса данной SIM-карты;

– проведение следственного действия, направленного на получение информации о соединениях между абонентами и (или) абонентскими устройствами; анализ полученной информации, установление владельцев абонентских номеров;

– при наличии информации об электронной почте, к примеру, получение потерпевшим по электронной почте письма, содержащего ссылку на установку вредоносной компьютерной программы, необходимо установить IP-адрес, MAC-адрес, Интернет-провайдера, у которого запросить и произвести выемку сообщений за интересующий период времени. При запрашивании у интернет-провайдера сведений об абоненте, которому были предоставлены конкретные IP-адреса, необходимо точно указывать время обращения и наименование ресурса. Это необходимо для существенного сужения круга лиц, которым предоставлялся интересующий следствие IP-адрес в случае использования технологии NAT (Network Address Translation – «преобразование сетевых адресов»), позволяющей предоставлять один IP-адрес нескольким пользователям одновременно[257];

– при установлении IP-адреса направить запрос об установлении лица, которому он предоставлялся и места предоставления[258];

– организация взаимодействия со специалистами АО «Лаборатория Касперского», компании F.A.C.C.T. (выделена в 2023 г. из компании Group-IB) и другими специалистами в сфере ИТТ. Как уже отмечалось, взаимодействие с такими структурами могут инициировать сами потерпевшие еще до начала процесса расследования;

– при установлении счета, на который были переведены денежные средства, необходимо направить запрос об установлении его владельца, привязанных

[257] Особенности квалификации и расследования хищений ... С. 35–36.
[258] Там же. С. 43–44.

абонентских номерах, электронной почте, об IP-адресах, использованных при управлении счетом; далее проведение допросов обысков[259];

– назначение соответствующих экспертиз и получение по ним заключений. По результатам проведенных экспертиз, по особенностям использованного ВПО, специфическим признакам совершения преступления, в результате взаимодействия со специалистами, выдвигаются предположения о возможной причастности к совершению преступления того или иного хакерского преступного объединения. Так, результаты проведения множества экспертиз свидетельствовали об использовании в совершении преступления ВПО, детектируемого как Lurk[260];

– получение информации посредством изучения записей с камер видеонаблюдения. Так, в случае совершения преступления с непосредственным участием преступника, к примеру, при обращении в финансовое учреждение, при получении, обналичивании денежных средств в банкоматах и т. д., изымаются, просматриваются записи с камер видеонаблюдения, расположенных не только в данных помещениях, но и на улицах, других помещениях, с целью установления признаков внешности преступников, маршрутов и средств передвижения.

Так, по делу Lurk, из банков были представлены записи камер видеонаблюдения, где две женщины, снимают с банкоматов денежные средства по различным банковским картам, на которых наклеены отрезки бумаги с паролями. Позже чеки по произведенным операциям, которые женщины забирали с собой, были изъяты у участников преступного сообщества. Только в ходе обыска у одного из них изъято 1909 чеков[261];

– получение необходимой информации посредством проведения допросов. К примеру, в ходе проведения допроса потерпевшего необходимо получить наиболее полную информацию об обстоятельствах, предшествующих совершению хищения, которые могли бы повлечь возможную некорректную работу компьютерных устройств, к примеру, установка или обновление каких-

[259] Особенности квалификации и расследования хищений ... С. 35–36.
[260] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...
[261] Там же.

либо компьютерных программ, получение на электронную почту писем «сомнительного» содержания, осуществление оплаты товара на различных сайтах. Также, наряду с прочим, выясняется информация о степени осведомленности кого-либо об имеющихся учетных записях потерпевшего, его профилях, логинах, паролях, подключенных услугах ДБО.

Представители различных организаций, указанных в предыдущих пунктах, могут быть допрошены в качестве специалистов с целью получения дополнительной оперативно значимой информации. К примеру, «представитель компании провайдера может быть допрошен в качестве свидетеля относительно сведений о логинах, анкетных данных, адресах абонентских подключений, конкретных внешних IP-адресах, с которых осуществлялся доступ к сети Интернет, типе IP-адреса (статический либо динамический), сроках и порядке заключения договора на представление интернет-соединений»[262];

– проведение обысков по месту жительства подозреваемых, жилых и нежилых помещениях, используемых для совершения преступной деятельности;

– организация взаимодействия с правоохранительными структурами различных государств, в т. ч. посредством направления соответствующих запросов. Как мы уже отмечали, еще одной из особенностей рассматриваемой преступной деятельности является ее трансграничный характер. Одним и тем же преступником или преступным сообществом преступления могут совершаться не только на территории разных регионов РФ, но и на территории разных стран. В данном случае крайне важным является вопрос взаимодействия с международными правоохранительными структурами. В настоящее время в данном направлении РФ сотрудничает со странами БРИКС, государствами-участницами СНГ, АСЕАН и др. При этом имеющийся уровень организации такого взаимодействия указывает на наличие некоторых трудностей.

В ходе проведенного исследования, 47,1 % опрошенных респондентов отметили совершение преступления из-за пределов РФ, отсутствие должного взаимодействия с правоохранительными структурами других государств, как

[262] Малыхина Н. И., Кузьмина С. В. Указ. соч. С. 241.

один из видов трудностей в ходе выявления, раскрытия и расследования рассматриваемого вида преступлений (Приложение 1).

Так, Е. С. Шевченко указывает, что «сложности сотрудничества по расследованию и раскрытию киберпреступлений с правоохранительными органами иностранных государств усугубляются тем, что в действующих законодательствах разных стран установлены свои нормы в отношении компьютерных преступлений, выработаны свои подходы к назначению и производству компьютерных экспертиз»[263].

Как справедливо заключает в своем исследовании С. М. Голятина, во взаимодействии со странами, не поддерживающими международное сотрудничество правоохранительных органов, возникают трудности в установлении данных: соединения о прохождении вызова от абонента IP-телефонии и пользователей социальных сетей, использующих VPN-сервисы и адресное пространство их операторов связи и интернет-провайдеров, владельцев доменных имен, зарегистрированных в этих странах, об электронных платежах, совершаемых с использованием интернет-ресурсов по технологии card2card, а также платежных систем и банковских карт банков-эмитентов, находящихся на территории этих стран[264]. Таким образом, для установления действительных IP-адресов оформляются соответствующие международные запросы.

Имеется информация о способе совершения преступления, при этом объем выявленных следов незначительный, сведения о личности преступника отсутствуют.

В ходе проведения анкетирования 50,8 % респондентов указали данную ситуацию в числе наиболее типичных (Приложение 1). Преимущественно данная следственная ситуация складывается в случаях использования при совершении преступления высококачественных вредоносных компьютерных программ, созданных высококвалифицированными компьютерными специалистами. Как уже отмечалось, такие программы работают скрытно и изощренно, способны к

[263] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : дис. … канд. юрид. наук. М.:, 2016. С. 35.

[264] Голятина С. М. Указ. соч. С. 82.

самоуничтожению и нейтрализации следов своего присутствия на компьютерных устройствах потерпевших. Объем выявляемых цифровых следов при таких ситуациях крайне незначителен, либо может вообще отсутствовать. Данные обстоятельства свидетельствуют о совершении «организованного» типа мошенничества, спланированного и совершенного на высоком качественном уровне, что, как правило, характерно для высокопрофессиональных хакерских объединений, создаваемых для многократного крупномасштабного совершения хищений денежных средств. Примером действия такой вредоносной компьютерной программы является ранее упомянутая программа Lurk, используемая для совершения преступлений одноименным хакерским ОПС.

Расследование преступлений данной категории занимает довольно продолжительное время. Наряду с большинством уже перечисленных действий, важную роль в данной ситуации занимает взаимодействие с подразделениями по борьбе с киберпреступлениями, а также с организациями, специализирующимися на обеспечении информационной безопасности, таких как АО «Лаборатория Касперского», компания F.A.C.C.T. Данными структурами «по крупицам» собираются и анализируются сведения относительно деятельности и численности данных хакерских группировок, используемом ими ВПО. В результате совместных усилий правоохранительных структур и специалистов в области компьютерной безопасности деятельность большинства хакерских объединений пресекается, при этом нередко для этого требуется не один год кропотливой работы. Наряду с вышеперечисленными следственными действиями и другими мероприятиями, значительную помощь в расследовании таких преступлений оказывает использование соответствующих баз данных. К примеру, при наличии информации об IMEI мобильного устройства, IMSI SIM-карты, номеров банковских счетов, адресов электронной почты и других сведений, возможно получение информации о возможности их использования при совершении других преступлений.

Необходимо отметить, что для изобличения преступной деятельности в данной ситуации особая роль также отводится проведению комплекса преимущественно негласных ОРМ.

Имеется информация о способе совершения преступления, личности преступника, а также выявлены следы преступления.

В ходе проведенного анкетирования 20,2 % опрошенных выделили данную ситуацию первоначального этапа расследования из числа наиболее типичных (Приложение 1). Разумеется, с учетом ранее приведенной классификации следственных ситуаций[265], данная ситуация является наиболее благоприятной и в случае собирания соответствующей доказательственной базы обладает хорошей судебной перспективой[266].

В случае установления личности преступника, в зависимости от ситуации, в дополнение к части ранее указанным следственным и иным действиям производятся его задержание, личный обыск, допрос, обыски по месту работы и месту жительства, наложение ареста на его имущество и т. п.

Имеется информация о способе совершения преступления, выявлены следы преступления, имеются сведения о личности преступника, однако его местонахождение неизвестно.

В ходе проведенного анкетирования 20,1 % опрошенных выделили данную ситуацию первоначального этапа расследования из числа наиболее типичных (Приложение 1). Наряду с большинством действий, указанных ранее, особое внимание в данной ситуации уделяется получению всесторонней информации о личности преступника: адресах регистрации и возможного проживания, зарегистрированном автотранспорте, объектах недвижимого имущества, номерах сотовой связи, приобретении билетов на различные виды общественного транспорта (железнодорожных, авиа-, автобусных, речных, морских) и лицах, с которыми он выезжал по различным направлениям, сбор информации о преступнике и его окружении посредством изучения сведений, размещенных на

[265] Криминалистика. М., 2010. С. 487–488.
[266] Гармаев Ю. П. Концепция «судебная перспектива по уголовному делу» … С. 177–181.

его страницах социальных сайтов сети Интернет, а также на страницах его родственников и близких друзей и т. д.

Получение оперативно значимой информации осуществляется посредством обращения к различным базам данных, получения ответов на соответствующие запросы, посредством проведения различных видов, как гласных, так и негласных, ОРМ: наведение справок, ПТП, СИТКС и т. д., анализ детализации соединений, проведение допросов лиц, могущих располагать необходимой информацией.

Также обоснованно целесообразным является применение программных комплексов «ЛКС Аналитика», «СПРУТ», «Крибрум», «Катюша», «Зеус», «Лисс-М», «Буратино», «Доктор Ватсон», «Демон Лапласа», которые, в том числе, способствуют получению систематизированной информации из различных общедоступных онлайн-источников, в т. ч. социальных сайтов, блогов и т. д.[267]

Итак, как мы видим, основные направления расследования типичных ситуаций первоначального этапа расследования мошенничества в сфере компьютерной информации, подразделяющиеся в зависимости от степени информативности относительно преступного деяния, ориентированы на установление его центральных элементов: способа, следовой картины и личности преступника. Объем собранной на данном периоде доказательственной информации во многом определяет направление и стратегию дальнейшего процесса расследования, а также ориентирует относительно степени успешности складывающейся судебной перспективы по делу.

Складывающиеся типичные ситуации последующего этапа расследования, как правило, систематизируют относительно степени признания подозреваемым своей вины в совершении преступления, а также достаточности, имеющихся в деле доказательств.

---

[267] Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учеб. пособие / А. А. Балашова [и др.]. М., 2021. С. 127.

Так, Н. И. Малыхина и С. В. Кузьмина выделяют следующие следственные ситуации последующего этапа расследования:

1. обвиняемый признает свою вину в совершении преступления, дает показания относительно обстоятельств преступления и соучастников, что подтверждается доказательствами по уголовному делу;

2. обвиняемый признает свою вину в совершении преступления, но в материалах уголовного дела содержится недостаточное количество доказательств его виновности;

3. обвиняемый отрицает свою вину в совершении преступления полностью или частично, но в материалах дела содержится достаточное количество доказательств, подтверждающих вину[268].

По мнению О. П. Бердниковой такими типовыми ситуациями являются следующие:

1. собрано достаточно доказательств для предъявления обвинения, однако подозреваемый отрицает свою причастность полностью или частично либо пользуется правом отказа от дачи показаний на основании ст. 51 Конституции РФ;

2. собранных на первоначальном этапе расследования доказательств недостаточно для предъявления обвинения всем участникам преступной группы и определения роли каждого;

3. подозреваемые признают свою вину в совершении мошенничества в сфере компьютерной информации по предварительному сговору, но отрицают наличие организованной группы, а доказательств, указывающих на ее существование, добыто недостаточно;

4. после завершения первоначальных следственных действий и ОРМ в отношении уже установленных эпизодов и выявленных лиц поступает оперативная либо процессуальная информация в отношении новых криминальных эпизодов, совершенных теми же подозреваемыми либо

[268] Малыхина Н. И., Кузьмина С. В. Указ. соч. С. 243–246.

появлением новых фигурантов имеющих непосредственное отношение к совершенным мошенничествам в сфере компьютерной информации[269].

Анализ судебно-следственной практики позволил выделить следующие типичные следственные ситуации, складывающиеся на последующем этапе расследования рассматриваемых преступлений:

I. Собранных по делу доказательств достаточно для установления вины подозреваемого, при этом:

1) подозреваемый признает свою вину в совершении преступления;

2) подозреваемый отрицает свою вину в совершении преступления;

3) подозреваемый частично признает свою вину, при этом отрицает:

а) совершение других, сопутствующих преступлений;

б) совершение преступления в составе ОПГ, организованного преступного сообщества.

II. Собранных по делу доказательств недостаточно для установления вины подозреваемого, при этом:

1) подозреваемый признает свою вину в совершении преступления;

2) подозреваемый отрицает свою вину в совершении преступления;

3) подозреваемый частично признает свою вину, при этом отрицает:

а) совершение других, сопутствующих преступлений;

б) совершение преступления в составе ОПГ, ОПС.

Собранных по делу доказательств достаточно для установления вины подозреваемого, при этом подозреваемый признает свою вину в совершении преступления.

В ходе проведенного анкетирования 37,6 % опрошенных респондентов выделили данную ситуацию из числа наиболее типичных (Приложение 1). Ситуация, при которой собранных по делу доказательств достаточно для изобличения преступной деятельности подозреваемого и установления его вины, является примером складывающейся хорошей судебной перспективы по делу.

[269]Бердникова О. П. Ситуационная характеристика последующего этапа расследования мошенничества в сфере компьютерной информации // VII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии» : мат-лы междунар. науч.-практ. конф. Калининград, 2019. С. 122.

Наличие признательных показаний подозреваемого укрепляет позицию обвинения и является наиболее благоприятной ситуацией для всего процесса расследования.

Так, гр. М., один из всех участников преступного сообщества Lurk, признал свою вину в совершении преступлений, его дело было выделено в отдельное производство, в результате чего он был осужден в 2018 г., остальные члены ОПС – только в 2022 г.[270]

Основными задачами в данном случае являются тактически грамотное проведение следственных действий, правильное оформление всех имеющихся в деле процессуальных документов, в т. ч. оформление и представление результатов ОРД, исключающих возможность признания доказательств недопустимыми, необоснованными.

Собранных по делу доказательств достаточно для установления вины подозреваемого, при этом подозреваемый отрицает свою вину в совершении преступления.

В ходе проведенного анкетирования 33,2 % опрошенных респондентов выделили данную ситуацию из числа наиболее типичных (Приложение 1). Также как и в предыдущей ситуации, основное внимание уделяется правильности оформления доказательственной базы. Несмотря на отрицание участия в совершении преступлений виновность лиц подтверждается комплексом собранных по делу доказательств. Так, по делу Lurk, 18 из 21 обвиняемого вину в совершении преступлений не признали, при этом собранные по делу доказательства свидетельствовали об обратном. Результатами проведенных экспертиз, ПТП и других ОРМ, показаниями свидетелей, обвиняемых и другими доказательствами вина преступников была доказана. Так, только анализ переписки между членами преступного сообщества с декабря 2015 г. по май 2016 г. свидетельствовал о совершении исследуемой преступной деятельности, в частности о заражении компьютеров ООО «ТТ-Трэвел», ООО «Стройинвест», Банк «Тааттаа», ПАО «Металлинвестбанк», КБ «Гарант-Инвест», подмене платежных поручений и

[270]Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 …

совершении переводов денежных средств на подконтрольные преступникам счета. В частности такими сообщениями являлись следующие: «завтра залив»; «сегодня вечером залив», «на 200 штук залили»; «банк, откуда льем, нужно снести нашего бота, так как завтра его будет ФСБ ковырять, придумай, у люма, винса была команда на удаление бота напрямую»; «31.12.2015 года обналичил 8 миллионов рублей»; «итого залили 700 млн, на радио освещают данную тему»; указания «по поиску компа буха и его заражению», нужно «сканить, делать скрины, заражать и при этом не попасться, оставаясь незамеченными»; утвердительный ответ организатора ОПС на направленное ему платежное поручение на ООО «Полет» на сумму 478 252,65 руб. с вопросом «Грабим?»; переписка о том, что на неделе будет залив на 500 млн и распределение действий: «заражает и домен хакает «meg», сливает лаве «momon»[271].

В ситуациях, когда *подозреваемый частично признает свою вину, при этом отрицает совершение других, сопутствующих преступлений, а также участие в совершении преступления в составе ОПГ, ОПС* (20,6 и 19,4 % опрошенных респондентов соответственно выделили данные ситуации из числа наиболее типичных (Приложение 1), как и в предыдущей ситуации, внимание уделяется тщательному сбору и правильности оформления доказательственной базы. Так, по делу Lurk, трое участников преступного сообщества, гр. Р., гр. К., гр. М-к, вину признали частично: двое в обналичивании денежных средств, третий в неправомерном доступе к компьютерной информации. При этом участие в совершении сопутствующих преступлений, а также в совершении преступлений в составе ОПС отрицали, однако полученными по делу доказательствами виновность подсудимых подтверждается. В основу приговора положены полностью признательные показания гр. М., который вину признал в полном объеме, а также признательные показания других обвиняемых, данные в ходе предварительного следствия. Так, гр. М. указал на используемую в преступной деятельности квартиру, а также на участников преступного сообщества, распределение между ними преступных ролей, эпизоды совершения хищений.

[271]Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

Кроме полученных показаний виновность указанных лиц подтверждалась результатами экспертиз, перепиской в системе Jabber и электронной почте, записями с камер видеонаблюдения, телефонными переговорами и другими доказательствами. В целом при собранном комплексе изобличающих вину доказательств позиция подсудимых о полном или частичном отрицании своей причастности к совершению преступлений судом была расценена как линия поведения и способ защиты от обвинения с целью избежать ответственности или снизить ее степень[272].

Так, по делу Lurk, несмотря на отрицание некоторых участников ОПС Lurk факта знакомства друг с другом и ведения совместной преступной деятельности, обратное подтверждается записями контактов с номерами участников ОПС, обнаруженными в изъятых мобильных телефонах, сохраненными входящими и исходящими сообщениями. Так, в папках «TelegramImage» и «ViberImage» содержались фотоиллюстрации, со сведениями о юридических лицах, используемых в преступной деятельности, и о распределении денежных средств[273].

Собранных по делу доказательств недостаточно для установления вины подозреваемого.

На типичность подвидов данной ситуации указали 55 % опрошенных респондентов, из которых 26,4 % выделили ситуацию, при которой *подозреваемый отрицает свою вину,* 10,1 % – ситуацию, при которой *подозреваемый признает свою вину* и 19,7 % – ситуацию, при которой *подозреваемый частично признает свою вину* в совершении преступления (Приложение 1).

В целом ситуация, при которой собранных по уголовному делу доказательств недостаточно для изобличения виновности подозреваемого, является наиболее проблематичной для процесса расследования. В данном случае, с целью установления дополнительных источников доказательств, целесообразно

[272]Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...
[273] Там же.

проведение повторных допросов, очных ставок, проведение соответствующих экспертиз и исследований, инициирование органам дознания поручений на проведение ОРМ и т. д. Основными задачами при такой ситуации является преодоление осуществляемого подозреваемым противодействия расследованию посредством подтверждения имеющихся в деле доказательств, получения новых и опровержения позиции подозреваемого. Данные цели достигаются посредством изменения тактики проведения допросов подозреваемого, установления иных лиц, причастных к совершению преступления[274].

В ситуации, когда *подозреваемый признает свою вину в совершении основного преступления, предусмотренного ст. 159.6 УК РФ, при этом отрицает совершение других, сопутствующих преступлений,* к примеру предусмотренных гл. 28 УК РФ «Преступления в сфере компьютерной информации» (на типичность данной ситуации указали 8,6 % опрошенных респондентов (Приложение 1)), особое внимание уделяется проведению соответствующих экспертиз, заключениям и показаниям специалистов и т. д. По результатам указанных мероприятий важно совместно со специалистом тактически грамотно спланировать и провести допросы подозреваемого, в ходе которых, вероятно, будут получены признательные показания.

При отрицании совершения преступления в составе ОПГ, ОПС (на типичность данной ситуации указали 11,1 % опрошенных респондентов) (Приложение 1) необходимо обратить внимание на получение доказательственной информации относительно связи подозреваемого с другими участниками. Что может достигаться как проведением соответствующих ОРМ, к примеру, ПТП, СИТКС, наблюдение, опрос, наведение справок и т. д., так и различных следственных действий, к примеру, допрос и очная ставка.

При этом, нацеливая процесс расследования на изобличение деятельности всего преступного объединения, целесообразно, при наличии возможности, несмотря на выявленный единичный факт преступного проявления, в ходе проведения предварительной проверки, продолжать проведение соответствующих

[274]Малыхина Н. И., Кузьмина С. В. Указ. соч. С. 245.

ОРМ, вплоть до осуществления оперативного внедрения в преступное объединение. И только после установления преступной иерархии, получения сведений об основных ее членах, а главное о лидере, организаторе, его заместителях, фиксации доказательственной информации противоправной деятельности, возможно произведение соответствующих задержаний. В дальнейшем производятся допросы задержанных, обыски и другие следственные действия, направленные на установление и фиксацию доказательственной информации, а также установление остальных членов объединения, определения их ролевых функций. Как правило, для проведения такой крупномасштабной операции требуется объединение усилий различных силовых структур, а также специализирующихся организаций в различных регионах РФ и даже за ее пределами. При расследовании рассматриваемых преступлений на территории различных государств особое внимание уделяется вопросам взаимодействия с международными правоохранительными органами и организациями, специализирующимися на противодействии совершению киберпреступлений.

Итогом расследования любого преступления должно являться получение о нем наиболее достоверного знания. Одним из инструментов достижения данной цели является выдвижение и проверка на различных этапах соответствующих криминалистических версий. В целом, весь процесс расследования по большому счету является процессом выдвижения и проверки различных криминалистических версий. Полученные таким образом результаты способствуют принятию соответствующих процессуальных решений, необходимой корректировке и оптимизации процесса расследования.

Несмотря на наличие различных классификаций криминалистических версий, в данном диссертационном исследовании считаем целесообразным в качестве основополагающих и направляющих весь процесс расследования избрать типовые общие версии расследования мошенничества в сфере компьютерной информации, При определении таковых опираемся на перечень версий, относительно расследования мошенничества при получении выплат,

приведенный в своем диссертационном исследовании А. В. Чумаковым[275]. Исходя из определенных нами и взятых за основу при построении методики расследования принципов, направленных на изобличение всей структуры организованной преступной деятельности по делам о мошенничестве в сфере компьютерной информации, выявление и расследование как основного, так и сопутствующих преступлений, с учетом особенностей совершения и расследования данного вида преступной деятельности, нами выделены следующие типовые общие версии[276]:

1) отсутствует состав как основного, так и сопутствующих преступлений. Данное обстоятельство является поводом для принятия соответствующего решения об отказе в возбуждении уголовного дела;

2) мошенничество в сфере компьютерной информации совершено при обстоятельствах, указанных в заявлении, сообщении и других документах, являющихся поводами для возбуждения уголовного дела;

3) рассматриваемое деяние является единственным эпизодом совершения мошенничества в сфере компьютерной информации;

4) кроме рассматриваемого деяния имеется информация, указывающая на многоэпизодность совершенного деяния;

5) помимо основного преступления, предусмотренного ст. 159.6 УК РФ, имеются признаки совершения сопутствующих преступлений;

6) преступление имеет организованный характер и совершено группой лиц, ОПГ или ОПС.

Относительно обозначенного нами принципа преимущественного выявления «организованного» мошенничества в сфере компьютерной информации, поддерживаем позицию А. К. Щербаченко, обозначившего в данном контексте типичные исходные и другие следственные ситуации и выдвигаемые в этой связи криминалистические версии, в т. ч.:

---

[275]Чумаков А.В. Указ. соч. С. 123–124.

[276] Харина Е. А. Типовые следственные ситуации первоначального этапа расследования мошенничества в сфере компьютерной информации // Закон и право. 2023. № 12. С. 276–277.

– в ситуации задержания участников преступного объединения, выдвигаемыми версиями могут быть предположения о том, что задержаны: а) все участники мошенничества; б) не все участники мошенничества; в) участники мошенничества и невиновные лица; г) невиновные лица;

– в ситуации задержания подозреваемого и наличии достаточной информации о совершении преступления группой лиц, версии включают предположение о том, что достаточно информации о совершении мошенничества группой лиц или невиновности: а) обо всех участниках и связях; б) лишь об основных участниках; в) задержан невиновный;

– в ситуации задержания подозреваемого, когда информация о совершении преступления группой лиц носит ориентирующий характер, наиболее характерными являются предположения о: а) роли мошенника в группе; б) составе группы; в) задержании невиновного[277].

В процессе расследования, наряду с общими криминалистическими версиями, постоянно выдвигаются и проверяются различные частные версии. Такие версии выдвигаются относительно обстоятельств совершения преступления, в частности способа совершения преступления, личности преступника, используемых вредоносных компьютерных программ, компьютерных средств, размера причиненного вреда и т. д. К примеру, в случае установления номера банковского счета, на который были переведены похищенные денежные средства, относительно владельца данного счета возможно выдвижение следующих частных криминалистических версий о том, что установленное лицо: а) является исполнителем преступления; б) является соисполнителем преступления; в) является «подставным» лицом, на имя которого зарегистрирован счет, карта; г) является лицом, утратившим банковскую карту; д) является лицом, не осведомленным об операциях, производимых по счету, при

[277] Щербаченко А. К. Типичные версии о мошенничестве, совершенном группой лиц, и их место в системе базовой методики их раскрытия и расследования // Философия права. 2020. № 1(92). С. 167.

этом преступник имеет беспрепятственный доступ к осуществлению таких действий.

Проверка выдвигаемых в процессе расследования версий достигается посредством определения соответствующих оперативных мероприятий, следственных и иных действий, результатом чего является поэтапное формирование достоверной картины преступления.

3.3. Тактика производства следственных действий при расследовании мошенничества в сфере компьютерной информации

Следственные действия являются уголовно-процессуальным инструментом механизма уголовно-правового реагирования, направленным на получение различного спектра информации, позволяющей в своей совокупности сформировать наиболее полное представление относительно объекта познания.

Особенности подготовки, совершения и сокрытия преступлений рассматриваемой группы, главная из которых заключается в совершении преступления в особом информационном пространстве с оставлением соответствующей цифровой следовой картины, проявились появлением закономерных особенностей подготовки, проведения и фиксации результатов отдельных следственных действий.

Результаты анализа судебно-следственной практики, подтвержденные результатами проведенного анкетирования сотрудников правоохранительных органов, свидетельствуют о том, что наиболее типичными следственными и процессуальными действиями, проводимыми в ходе расследования мошенничества в сфере компьютерной информации, являются: осмотр места происшествия (45,9 %), допрос (81,2 %), обыск (53,4 %), выемка (63,3 %), изъятие электронных носителей информации (71,5 %), осмотр предметов (документов) (71,5 %), назначение экспертизы (67,9 %), контроль и запись переговоров (24 %), наложение ареста на имущество (30,2 %) (Приложение 1).

В рамках данного диссертационного исследования осветим тактические особенности проведения следственных действий вызывающих наибольшие вопросы правоприменителей.

Осмотр места происшествия, как правило, является первым следственным действием, соприкасающимся с событием преступления и его следовой картиной, ключевой целью которого является получение информации, способствующей установлению обстоятельств совершения преступления.

Учитывая то, что преимущественный объем доказательственной информации содержат цифровые следы, а также исходя из анализа судебно-следственной практики, указывающей на наличие у правоприменителей пробелов в области правильности и грамотности взаимодействия с ними (на что указали 19,8 % респондентов) (Приложение 1), считаем необходимым, в рамках данного диссертационного исследования, обратить внимание на способы обнаружения и изъятия данных следов. Несомненно, от тактически и технически правильно проведенной процедуры обнаружения и изъятия данных следов зависит их фиксация, сохранность и возможность представления для проведения экспертных оценок.

Условно проведение осмотра места происшествия включает в себя подготовительный, основной и заключительный этапы. Наряду с общими требованиями, подготовка к проведению рассматриваемого следственного действия, имеет ряд особенностей. Прежде всего, это касается необходимости присутствия в ходе проведения следственного действия соответствующего специалиста.

Необходимо отметить, что, согласно ч. 2 ст. 164.1 УПК РФ, электронные носители информации изымаются с участием специалиста, т. е. его участие в ходе производства следственного действия в таком случае становится обязательным. При этом законодатель не оговаривает случаи возможного отсутствия такого специалиста при изъятии электронных носителей информации, не требующих специальных познаний, например флеш-карт, магнитных дисков. Поэтому, с

учетом наличия взглядов различных ученых[278], имеющейся судебной практики, допускающей правомерность изъятия подобных предметов без участия специалиста, также считаем проведение таких действий вполне оправданным.

Также, в зависимости от характера преступления, для участия в рассматриваемом следственном действии целесообразно привлекать специалистов, «компетентных в конкретной области, связанной с компьютерными системами и технологиями: инженер-программист, специалист по сетевым технологиям (администратор вычислительных сетей), системам электросвязи (в т. ч. слаботочным системам) и др.[279]

Несмотря на то, что особая роль в ходе проведения осмотра места происшествия по исследуемым противоправным деяниям отводится грамотным действиям участвующего в мероприятии специалиста, необходимо учитывать наличие возможных технических мер противодействия. Особенно это важно при проведении следственного действия в связи с совершением высокоорганизованного преступления в сфере компьютерной информации, когда уровень подготовленности к преступлению и сокрытию его следовой картины очень высоки. Одним из вариантов такого противодействия может быть уничтожение компьютерной информации. Так, к примеру, в квартире братьев П. находилась электромагнитная пушка для размагничивания жестких дисков[280].

А. Н. Першиным, М. В. Бондаревой такой вид противодействия именуется как «техническое противодействие расследованию», как правило, планируемое еще на стадии подготовки преступления. Одними из его видов является возможность удаленного доступа к информации, ее размещение на облачных

---

[278] Андриенко Ю. А. Отдельные аспекты использования информационных технологий и работы с электронными носителями информации в доказывании по уголовным делам // Вестник Сибирского юридического института МВД России. 2018. № 3 (32). С. 99–105 ; Шигуров А. В., Подольный Н. А. Проблемы правового регулирования изъятия электронных носителей информации и копирования с них информации при производстве следственных действий // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2020. № 1 (49). С. 169–174 ; Зуев С. В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С. 58–60 ; Науменко О.А. Криминалистические аспекты исследования цифровых объектов при расследовании преступлений // Общество и право. 2023. № 3 (85). С. 76-81.

[279] Меркулова М. В. О некоторых проблемах осмотра персонального компьютера // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика : сб. ст. XVIII Междунар. науч.-практ. конф. Барнаул, 2020. С. 153–154.

[280] Братья по кибероружию ...

сервисных хранилищах, а также аренда серверов, расположенных за пределами РФ, делающая невозможной процедуру их изъятия[281].

Поэтому, с учетом вышеуказанного, на этапе подготовки следственного действия необходимо предусмотреть готовность к нейтрализации возможного противодействия. В этой связи, одним из эффективных методов «является применение средств радиоподавления, препятствующих возможности дистанционной подачи команд на уничижение (блокирование, модификацию) доказательственной информации с использованием беспроводных компьютерных сетей и сетей мобильной связи. Для целей обнаружения скрытых или замаскированных электронных носителей информации, содержащих электронные компоненты, применяются нелинейные локаторы[282].

Наряду с вышеуказанными действиями, необходимо принять меры к подготовке специальных технических средств и устройств, способствующих обнаружению и изъятию цифровых следов и их носителей. Так, целесообразно использовать «наиболее эффективные программные и аппаратные средства работы с электронной информацией, позволяющие более качественно и оперативно решать исследовательские задачи, такие как: Cellebrite UFED, MSAB XRY, «Мобильный Криминалист», Rusolut, Magnet AXIOM, Belkasoft Evidence Center, X-Ways Forensics, Elcomsoft Mobile Forensic Bundle, ACELab»[283].

Еще одной особенностью подготовки к проведению данного следственного действия по преступлениям рассматриваемой группы является рекомендация о привлечении в качестве понятых лиц, обладающих определенными познаниями в сфере компьютерной информации, понимающих суть производящихся с компьютерной техникой и компьютерной информацией манипуляций и могущих, в случае необходимости, подтвердить достоверность происходящего[284].

Итак, прибыв непосредственно на место происшествия, до начала проведения следственного действия целесообразно выполнение следующих действий: удалить посторонних лиц и организовать охрану места происшествия,

---

[281]Першин А. Н. «Техническое противодействие» расследованию преступления: понятие и содержание // Российский следователь. 2022. № 7. С. 7–11.

[282] Использование информации, содержащейся на электронных носителях … С. 69–70.

[283] Гаспарян Г. З. Указ. соч. С. 169.

[284]Васюков В. Ф. Тактические проблемы проведения осмотра места происшествия при расследовании мошенничества в сфере компьютерной информации // Право и образование. 2017. № 2. С. 106–107.

но, прежде всего, сохранить все объекты места совершения преступления в том состоянии, в каком они находятся на момент начала следственного действия[285]; «провести опрос потерпевшего, ответственных лиц и свидетелей обо всем, что могло измениться в обстановке или категории информации, подлежащей обработке [286] ; «подготовить необходимую компьютерную технику (ноутбук, лазерные диски, флеш-накопители), программное обеспечение, с помощью которой будет произведено считывание и хранение изъятой информации, а также произвести инструктаж для членов следственно-оперативной группы»[287].

Приступая к проведению следственного действия необходимо точно определить границы места происшествия, уточнить расположение проложенных локальных сетей, компьютеров и (или) другого оборудования и средств, относящихся к совершенному преступлению, что позволит установить места хранения носителей информации[288].

При проведении основной части осмотра места происшествия используется тактический прием «от центра – к периферии», где «центром» являются компьютерно-технические средства[289].

Особое внимание уделяется осмотру рабочей поверхности места расположения компьютерного средства с целью установления криминалистически важной информации зафиксированной на различных носителях. Такими сведениями могут быть данные логинов, паролей, учетных записей и т. д.

Большая часть времени в ходе проведения осмотра места происшествия по делам рассматриваемой группы отводится *выемке*, в ходе которой производится осмотр и изъятие электронных носителей информации.

По общему правилу *изъятию* подлежат все носители цифровых следов, имеющие отношение к совершению преступления. При этом, как верно также

---

[285] Шевченко Е. С. Указ. соч. С. 105.

[286] Мазуров И. Е. Методика расследования хищений, совершаемых с использованием интернет-технологий : дис. … канд. юрид. наук. Казань, 2017. С. 73.

[287] Кузьмин М. Н., Пахомова Е. В. К вопросу проведения тактики следственных действий по уголовным делам, связанным с мошенничеством в сфере компьютерной информации // Юристъ-Правоведъ. 2022. № 3 (102). С. 70.

[288] Шевченко Е. С. Указ. соч. С. 106.

[289] Мазуров И. Е. Указ. соч. С. 72–73.

отмечает А. Н. Першин, в случаях отсутствия такой возможности, осмотр и изучение таких носителей производятся на месте его обнаружения[290].

В ходе диссертационного исследования установлено, что в ходе раскрытия и расследования рассматриваемых преступлений наиболее часто изымались следующие носители цифровых следов: смартфоны, сотовые телефоны (на что указало 84,3 % респондентов), системные блоки персональных компьютеров, мониторы и другие периферийные устройства (68,4 %), ноутбуки, планшеты, цифровые блокноты (66,4 %), жесткие диски (57,3 %), USB-накопители, компакт-диски, карты памяти и другие накопители информации (58 %), модемы, серверы (30 %) (Приложение 1).

В связи с этим И. Е. Мазуровым определены следующие позиции, которых следует придерживаться при изъятии электронных носителей информации, в т. ч.:

– акцентировать внимание понятых на действиях специалиста;

– выемка работающих компьютерных и технических средств допускается после: остановки выполнения операции, закрытия исполняемых программ; записи информации, сохраненной в оперативной памяти;

– изъятые компьютерные и технические средства опечатываются с исключением возможности работы с ними;

– изъятые машинные носители информации (далее – МНИ) упаковываются в пакет из фольги, опечатываются и с описью вложения помещаются в алюминиевый контейнер, исключающий воздействие электромагнитных, магнитных полей и направленных излучений;

– запрещается приклеивание к МНИ и документам посторонних предметов, использовать для скрепления степлер, твердые остроконечные предметы, пользоваться пластилиновыми печатями;

– изъятые принтеры и их расходные материалы упаковываются в отдельную тару;

[290] Першин А. Н. Осмотр сетевых информационных ресурсов – новый вид следственного действия? // Российский следователь. 2020. № 1. С. 13–16.

– в случае необходимости производится копирование информации на МНИ, отличительные признаки которого вносятся в протокол с видеофиксацией происходящего;

– отличительные признаки изымаемого отражаются в протоколе осмотра места происшествия[291].

Другими авторами также указываются специфические особенности работы по изъятию электронных носителей информации:

– в случае изъятия видеорегистраторов не рекомендуется извлекать из них накопитель информации; в случае изъятия сервера, изымается полностью его системный блок; не извлекать из изымаемого телефона SIM-карты, карты памяти; при изъятии смартфона, синхронизированного с компьютером или ноутбуком, целесообразно также изъятие и данных компьютерных средств[292];

– наиболее оптимальным способом упаковки носителей информации является помещение изъятого компьютерного средства целиком в жесткую опечатываемую коробку, которую вместе с листом с описанием упакованных носителей необходимо положить в полиэтиленовый пакет и герметично заклеить[293].

Установленные и изъятые в ходе проведения осмотра следы преступления являются объектами назначения различных видов экспертиз.

В ходе проведения осмотра места происшествия, особое внимание, кроме установления, осмотра и изъятия компьютерных и технических средств, также уделяется установлению, осмотру, истребованию и изъятию различного рода документов и других предметов. К примеру, такими документами, могут быть должностная инструкция, трудовой договор (при совершении хищения сотрудником организации), документы, свидетельствующие об оказании услуг подключения к сети провайдером, об открытии банковского счета, электронного

---

[291] Мазуров И. Е. Указ. соч. С. 76–81.

[292] Перякина М. П., Унжакова С. В., Шишкина Н. Э. Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства // Сибирский юридический вестник. 2014. № 3 (86). С. 83–84.

[293] Ростовцев А. В., Кокорев Р. А., Берестенко Е. Д. Электронные носители информации в уголовном судопроизводстве : учеб. пособие. Старотеряево, 2021. С. 45.

кошелька, расходные накладные, документально подтвержденные сведения о произведенных движениях денежных средств и совершении финансовых операций и другие документы, содержащие следы преступления.

Как уже отмечалось, одним из мощных будущих доказательственных аргументов могут служить записи с камер видеонаблюдения, поэтому в ходе осмотра места происшествия на установление видеозаписывающих устройств следует обратить особое внимание.

Указанный порядок проведения осмотра места происшествия, как правило, характерен при совершении хищения денежных средств у юридических лиц, а также когда известен исполнитель преступления и место непосредственного осуществления объективной стороны преступного деяния. В случае же совершения дистанционного хищения у физических лиц, когда, преимущественно, отсутствует какая-либо информация относительно виновного лица, особое внимание уделяется осмотру компьютерных устройств, сотовых телефонов или других объектов, неправомерным воздействием на которые совершено хищение.

При проведении рассматриваемого следственного действия также целесообразно проведение фото- и видеосъемки, позволяющей зафиксировать как общую обстановку места происшествия, так и отдельные ее элементы сосредоточения и концентрации объектов, являющихся носителями следов преступления.

Все криминалистически важные сведения и ход проведения осмотра фиксируются в протоколе осмотра места происшествия по общему правилу. При этом необходимо отражать сведения об использованных специальных устройствах, производимых действиях специалиста, «о принадлежности изымаемых носителей информации конкретному лицу», об уникальных контрольных суммах (хэш-суммах) интересующих следствие файлов[294].

С учетом специфики рассматриваемой группы преступлений, более пристальное внимание обратим на особенности *осмотра предметов,* а именно,

[294] Гаспарян Г. З. Указ. соч. С. 179.

носителей цифровых следов. Проведение данного следственного действия также условно подразделяется на три этапа. На стадии подготовки также решается вопрос привлечения специалиста, участии понятых.

Рабочая стадия заключается в непосредственном осуществлении следственного действия. В связи с имеющимся в настоящее время многообразием электронных носителей информации и различием в осуществляемых ими функциях осмотр данных предметов также может иметь некоторые специфические особенности.

Итак, при включенном и не заблокированном компьютерном устройстве необходимо включить «режим полета» и отключить блокировку экрана.

Далее необходимо установить идентификационные признаки осматриваемого устройства: IMEI (наиболее простым способом определения IMEI, серийного номера, ICCID является набор на клавиатуре команды – *#06#), телефонный номер SIM-карты, IMSI, MAC-адрес, IP-адрес, операционной системы (просмотр данных сведений станет возможным при проходе по следующему пути – Настройки/О телефоне/Все параметры/Общая информация). При дальнейшем осмотре устройства посредством просмотра различных приложений устанавливаются список контактов его владельца (который можно сохранить на персональный компьютер и распечатать), сведения о всех вызовах и сообщениях (в протоколе указываются время начала, окончания разговоров, содержание сообщений). Также целесообразно отображать сведения о передвижении устройства за необходимый период времени, геопозиционные сведения произведенных фотоснимков, истории посещения веб-страниц, об установленных приложениях социальных сетей («Одноклассники», «ВКонтакте» и т. д.). Практика показывает, что преимущественное общение лиц противоправной направленности осуществляется с использованием различных мессенджеров, таких как Telegram, WhatsApp, Viber и др. Такие приложения обладают информацией о контактах, звонках, сообщениях, фотографиях, видеозаписях, маршрутах передвижения фигуранта. При этом целесообразно принятие мер противодействия уничтожению имеющейся переписки посредством

установления соответствующего таймера. Так, к примеру, с этой целью в популярном приложении Telegram «необходимо изменить настройки–закладка–Setself–destructtimer – с периода времени на off 1». В целом, информация, находящаяся на осматриваемом устройстве должна быть сохранена на внешних носителях, к примеру, с помощью такой программы как «Мобильный криминалист», программно-аппаратного комплекса UFED. При составлении протокола указываются сведения обо всех обнаруженных и изъятых объектах, в т. ч. электронных носителях информации, возможно оформление схемы их обнаружения, изготовление фотоснимков[295].

На заключительном этапе следственного действия, как правило, используются два способа фиксации проведенного осмотра электронных носителей информации: посредством вставления в описательную часть протокола снимков экрана, поэтапно сделанных с помощью функции Print Screen; посредством текстового описания производимого осмотра с размещением соответствующих изображений в приложении к протоколу. Наиболее приемлемой является тактика осмотра, при которой указывается путь к установленной информации с последующим размещением соответствующего изображения[296].

Так, по делу Lurk, в результате осмотра изъятых предметов, специалистом в сфере информационной безопасности АО «Лаборатория Касперского» проверены банковские карты «БАНК24РУ», установлено, что на картах перезаписана магнитная полоса, что используется для активации вредоносной программы Backdoor.Win32.Skimer на инфицированных банкоматах. На осмотренной флеш-карте содержится список лиц, на чьи имена оформлены банковские счета, а также исполняемый файл, который является генератором ключей вышеуказанной программы. На изъятом компьютере, в каталоге с наименованием, содержащим слово Ялта, находились фотографии участников ОПС, в т. ч. фотография с выложенным из камней текстом «LUM Крым ждет тебя»[297].

---

[295] Использование информации, содержащейся на электронных носителях ... С. 80–96.
[296] Там же. С. 70–74.
[297] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

В ходе осмотра, изъятия носителей цифровых следов следует избегать типичных ошибочных действий, в т. ч. отсутствия отражения в протоколе действий, могущих повлечь модификацию компьютерной информации. Так, «открытие и просмотр файлов модифицируют служебную и иную информацию на электронном носителе информации, что в дальнейшем не позволяет произвести повторную экспертизу, так как становится невозможным восстановление ранее существовавших удаленных файлов»[298].

Еще одним наиболее распространенным следственным действием при расследовании рассматриваемых преступлений является *обыск.*

Учитывая то обстоятельство, что наибольшей информативностью по исследуемым преступлениям обладают цифровые следы, а также с учетом существующей возможности их уничтожения за считанные секунды, решение о проведении обыска, отыскании следов, их фиксации и изъятии должно приниматься взвешенно и при этом незамедлительно. Так, 39,4 % опрошенных сотрудников отметили несвоевременность проведения неотложных следственных действий в качестве допускаемых типичных ошибок проведения расследования.

Как и проведение других следственных действий, проведение обыска включает в себя подготовительный, рабочий и заключительный этапы.

Мероприятия, проводимые на этапе подготовки к обыску, схожи с мероприятиями, проводимыми на этапе подготовки к осмотру места происшествия, при этом, к ним также относится выбор наиболее рационального времени проведения следственного действия, составление плана проведения, определения способа проникновения в обыскиваемое помещение и обеспечение мер внезапности проведения обыска и безопасности его участников[299].

Особенно обеспечение вышеуказанных мер безопасности необходимо при проведении обыска в отношении пресечения деятельности «организованного» мошенничества в сфере компьютерной информации. В частности в отношении

---

[298] Иванов П. О. Использование специальных компьютерных знаний при расследовании преступлений: проблемные вопросы подготовки экспертов // Закон и общество: история, проблемы, перспективы : мат-лы XXVI Межвуз. междунар. науч.-практ. конф. студентов и аспирантов, посвящ. 70-летию Красноярского ГАУ. Красноярск, 2022. С. 293.

[299] Соколов А. Б. Организационно-тактическая деятельность следователя на подготовительном этапе проведения обыска // Криминалистика: вчера, сегодня, завтра. 2021. № 4(20). С. 81–82.

членов преступного объединения обыск целесообразно проводить одновременно. Так, 18 мая 2016 г. одновременно в 15 регионах РФ произошло задержание порядка пятидесяти лиц, подозреваемых в причастности к деятельности преступного сообщества Lurk. Одновременно с задержанием производились обыски, принудительный доступ в помещения организовывали вооруженные сотрудники ФСБ, МЧС России. В ходе обыска кроме других предметов были изъяты пистолеты, автоматы и боеприпасы к ним[300].

При этом целесообразно использование следующих рекомендаций: провести опрос присутствующих при следственном действии в целях добровольной выдачи носимых электронных носителей информации, мобильных устройств; ограничить доступ к имеющимся электронным носителям информации; проверить мониторы, модемы, другие устройства на наличие слотов для карт памяти; тщательно изучить брелоки, сумки, барсетки, часы присутствующих в помещении, где проводится следственное действие; в случае проведения следственного действия в жилом помещении необходимо исследовать смарт-технику, телевизоры и любые персональные электронные устройства; изучению подлежат рабочая поверхность рабочих столов для обнаружения имен пользователей, паролей и учетных записей электронной почты[301].

Соответствующие сведения о логинах, паролях могут быть получены и от самих подозреваемых. Так, по делу Lurk, один из участников преступного сообщества в ходе проведения у него обыска сообщил пароль для входа в учетную запись пользователя. Во время проведения следственного действия необходимо контролировать действия подозреваемых. Так, в ходе обыска, один из членов ОПС Lurk выкинул с балкона флеш-карту, которая была найдена, изъята и осмотрена[302].

Наряду с обнаружением и изъятием цифровых следов немаловажными задачами в ходе проведения обыска является установление других материальных следов: различных документов (банковских договоров, счетов, платежных

[300] Антоненков Д. Указ. соч.
[301] Использование информации, содержащейся на электронных носителях … С. 69.
[302] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

поручений, договоров об оказании услуг связи, интернет-соединений, инструкций к техническим средствам и устройствам, документов, удостоверяющие личность (в т. ч. имеющие признаки подделки), договоров аренды, свидетельства о регистрации движимого и недвижимого имущества и т. д.), записных книжек, отдельных листов с записями, содержащих криминалистически важную информацию), следов пальцев рук и т. д. В ходе проведения обыска также подлежат установлению и изъятию денежные средства, дорогостоящие предметы и элементы роскоши (ювелирные украшения, драгоценности, часы и т. д.), могущие служить обеспечением гражданских исков.

Так, по делу Lurk в ходе обыска в одном из помещений изъяты в большом количестве USB-накопители, CD-диски, ноутбуки, комплекты тарифных пакетов SIM-карт оператора сотовой связи «МТС» в количестве 278 шт., «Билайн» в количестве 244 шт., «Мегафон» в количестве 8 шт., печати организаций, денежные средства в размере 27 010 руб., пластиковые карты «Банк24.ру» в количестве 221 шт., открытые на физических лиц, и банковские чеки о высылке одноразовых паролей и иных банковских операций, роутеры, более 60 шт. мобильных телефонов, 6 чеков на единоразовую покупку в АО «Связной Логистик» в большом количестве телефонов, платежные поручения, трудовые договоры. В ходе обыска в другом помещении были изъяты ожерелья, серьги, кольца, цепи, кулон, браслеты; ручные часы, шкатулки, монеты, статуэтка, кошелек, сертификаты, бумажные бирки, кассовые и товарные чеки на вышеуказанные ювелирные изделия, денежные средства[303].

Несомненно, одним из ключевых следственных действий, требующим высокой степени сосредоточения и мобилизации потенциала следователя (дознавателя), является проведение *допроса*.

Идеальным результатом грамотно спланированных и проведенных допросов должно явиться получение правдивых показаний, гарантированной доказательственной базы изобличения преступной деятельности подозреваемого,

[303] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

позволяющей сформировать хорошую судебную перспективу по уголовному делу и реализовать принципы уголовно-правового воздействия.

Наряду с тактическими приемами, применяемыми при проведении допросов по любому из уголовных дел, несомненно, тактика подготовки и проведения допроса в ходе расследования мошенничества в сфере компьютерной информации, в силу специфичности способов совершения и сокрытия преступлений, имеет свои специфические отличия.

Итак, проведение данного следственного действия начинается с тщательной подготовки к его проведению.

В подготовительную часть проведения допроса по делам о совершении мошенничества в сфере компьютерной информации, как правило, входят следующие действия:

– получение специальных знаний посредством консультирования со специалистами. В ходе таких консультаций лицом, производящим расследование могут быть получены сведения относительно используемой специальной терминологии, о механизме действия ВПО, об оставленных в ходе совершения преступления цифровых следах и т. д. Кроме того, в зависимости от технической сложности совершения преступления, целесообразно присутствие такого специалиста непосредственно во время допроса. Так, присутствующий на допросе специалист, выслушав показания допрашиваемого, с учетом имеющихся у него познаний, может установить наличие существенных расхождений между повествуемой подозреваемым (обвиняемым) информацией и характером следовой картины совершенного преступления. Наряду с вышеуказанными, в качестве специалистов могут выступать лица, обладающие познаниями в других областях, например, в финансово-кредитной сфере;

– в случае совершения хищения у юридического лица производится ознакомление со спецификой его деятельности, в частности с организацией рабочего процесса, при осуществлении которого совершено хищение; организацией информационной защиты и т. д. С этой целью может производиться ознакомление с должностными инструкциями сотрудников, правилами

внутреннего трудового распорядка, результатами произведенных ревизий и другими документами организационного и финансового характера;

– доскональное ознакомление следователя со всеми материалами дела[304]. Данные мероприятия проводятся для уточнения и систематизации всех показаний потерпевших, свидетелей, результатов проведенных осмотров, исследований, заключений и других следственных действий и оперативных мероприятий, ознакомление с результатами направленных запросов, полученными выписками, справками, результатами проведенных ОРМ, с целью определения имеющейся к данному моменту доказательственной базы, наличия возможных противоречий в показаниях, несоответствия со следовой картине и т. д.;

– подготовка вопросов, определение их правильной последовательности, минимизирующей возможность подозреваемого дачи ложных показаний. Целесообразно такую подготовку осуществлять совместно со специалистом в сфере компьютерной информации, в частности это касается определения вопросов относительно технической части способа преступления, использованного ВПО, компьютерных устройств, технических средств и т. д.

– ознакомление с личностью подозреваемого. С этой целью в отношении лиц, проходящих обучение, необходимо ознакомиться с характеристикой по месту учебы и месту жительства; в отношении работающих лиц ознакомление также производится с личным делом, анкетой и возможными результатами прохождения конкурсных испытаний и других проверок при трудоустройстве на работу, сведениями об образовании, перемещении по должностям, прежним местам работы. Проводится сбор сведений в отношении подозреваемого по имеющимся информационно-справочным учетам, в т. ч. о привлечении к уголовной, административной ответственности, о зарегистрированных объектах недвижимого имущества, автотранспортных средствах, SIM-картах, банковских счетах, электронных кошельках, регистрации в качестве индивидуального предпринимателя, участии в деятельности юридических лиц. В качестве сведений о ранее судимых лицах, могут быть использованы данные, полученные при

[304] Мазуров И. Е. Указ. соч. С. 97.

изучении архивных дел; в отношении лиц, отбывавших наказание в виде лишения свободы, такими сведениями могут быть характеризующие материалы из учреждений уголовно-исполнительной системы. Целесообразно установление и изучение страниц подозреваемого, зарегистрированных на различных сайтах сети Интернет. Также возможно изучение истории и характера общения в используемых фигурантом мессенджерах. Так, к примеру, даже удаленные приложения Telegram и Viber оставляют на компьютере информацию, позволяющую восстановить данные сведения[305].

В параграфе 2.3. нами приведена классификация личностей типичных преступников рассматриваемой группы преступлений, дана их подробная характеристика. С учетом выявленной степени организованности совершенного преступления, способа его совершения и оставленных следов, можно определить к какой из указанных групп типичных преступников относится подозреваемый (обвиняемый). Ознакомившись с приведенным описанием можно уяснить некоторые особенности характеристики и способа мышления таких преступников.

Как справедливо отмечают авторы учебника, «успех допроса зависит от того, насколько полно следователь учтет и использует – для установления психологического контакта – особенности личности допрашиваемого: его психики, культурного и образовательного уровня, профессии, мировоззрения и т. п.»[306].

Поэтому, учитывая данную различным группам преступников характеристику степени осознанности и образа мышления, процесс подготовки и само проведение допроса могут существенно отличаться.

Так, подготовка к проведению следственного действия в отношении высококвалифицированного преступника, обладающего незаурядными способностями разработки вредоносных компьютерных программ высочайшего класса и способов сокрытия компьютерных преступлений будут отличаться от подготовки к проведению допроса в отношении «бытового», «случайного» преступника.

---

[305] Исследование остаточных артефактов Viber и Telegram в операционной системе Windows / А. И. Бородин [и др.] // Бизнес-информатика. 2019. Т. 13, № 4. С. 39–48.

[306] Криминалистика. М., 2010. С. 576.

Очевидно, что в первом случае такой этап потребует от лица, производящего допрос, вложения несравнимо больших усилий, прежде всего обязательного получения консультаций специалистов в сфере компьютерной информации. Кроме того, с учетом логического склада ума, умения такими преступниками анализировать и охватывать сознанием всю происходящую ситуацию и просчитывать варианты ее развития, к специфике построения вопросов, их очередности, «демонстрации осведомленности о деталях преступления» [307] , с учетом имеющихся доказательств и нацеленности на изобличении каких-либо противоречий или лжи, также следует отнестись более внимательно. При этом целесообразно, составить план проведения следственного действия с определением основных указанных позиций.

Хотя, учитывая саму суть отношений подозреваемого, обвиняемого с лицом, производящим расследование, то можно отметить, что преимущественное большинство таких отношений потенциально являются конфликтными, либо напряженными, поскольку основаны на уголовно-правовом воздействии одного на другого.

Действительно, при проведении вербальных следственных действий, особенно допроса подозреваемого, обвиняемого, установление психологического контакта имеет ключевое значение, особенно, при ожидаемом противодействии.

И в данном случае результаты изучения личности подозреваемого, обвиняемого являются решающими в избрании тактики установления такого контакта. Так, в случае совершения преступления «бытовым», «случайным» преступником, тем более при совершении преступления впервые, целесообразно установление благоприятного психологического контакта, посредством проявления следователем своего рода заботы о судьбе подозреваемого, сопереживания о случившемся и заинтересованности в минимизации меры уголовно-правовой реакции на совершенное преступление. В данном контексте на лицо, производящее расследование возлагается большая ответственность, как на человека, от степени грамотности распоряжения властными полномочиями

[307] Криминалистика. М., 2010. С. 576.

которого, может зависеть будущая судьба человека. Проявленное таким образом мастерство и мудрость следователя способны убедить человека в раскаянии, даче признательных показаний и планировании будущей жизни исключительно в правовом поле, не прибегая при этом к проявлению каких-либо элементов противоправного поведения. Очень важно проведение такой работы с молодыми преступниками, которые, нередко, получили специальные познания в ИТТ являясь студентами профильных кафедр учебных заведений различного уровня. Разъяснения о потребности и необходимости применения имеющихся у них познаний, не прибегая к нарушению уголовно-правовой границы дозволенного, с учетом происходящих изменений, способны побудить к внесению такими лицами существенного неоценимого вклада в развитие государства и общества в целом.

Совсем иначе обстоит дело с установлением психологического контакта с допрашиваемыми, имеющими устоявшиеся убеждения противоправной направленности, не склонными к раскаянию и активно противодействующие расследованию.

В данной ситуации определенное психологическое преимущество в случае нахождения подозреваемого под стражей может быть получено в результате возможного появления страха быть осужденным к наказанию в виде лишения свободы, что, вероятно, будет способствовать изменению занятой им противодействующей позиции.

Еще одним тактическим инструментом получения правдивых показаний допрашиваемого является предъявление полученных доказательств, изобличающих или указывающих на его виновность. Так, в зависимости от способа преступления, уровня профессиональной подготовленности, классности используемых вредоносных программ, очевидность цифровых следов может быть различной.

При этом, даже несмотря на наличие незначительного объема цифровых следов в результате использования высококачественного ВПО, поэтапное предъявление допрашиваемому других видов полученных доказательств, может

выявить наличие существенных противоречий в даваемых показаниях, убедить в разоблачении преступной деятельности и склонить к даче правдивых показаний.

Учитывая нацеленность настоящей методики на изобличении «организованного» мошенничества в сфере компьютерной информации, тактическим приемом допроса подозреваемых, обвиняемых, является убеждение в даче признательных показаний другими членами преступного объединения относительно самого допрашиваемого и деятельности преступного формирования.

Так, в случае установления с допрашиваемым благоприятного психологического контакта, намерения последнего к даче правдивых показаний, задача лица, производящего допрос, заключается в выяснении и фиксации всех обстоятельств произошедшего.

К примеру, при допросе исполнителя, выясняется каким образом он стал членом преступного формирования, что входило в круг его обязанностей, кто курировал его деятельность, что ему известно об остальных членах объединения, в случае осуществления конспиративного общения и отсутствии у конкретных исполнителей осведомленности о членах объединения, занимающих руководящие функции, выясняются все детали такого общения: посредством каких средств связи, мессенджеров, телефонных номеров, электронных почт, при неосведомленности об установочных данных остальных членов объединения, выясняется какие использовались «ники», каким образом исполнитель получал задания и денежные средства за их исполнение и т. д.

Большего внимания требует допрос организатора и лиц, выполняющих в объединении руководящие функции. В большинстве случаев такие допросы проходят в ситуации противодействия расследованию: полного или частичного отказа от дачи показаний, дачи ложных показаний. Нами уже отмечалось, что в силу обладания определенными, а подчас незаурядными способностями в сфере ИТТ, такие специалисты убеждены в своей исключительности и неизобличаемости осуществляемой им преступной деятельности. Наиболее эффективными при осуществлении допроса является использование следующих тактических приемов и комбинаций:

– разъяснения преимущества способствования расследованию и дачи признательных показаний;

– акцентирование внимания на «гениальности» написанной вредоносной компьютерной программы, высоком уровне организации преступного объединения;

– «использование антипатии, питаемой допрашиваемым к кому-либо их соучастников»[308];

– сообщение о том, что другие члены объединения уже дали признательные показания в отношении допрашиваемого и деятельности преступного объединения в целом;

– поэтапное предъявление доказательств преступной деятельности допрашиваемого с демонстрацией наличия противоречий в показаниях допрашиваемого;

– «использование фактора внезапности путем постановки неожиданных вопросов в ситуации, когда допрашиваемый таких вопросов не ждет»[309];

– «использование противоречий между интересами соучастников»[310];

– постановка дополнительных вопросов, способных проявить наличие противоречий в показаниях или изобличить во лжи.

В целом совокупность приемов логического и эмоционального воздействия, а также тактических комбинаций посредством воздействия на волевую мобилизацию допрашиваемого[311] способствуют созданию благоприятных условий получения правдивых показаний допрашиваемого.

Эмоциональное состояние и внешний вид лица, производящего допрос должны излучать и демонстрировать абсолютную уверенность в наличии достаточных доказательств изобличения преступной деятельности допрашиваемого и неотвратимости последующего наказания.

На повторных допросах, с учетом сложившейся ситуации, указанные приемы применяются по мере целесообразности. «При этом важно избрать

---

[308] Криминалистика. М., 2010. С. 589.
[309] Там же.
[310] Там же. С 586.
[311] Ахмедшин Р. Л. Тактика коммуникативных следственных действий. Томск, 2014. С. 147.

наступательную стратегию, построенную на имеющихся в материалах дела опровержениях доводов подозреваемого, несостоятельности избранной им позиции»[312].

В настоящее время, ряд авторов[313] указывают на возможность использования в ходе допроса таких методов как профайлинг[314] и верификация[315]. Несомненно, все это в той или иной мере может способствовать установлению степени правдивости показаний и достижению целей допроса. Видится, что наиболее информативным в данном контексте будет выяснение необходимой информации посредством проведения инструментального психофизиологического опроса. Сама процедура проведения данного мероприятия является крайне нетипичной для допрашиваемого и с учетом имеющегося в социуме стереотипа неизбежности изобличения во лжи, может способствовать получению достоверных показаний.

Как известно, сам допрос условно подразделяется на первоначальную стадию, в ходе которой заполняется анкетная часть протокола следственного действия, основную, в ходе которой допрашиваемый повествует о произошедшем и отвечает на поставленные вопросы и заключительную, на которой происходит оформление результатов проведенного допроса.

Видится, что проведение допросов потерпевших не вызывает каких-либо затруднений и сводится к получению наиболее полной информации о событии преступления. Наряду с этим, с учетом специфики совершения преступлений рассматриваемой группы, целесообразно выяснение следующих позиций: посредством неправомерного воздействия на какое компьютерное средство было совершено преступление; как были выявлены признаки совершения преступления; какие события или действия с компьютерными средствами

---

[312] Тагиров Р.А. Первоначальный этап расследования мошенничества в сфере кредитования: дис. … канд. юрид. наук. Уфа, 2022. С. 178.

[313] Голятина С. М. Указ. соч. С. 135–140 ; Мадянов А.В. Использование методов профайлинга и верификации в ходе предварительного расследования / А. В. Мадянов, Н. Ю. Васильева, С. Н. Болховитина // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 329–333.

[314] Профайлинг – совокупность психологических методов оценки и прогнозирования поведения человека на основе анализа наиболее информативных частных признаков: характеристик внешности, вербального и невербального поведения, вегетатики. URL: https://ru.wikipedia.org/wiki/Профайлинг (дата обращения: 01.02.2023).

[315] Верификация – процедура проверки истинности знаний. URL: https://ru.wikipedia.org/wiki/Верификация (дата обращения: 01.02.2023).

предшествовали совершению преступления (к примеру, получал ли потерпевший письма по электронной почте, скачивал, обновлял ли приложения); кто еще может пользоваться компьютерным устройством; установлено ли антивирусное программное обеспечение; с каким Интернет-провайдером заключен договор об оказании услуг; сохранены ли сведения о логинах, паролях на компьютерном устройстве; имеются ли сведения о лице, совершившем преступление и т. д.

В случае совершения преступления в отношении юридического лица помимо установления общих вопросов, касающихся его организационно-правовой формы, видах деятельности, правилах внутреннего трудового распорядка, выясняются сведения о способе организации информационной безопасности, лицах, имеющих право доступа к соответствующей компьютерной информации, и лицах, ответственных за обеспечение информационной безопасности, установленных способах прохождения процедуры аутентификации при обращении с компьютерной информацией, установлено ли антивирусное программное обеспечение, предшествовавших совершению преступления возможных обстоятельствах некорректной работы компьютерных устройств, обнаружения признаков совершения преступления, размере причиненного ущерба, проведенных ревизиях и т. д.

Как правило, основная часть допроса начинается с выяснения уровня специальных познаний в сфере компьютерной информации, наличия соответствующего образования, подготовленности. Далее выясняются сведения о подготовке, способе совершения и сокрытия преступления: когда сформировался умысел на совершение хищения; какие компьютерные, технические и специальные средства использованы для совершения преступления; способы приискания указанных средств и предметов; какое ВПО использовано при совершении преступления; используемая вредоносная компьютерная программа была написана самостоятельно или приобретена (где, у кого, при каких обстоятельствах); в случае использования готовой вредоносной программы, была ли осуществлена ее модификация; когда и каким способом была установлена вредоносная компьютерная программа на компьютерное устройство

потерпевшего (и, возможно, на компьютерные устройства других лиц); с каких компьютерных устройств производился несанкционированный доступ; какие компьютерные устройства, технические средства использовались для совершения преступной деятельности; на какие счета, банковские карты, электронные кошельки были переведены похищенные денежные средства, на кого они зарегистрированы; когда, где и кем были обналичены данные денежные средства; если преступление совершено с использованием логина и пароля других лиц, каким образом были получены сведения о них; способствовал ли совершению преступления кто-либо из сотрудников юридического лица; преступление совершено единолично, группой лиц, ОПГ или ОПС.

В случае обладания информацией об «организованном» совершении преступления наряду с другими позициями выясняется: кем, когда были приисканы соисполнители преступления; сведения о количестве, структуре, ролевых функциях участников формирования; местах нахождения компьютерных устройств, технических средств, написания соответствующих компьютерных программ, используемых для совершения преступлений, сведения о юридических, физических лицах, в отношении которых совершались преступления, какие средства связи использовались для общения между участниками объединения; где находятся похищенные денежные средства; каким образом приобретались предметы, используемые для совершения преступлений, к примеру, незарегистрированные SIM-карты и т. д.

Как показывает анализ следственно-судебной практики, при расследовании «организованного» мошенничества в сфере компьютерной информации не приходится надеяться на стремление участников объединения к даче признательных показаний и сотрудничеству со следствием. Так, при проведении расследования в отношении 22 подозреваемых по делу Lurk, только один из них стал давать правдивые показания, заключил досудебное соглашение и был

осужден в 2018 г., тогда как расследование в отношении остальных членов сообщества продолжалось, после чего они были осуждены только в 2022 г.[316]

3.4. Использование специальных знаний при расследовании мошенничества в сфере компьютерной информации

Успешность проведения расследования уголовного дела зависит в том числе от своевременности, квалифицированности применения специальных знаний, особую актуальность данное обстоятельство приобретает в связи с расследованием преступлений в сфере компьютерной информации.

Специфика подготовки, совершения и сокрытия мошенничества в сфере компьютерной информации неминуемо указывает на безоружность выявления, раскрытия и расследования рассматриваемых преступлений без использования специальных знаний.

Как уже отмечалось, механизм образования цифровых следов, содержащих преимущественный объем доказательственной базы по таким делам, нераспознаваем обыденным сознанием, в связи с чем процесс их установления и познания требует обладания соответствующими знаниями и навыками, именуемыми в уголовно-правовом поле «специальными знаниями». Все это побуждает, а в ряде случаев и обязывает, к необходимости использования данного инструмента.

В связи с отсутствием законодательного закрепления понятия «специальные знания» считаем верной и придерживаемся формулировки, данной в данном контексте Е. Р. Россинской, в соответствии с которой специальные знания – это система теоретических знаний и практических навыков в области конкретной науки либо техники, искусства, ремесла, приобретаемых путем специальной подготовки и профессионального опыта и необходимых для решения вопросов,

[316] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

возникающих в процессе уголовного, гражданского, административного судопроизводства[317].

Несмотря на многообразие знаний, с необходимостью применения которых может столкнуться следователь (дознаватель) в ходе проведения расследования и нисколько не преуменьшая их значимость, учитывая специфику рассматриваемой преступной деятельности, в настоящем диссертационном исследовании акцент будет сделан на использовании таких познаний применительно к сфере информационных технологий.

Как известно, выделяют процессуальные (регламентируемые уголовно-процессуальными нормами) и непроцессуальные (регламентируются нормами административного права) формы использования специальных знаний. К первой относится: участие специалистов при производстве следственных действий, производство судебных экспертиз, заключения специалиста. Во вторую группу входят: предварительное исследование, консультации со специалистами, проведение проверок, ревизий и других проверочных действий[318].

Формами применения специальных знаний в ходе расследования рассматриваемых преступлений является как привлечение специалистов, экспертов, так и самостоятельное применение специальных знаний лицами, производящими расследование (дознание).

Так, современный уровень подготовки юристов, предполагает получение определенных познаний в сфере компьютерной информации, позволяющий лицам, ставшим следователями (дознавателями), оперативными сотрудниками производить ряд как процессуальных, так и непроцессуальных, действий, требующих таких познаний, самостоятельно. Кроме того, соответствующими познаниями обладают сотрудники специально созданных подразделений по борьбе с киберпреступлениями. При этом постоянное усовершенствование инструментов компьютерных технологий приводит к усилению степени их

---

[317] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. 4-е изд., доп. М., 2018. С. 9.

[318] Зеленский В. Д. О процессуальных и организационных формах использования специальных знаний в расследовании // Общество и право. 2012. № 1 (38). С. 211.

защиты и противодействия, преодоление которых под силу только лицу, обладающему соответствующими познаниями. Тем более данное обстоятельство касается технических средств и компьютерных устройств, которыми оперируют представители «организованного» мошенничества в сфере компьютерной информации.

Так, 22,9 % опрошенных сотрудников, в качестве имеющихся трудностей при расследовании таких преступлений указали отсутствие специальных познаний и должной квалификации лиц, производящих выявление, раскрытие, расследование преступления, при этом 19,5 % опрошенных указали на трудности в привлечении таких специалистов (Приложение 1).

При этом неизбежность обращения к специальным знаниям требует от инициирующей стороны ответственного отношения к выбору их обладателей. Так, авторами делается акцент на том, что «необходимо привлекать грамотных специалистов, которые имеют определенные знания и умения в данной области»[319].

В данном контексте, опрошенные А. И. Семикаленовой и И. А. Рядовским, специалисты указали, что «следует привлекать специалистов, область познаний которых должна быть достаточна широка: в сфере компьютерных устройств и программирования, в области сетевого взаимодействия и эксплуатации сетевой инфраструктуры и т. п., либо следует привлекать нескольких специалистов с углубленными познаниями в определенных областях компьютерно-информационных технологий»[320].

К примеру, при совершении хищения посредством неправомерного воздействия на мобильное устройство, критерием в выборе соответствующего специалиста является «понимание алгоритма функционирования вредоносных

[319] Лантух Э. В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации // Всероссийский криминологический журнал. 2020. Т. 14, № 6. С. 885.

[320] Семикаленова А. И. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6 (103). С. 182.

компьютерных программ, предназначенных для хищения денежных средств с платежных карт клиентов банка»[321].

Итак, привлекаемыми лицами, обладающими специальными познаниями в сфере информационных технологий могут быть: сотрудники подразделений по борьбе с киберпреступлениями; сотрудники экспертно-криминалистических центров МВД России, в которых в дальнейшем проводится компьютерная экспертиза, а также сотрудники различных соответствующих организаций, как правило, специализирующиеся на оказании услуг в сфере компьютерной информации.

Так, по делу Lurk экспертизы компьютерных устройств проводились сотрудниками АНО «Судебный эксперт», ООО «Траст», Group-IB, ООО «Эксперт-Урал», ООО «БИЗОН», АО «Лаборатория Касперского»[322].

Проведенное диссертационное исследование позволило систематизировать имеющиеся представления об использовании специальных знаний в процессе расследования и относительно мошенничества в сфере компьютерной информации структурированную форму их использования представить следующим образом:

– при подготовке и проведении оперативно-розыскных мероприятий;

– при подготовке и проведении следственных действий;

– при получении консультаций и заключений специалиста;

– при назначении и проведении судебных экспертиз.

Рассмотрим указанные позиции более подробно.

При подготовке и проведении оперативно-розыскных мероприятий

Использование специальных знаний в процессе осуществления ОРД является мощнейшим инструментом получения криминалистически важной информации, способствующей установлению достоверной картины совершенного преступления. Поэтому не стоит пренебрегать данной возможностью. Так, 13 %

[321] Кравец Е. Г. Комплекс специальных знаний, необходимых при расследовании хищений, совершаемых с использованием вредоносных компьютерных программ // Юридическая наука и правоохранительная практика. 2020. № 3 (53). С. 123.

[322] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

опрошенных респондентов указали уделение недостаточного внимания консультациям со специалистами в качестве одной из типичных ошибок, допускаемых оперативными сотрудниками (Приложение 1).

Возможность использования специальных знаний в ходе проведения ОРМ предусмотрена ст. 6 Федерального закона «Об оперативно-розыскной деятельности»[323], при этом не регулируется нормами УПК РФ, в связи с чем имеет непроцессуальный характер.

Учеными выделяются следующие формы использования специальных знаний при осуществлении оперативно-розыскной деятельности:

– «консультирование; проведение документальных проверок и ревизий; проверка по картотекам, коллекциям и базам данных; проведение предварительных (в т. ч. экспресс) исследований; применение технических средств»[324];

– изготовление субъективных портретов; изготовление розыскных таблиц о лицах, предметах, орудиях преступлений; формирование и ведение экспертно-криминалистических учетов; обследование помещений, зданий, сооружений, участков местности и транспортных средств; фотосъемка, видео- и аудиозапись ОРМ, участие в отборе образцов для сравнительного исследования и т. д.[325].

В параграфе 3.1. настоящего диссертационного исследования нами уже указывались ОРМ, наиболее часто проводимые в ходе выявления, раскрытия и расследования рассматриваемого вида преступлений. При этом существуют случаи, когда получение необходимой информации возможно только посредством проведения ОРМ, что вызывает у правоприменителей определенные трудности. К примеру, в настоящее время единственным законным способом получения компьютерной информации с удаленных компьютерных систем и сетей является проведение соответствующих ОРМ, что особенно важно при расследовании преступлений, совершенных с использованием методов шифрования информации.

---

[323] Об оперативно-розыскной деятельности : федер. закон от 12.08.1995 № 144-ФЗ : ред. от 29.12.2022 г.// Доступ из справ.-правовой системы «КонсультантПлюс».

[324] Жукова Н. А. К вопросу об использовании специальных знаний в оперативно-розыскной деятельности // Гуманитарный научный вестник. 2021. № 7. С. 169–170.

[325] Аминев Ф. Г. Особенности использования специальных знаний как составной части методики расследования преступлений, связанных с экстремизмом и терроризмом // Правовое государство: теория и практика. 2017. № 3 (49). С. 133.

Так, одной из задач специалиста при проведении следственных действий и ОРМ большинство опрошенных авторами правоприменителей видят в обеспечении доступа к компьютерным данным, имеющим значение для дела, которые при осмотре электронных носителей информации могут быть в зашифрованном виде[326].

При подготовке и проведении следственных действий

Как нами уже отмечалось, наряду с общими чертами применения специальных знаний при подготовке и проведении присущими большинству следственных действий, каждое из них относительно исследуемой преступной деятельности имеет свои особенности, которые в подробном виде рассмотрены в предыдущем параграфе.

Отметим лишь важность и необходимость осуществления данной процедуры применительно к рассматриваемой категории преступлений. Так, 18,7 % опрошенных респондентов указали уделение недостаточного внимания консультациям со специалистами в качестве одной из типичных ошибок, допускаемых следователями (дознавателями) при расследовании данных преступлений (Приложение 1).

В ходе расследования преступлений рассматриваемой категории возможно привлечение специалистов и для проведения других следственных действий.

К примеру, при расследовании хищения, совершенного посредством неправомерного воздействия на мобильные телефоны, смартфоны, подключенные к услуге «Мобильный банк», системе ДБО, согласно ст. 186.1 УПК РФ, производится получение информации о соединениях между абонентами и (или) абонентскими устройствами. При этом осмотр полученного протокола телефонных соединений может вызывать у следователя (дознавателя) ряд трудностей, для разрешения которых целесообразно привлечение специалиста из

[326] Семикаленова А. И. Указ. соч. С. 180–181.

числа технических сотрудников организации, оказывающей услуги связи. В результате проведенной совместной работы уясняется, отправлялись ли, а если отправлялись, то с какого мобильного устройства и с какого места, команды на подтверждение перевода денежных средств[327].

При получении консультаций и заключений специалиста

Преимущественное большинство консультаций специалистов получается при подготовке к проведению следственных действий. В ходе расследования рассматриваемой группы преступлений такими специалистами могут быть специалисты в области бухгалтерии, банковского дела, организации оборота безналичных, электронных денежных средств, организации осуществления телефонной, сотовой связи, интернет соединений и т. д.

Помимо проведения соответствующих компьютерно-технических экспертиз от компаний, специализирующихся на обеспечении информационной безопасности возможно получение другой справочно-ориентирующей информации. Так, по делу Lurk в АО «Лаборатория Касперского» запрошена справка о наличии в вирусных базах сведений, ассоциированных с доменным именем. Вирусная база Лаборатории Касперского – это хранилище, базы данных, которые отвечают за обслуживание, работу для обеспечения защиты пользователей[328].

Помимо проведения различных видов компьютерно-технических экспертиз при совершении многоэпизодных хищений, помощь специалиста может понадобиться при сопоставлении и оценке взаимосвязи эпизодов друг с другом. Так, по делу Lurk привлеченному специалисту представлены заключения специалистов и экспертов по результатам исследования электронных носителей информации, проведенные в разное время по различным эпизодам преступлений. По результатам изучения специалист указал на сопоставляемый между собой

[327] Кравец Е. Г. Указ. соч. С. 121–122.
[328] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

уникальный идентификатор программного компонента, который прописывается в реестре операционной системы Microsoft Windows[329].

При этом форма полученной консультации может так и остаться непроцессуальной, а может получить и доказательственное значение путем проведения допроса специалиста или получения его заключения.

При назначении и проведении судебных экспертиз

Несмотря на многообразие форм применения специальных знаний в ходе уголовно-правового реагирования на совершенное мошенничество в сфере компьютерной информации одной из его главных форм является проведение судебных экспертиз, результаты которых могут стать главным доказательственным аргументом изобличения преступной деятельности.

Сущность данной формы использования специальных знаний заключается «в анализе … сведущим лицом (экспертом) предоставляемых в его распоряжение материальных объектов экспертизы (вещественных доказательств), а также различных документов в целях установления фактических данных, имеющих значение для правильного разрешения дела»[330].

В ходе проведения расследования мошенничества в сфере компьютерной информации назначаются и проводятся различные виды экспертиз, в т. ч. дактилоскопическая (на что указали 7,1 % респондентов), почерковедческая (на что указали 7,4 % респондентов), экспертиза реквизитов документов (на что указали 18,8 % респондентов), компьютерно-техническая экспертиза (на что указали 97,3 % респондентов), судебно-бухгалтерская (позволяющая определить движение денежных средств по счету)[331](на что указали 17,2 % респондентов), судебно-психиатрическая (на что указали 6 % респондентов), финансово-экономическая, судебная автороведческая, технико-криминалистические

[329] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

[330] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе … М., 2018. С. 12.

[331] Маилян А. В. Совершенствование методики расследования хищения с использованием электронных средств платежа : дис. … канд. юрид. наук. Ростов н/Д, 2021. С. 182–183.

экспертизы и другие. Так, к примеру, гр. К. – лидер преступного сообщества Lurk был направлен на психиатрическую экспертизу, в т. ч. после сообщенных им сведений о принадлежности сотрудников ФСБ к осуществлению преступной деятельности [332] . В результате проведенной по данному делу финансово-экономической экспертизы установлено, что перед совершением хищения остаток на счете в банке составлял 114 830 391,22 руб., после чего на счета 228 физических лиц было перечислено 99 705 000,00 руб.[333]

Однако основным видом судебных экспертиз, производящихся в ходе расследования мошенничества в сфере компьютерной информации, являются экспертизы, именуемые Е. Р. Россинской как «судебные компьютерно-технические экспертизы», основное назначение которых автор видит в определении «статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним ее исследованием»[334].

Как верно отметили К. В. Муравьев и М. Г. Ермаков, в различных ведомствах название такой экспертизы отличается. Так, в Минюсте России, согласно приказу Минюста России от 27.12.2012 № 237 [335] , при назначении соответствующего исследования правомерно использовать термин «компьютерно-техническая экспертиза». Рассматриваемая деятельность в МВД России регламентирована приказом от 29.06.2005 № 511[336], который в качестве

---

[332] Антоненков Д. Указ. соч.

[333] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 ...

[334] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. 3-е изд., доп. М. : Норма ; ИНФРА-М, 2011. С. 472.

[335] Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России : приказ Минюста России от 27.12.2012 № 237 // Доступ из справ.-правовой системы «КонсультантПлюс».

[336] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних Российской Федерации : приказ МВД России от 29.06.2005 № 511 // Доступ из справ.-правовой системы «КонсультантПлюс».

правильного названия такого исследования обозначает «компьютерная» экспертиза[337].

Е. Р. Россинской, Е. И. Галяшиной приводится следующая классификация рассматриваемых экспертиз:

– аппаратно-компьютерная экспертиза;

– программно-компьютерная экспертиза;

– информационно-компьютерная экспертиза (данных);

– компьютерно-сетевая экспертиза[338].

При этом, несмотря на разнообразие наименований, авторы указывают на целесообразность указания в постановлении о производстве судебной экспертизы судебную компьютерно-техническую экспертизу, а не ее родовое наименование[339].

Итак, рассмотрим указанные виды экспертиз подробнее:

– в ходе проведения *аппаратно-компьютерной экспертизы* исследованию подвергаются технические (аппаратные) средства компьютерной системы. Предметом экспертизы является установление интересуемых фактов и обстоятельств уголовного дела посредством исследования закономерностей эксплуатации аппаратных средств компьютерной системы - материальных носителей информации. Объектами исследования могут являются персональные компьютеры, мобильные телефоны, серверы, периферийные устройства, флеш-карты, магнитные, лазерные диски и т. д.[340].

Так, по делу Lurk при назначении экспертизы сервера модели Proliant DL380 GEN8 с жесткими дисками вопросы ставились о наличии на данных объектах программ, заведомо предназначенных без ведома пользователя для уничтожения, блокирования, модификации, копирования информации, программ для удаленного или сетевого управления компьютером, следах их работы и способе появления на исследуемых объектах. В результате такие программы были

---

[337] Муравьев К. В., Ермаков М. Г. Современные возможности судебно-компьютерной экспертизы и меры по совершенствованию практики ее назначения при расследовании преступлений, связанных с незаконным оборотом наркотических средств «дистанционным» способом // Вестник Восточно-Сибирского института МВД России. 2019. № 3 (90). С. 184–185.

[338] Россинская Е. Р. Галяшина Е. И. Настольная книга судьи: судебная экспертиза. М. : Проспект, 2021. С. 379.

[339] Там же. С. 389.

[340] Там же. С 379.

обнаружены, о чем было указано в исследовательской части экспертного заключения[341];

– в ходе *программно-компьютерной экспертизы* проводится исследование программного обеспечения. Предметом экспертизы являются закономерности разработки и применения программного обеспечения. Объектами исследования являются системное и прикладное программное обеспечение, вспомогательные программы, средства разработки программ и т. д.[342];

– целью *информационно-компьютерной экспертизы (данных)* является поиск, обнаружение, анализ и оценка информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе. Объектами экспертизы являются различного рода файлы[343];

– *компьютерно-сетевая экспертиза* проводится, в том числе, с целью установления свойств аппаратного средства, программного обеспечения, вычислительной сети и т. д. Результатом проведения такой экспертизы может являться, в том числе, установление признаков «несанкционированного» доступа. является установление возможного доступа к сети Интернет. Одной из разновидностей данной экспертизы является *судебная телематическая экспертиза* при которой производится исследование средств телекоммуникаций и подвижной связи[344];

Стоит отметить, что указанный перечень не является исчерпывающим и в настоящее время, в связи с расширением возможностей судебной экспертизы, мы являемся свидетелями появления ее новых видов. Так, М. А. Гудкова сообщает, что одним из таких видов является *информационно-аналитическая экспертиза*. Объектами исследований могут являться массивы данных о детализации телефонных соединений, финансовых транзакциях, об IP-адресах и адресах электронной почты, данные из социальных сетей, сведения о передвижении

---

[341] Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1 …
[342] Россинская Е. Р., Галяшина Е. И. Указ. соч. С. 381–382.
[343] Там же.
[344] Там же. С. 386–389.

транспортных средств и т. д. Результатами проведенных экспертиз могут быть: выявление общих признаков у ряда преступлений, установление лица, совершившего преступление, его соучастников, маршрутов их передвижения, оценка правдивости показаний допрашиваемого в случае возникновения противоречий о его местонахождении, передвижении[345].

Несомненно, в ходе расследования «организованного» мошенничества в сфере компьютерной информации проведение информационно-аналитической экспертизы является наиболее целесообразным и необходимым.

Экспертизой, сущность которой также направлена на установление криминалистически важной информации в ходе расследования преступлений в сфере компьютерной информации, является *судебная автороведческая экспертиза*, объектами которой, в том числе, могут быть переписка в социальных сетях, блогах, SMS-сообщения, сообщения в различных мессенджерах (WhatsApp, Viber, Telegram и т. д.), содержание фонограмм разговоров, аудио-/видеозаписи выступлений и т. д.[346]

Кроме того, в ходе проведения расследования возможно проведение «комплексных судебных экспертиз, например, с привлечением специалистов в области криптографии и защиты информации или видеотехники при исследовании видеозаписей, произведенных или обработанных с помощью компьютерных средств и программного обеспечения»[347].

Кроме того, в случае необходимости в процессе расследования, возможно проведение комплексных экспертиз, в т. ч.:

– судебно-автороведческой и компьютерно-технической, в ходе которой возможно установление авторства компьютерной программы;

– экспертизы программного обеспечения и судебно-бухгалтерской экспертизы, в ходе которой устанавливается возможность внесения изменений в

---

[345] Гудкова М. А. Актуальные вопросы информационно-аналитических исследований // Расследование преступлений: проблемы и пути их решения. 2018. № 3 (21). С. 156–157.

[346] Сааков Т. А. Судебная автороведческая экспертиза объектов из цифровой среды при установлении деморафических характеристик автора // Законы России: опыт, анализ, практика. 2020. № 4. С. 96–103.

[347] Противодействие преступлениям, совершаемым в сфере информационных технологий: учебник / В.В. Гончар [и др.]. М., 2021. С. 196.

результаты проведения расчетов и отчетности посредством осуществления несанкционированного воздействия на программное обеспечение, кто из сотрудников имеет такие возможности[348];

– судебной компьютерно-технической и судебно-технической экспертизы документов, необходимость проведения которой вызвана исследованием поддельных ценных бумаг, документов, кредитных карт, изготовленных с использованием информационных технологий[349].

Процесс производства рассматриваемого вида экспертиз предполагает использование соответствующих технических средств и программного обеспечения:

– «UFED (Universal forensic extraction device) – прибор, позволяющий извлекать данные из 95 % всех сотовых телефонов (смартфонов, планшетов) о паролях, контактах, переписке, вызовах, используемых приложениях, местоположении и т. д.;

– MSAB Office – программно-аппаратный комплекс, позволяющий извлекать данные с мобильных устройств, в т. ч. удаленные, и создавать комбинированный отчет;

– «Мобильный криминалист» – программный комплекс, позволяющий преодолевать паролевую защиту мобильных устройств, восстанавливать удаленную информацию, извлекать данные из защищенных криптографией приложений, определять общие связи нескольких пользователей, получать их переписку в социальных сетях и различных мессенджерах;

– Belkasoft Evidence Center – программное обеспечение, позволяющее получать данные из большинства компьютерных и мобильных операционных систем путем анализа сведений, содержащихся в оперативной памяти, жестких магнитных дисках, резервных копиях, облачных хранилищах и т. д.»[350];

– «программный комплекс, состоящий из программ «Зверобой», «Следопыт», Octopus (позволяющий исследовать сведения о местоположении

[348] Противодействие преступлениям, совершаемым …С. 196
[349] Россинская Е. Р., Галяшина Е. И. Указ. соч. С. 389–391.
[350] Муравьев К. В., Ермаков М. Г. Указ. соч. С. 187.

абонента, его перемещении, активности в социальных сетях); специализированные программы «Курс» и «Лис-М» (производящие анализ данных по открытым источникам данных сети Интернет); аппаратно-программный комплекс «Сегмент-С» (позволяющий производить анализ детализации абонентов и трафика базовых станций)»[351].

Назначение экспертизы предполагает вынесение соответствующего постановления, при этом особого внимания требует определение и формулировка вопросов, позволяющих выяснить все необходимые обстоятельства. Так, треть опрошенных сотрудников, которым приходилось назначать компьютерно-технические экспертизы, испытывали при их назначении соответствующие трудности (Приложение 1). Рекомендуется производить консультации с экспертами, в ходе которых знакомить их «с фабулой дела и версиями следствия, требующими проверки, после чего, с учетом индивидуальных особенностей каждой ситуации, формулируются вопросы, которые будут поставлены на разрешение эксперта» [352] . Однако на практике имеются случаи, когда правоприменители сталкиваются со сложностями привлечения таких специалистов на данном этапе, в результате чего ряд ключевых обстоятельств по делу остаются не установленными[353].

Наряду с указанным, поставленные перед экспертом вопросы должны отвечать следующим критериям:

– корректная с правовой и технической точек зрения формулировка;

– соответствие фактическим возможностям эксперта (экспертного учреждения), его компетенции и оснащенности;

– точное и однозначное отражение цели и прогнозируемого результата исследования.

Итак, при назначении судебной экспертизы и выборе соответствующего экспертного учреждения необходимо исходить из следующих обстоятельств:

[351] Гудкова М. А. Указ. соч. С. 160.
[352] Там же. С. 158.
[353] Скоробогатов К. С. Использование специальных знаний при расследовании мошенничества в сфере компьютерной информации // Пермский период : сб. мат-лов IX Междунар. научно-спортивного фестиваля курсантов и студентов образовательных организаций. Т. 1. Пермь, 2022. С. 297–298.

наличия экспертных учреждений, проводящих исследования рассматриваемого вида и их возможности; реальной возможности произвести экспертизу в короткие сроки; территориальности расположения экспертного подразделения; возможности производства судебно-компьютерной экспертизы по месту нахождения электронных носителей и иных объектов экспертизы; наличия у эксперта допуска на производство одновременно судебно-компьютерной экспертизы и смежных экспертиз; компетентности эксперта[354].

При этом в настоящее время недостаточная компетенция следователей (дознавателей) в вопросе назначения компьютерно-технических экспертиз влечет за собой возникновение ряда проблемных вопросов. Так, В. Р. Гайнельзяновой в этой связи выделены следующие проблемы:

– увеличение сроков производства экспертиз в связи с неправильной формулировкой вопросов. Так, на длительность сроков проведения экспертиз указало 17,4 % опрошенных респондентов (Приложение 1);

– направление на исследование нескольких объектов в рамках вынесения одного постановления о назначении экспертизы;

– предоставление следователем (дознавателем) не в должном объеме либо не соответствующих делу материалов, необходимых для производства экспертизы;

– несвоевременность вынесения постановления о назначении экспертизы[355].

Итак, как видим, специфичность исследуемой преступной деятельности предполагает неминуемость обращения к специальным знаниям, возможности и потенциал которых являются мощным инструментом и способствуют эффективному выявлению, раскрытию и расследованию преступлений.

---

[354] Муравьев К. В., Ермаков М. Г. Указ. соч. С. 188.

[355] Гайнельзянова В. Р. Возможности судебной компьютерно-технической экспертизы при расследовании преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. 2021. № 1(91). С. 149.

ЗАКЛЮЧЕНИЕ

Проведенное диссертационное исследование мошенничества в сфере компьютерной информации позволило определить и сформулировать следующие основные положения.

На первоначальном этапе формирования методики установлено, что специфической особенностью исследуемого преступного деяния является его преимущественное совершение в совокупности с сопутствующими преступлениями, которыми, как правило, являются деяния, предусмотренные гл. 28 УК РФ «Преступления в сфере компьютерной информации». В связи с чем, сделан вывод о том, что формирование криминалистической методики, касающейся расследования исключительно деяния, предусмотренного ст. 159.6 УК РФ, было бы действием принципиально неверным, обедняющим научную и практическую значимость научного труда.

Поэтому, проведенное научное исследование позволило прийти к выводу о целесообразности, при выборе основания формирования методики расследования, выбора соответствующего уголовно-правового, а также криминалистического критериев. Так, в качестве уголовно-правового критерия принято сочетание как основного деяния, предусмотренного ст. 159.6 УК РФ, так и ряда сопутствующих. В качестве криминалистического критерия основания формируемой методики определены соответствующие криминалистические признаки, присущие рассматриваемой группе преступлений. На основе данной позиции определено понятие мошенничества в сфере компьютерной информации в криминалистическом аспекте. Приведены и обоснованы некоторые методологически значимые параметры формируемой криминалистической методики:

1. Актуальность создания данной методики продиктована низким уровнем раскрываемости, высокой латентностью исследуемой преступной деятельности, а также отсутствием должных соответствующих методических разработок.

2. Установлено, что наибольшую общественную опасность представляют «организованные» формы мошенничества в сфере компьютерной информации, в связи с чем при формировании методики избран приоритет изобличения данного типа рассматриваемой преступной деятельности.

3. Представленная методика расследования мошенничества в сфере компьютерной информации является частной по отношению к более общим методикам, комплексной, полиобъектной, «диссертационной», относящейся к группе еще меньшей степени общности, включающей в себя видовые и подвидовые методики.

4. По объему формируемая методика является не полноструктурной, а представлена в виде особенностей методики, отражающая наиболее актуальные аспекты исследуемой преступной деятельности.

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

Во второй главе диссертационного исследования представлена криминалистическая характеристика мошенничества в сфере компьютерной информации, которая включает в себя следующие элементы: типичные способы, обстановка, типичные следы мошенничества в сфере компьютерной информации, а также личность типичных преступника и потерпевшего. Типичные способы рассматриваемой преступной деятельности приведены относительно анализа правоприменительной практики, имеющихся разъяснений действующего

законодательства, мнения ученых и призваны способствовать устранению случаев неправильной квалификации. Выделены «организованный», «несложный» «простой» тип мошенничества в сфере компьютерной информации, а также деяния, совершенные посредством основного преступления, а также основного и сопутствующего. Представлена авторская классификация типичных преступников относительно имеющихся познаний в сфере ИТТ. Особенностью следовой картины рассматриваемой преступной деятельности является то, что преимущественный объем доказательственной информации содержат цифровые следы. Приводятся особенности следовой картины, оставляемой преступниками различной категории. В качестве дополнительного элемента обстановки преступной деятельности предлагается включить обладание различными компьютерными устройствам, программно-аппаратными и другими техническими средствами.

Также определены основные направления расследования мошенничества в сфере компьютерной информации: выявление, раскрытие и расследование «организованного» мошенничества в сфере компьютерной информации; изобличение и пресечение преступной деятельности всех членов преступных формирований, и прежде всего организаторов.

В третьей заключительной главе рассмотрены особенности возбуждения и расследования уголовных дел данной категории. Особенностями этапа возбуждения уголовного дела являются нацеленность на обнаружение, изъятие, исследование, в том числе, цифровых следов, образованных в результате взаимодействия с компьютерной информацией и их носителей. Определены подлежащие установлению и доказыванию обстоятельства. Приведены критерии оценки собранной в результате доследственной проверки информации с позиции складывающейся судебной перспективы по делу.

Рассмотрены типичные следственные ситуации начального и последующего этапа расследования мошенничества в сфере компьютерной информации, предложен алгоритм действий по их разрешению. В качестве приоритета выбрана нацеленность на выявление, раскрытие, расследование «организованного» типа

мошенничества. С этой целью предложены рекомендации по изобличению преступной деятельности посредством проведения ОРМ оперативное внедрение. Приводятся типичные ошибки, допускаемые оперативными сотрудниками, следователями (дознавателями) в ходе выявления, раскрытия, расследования преступлений рассматриваемой категории. Особенность проведения следственных действий по делам рассматриваемой категории преимущественно заключается в особенности работы с цифровыми следами, их носителями, необходимости использования соответствующих специальных знаний.

Таким образом, сформулированные теоретические положения, систематизированный практический опыт, заключения и рекомендации могут быть положены в качестве основы для дальнейших научных исследований в данной сфере правоотношений, а также использоваться в практической деятельности сотрудников, занимающихся выявлением, раскрытием, расследованием мошенничества в сфере компьютерной информации.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые, нормативные и иные акты

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. : с изм. от 01 июля 2020 г. // Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63ФЗ : ред. от 04 августа 2023 г. // Доступ из справ.-правовой системы «КонсультантПлюс».

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ : ред. от 25 декабря 2023 г. // Доступ из справ.-правовой системы «КонсультантПлюс».

4. Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ (ред. от 29 декабря 2022 г.) // Доступ из справ.-правовой системы «КонсультантПлюс».

5. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : Федеральный закон от 29 ноября 2012 № 207-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

6. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон от 06 июля 2016 г. № 374-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

7. О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 09 мая 2017 г. № 203 // Доступ из справ.-правовой системы «КонсультантПлюс».

8. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних Российской Федерации :

Приказ МВД России от 29 июня 2005 г. № 511 // Доступ из справ.-правовой системы «КонсультантПлюс».

9. О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений: Приказ МВД России от 03 апреля 2018 г. № 196 // Доступ из справ.-правовой системы «КонсультантПлюс».

10. Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России: Приказ Минюста России от 27 декабря 2012 г. № 237 // Доступ из справ.-правовой системы «КонсультантПлюс».

11. Инструкция «О порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд», утверждена Приказом МВД России № 776, Министерства обороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013 г. // Доступ из спра.-правовой системы «КонсультантПлюс».

12. Пояснительная записка к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» / Паспорт проекта федерального закона № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы) // Доступ из справ.-правовой системы «КонсультантПлюс».

Постановления Пленума Верховного Суда Российской Федерации

13. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях,

совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 // Доступ из справ.-правовой системы «КонсультантПлюс».

14. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Росссийской Федерации от 30.11.2017 № 48 (ред. от 15.12.2022) // Доступ из справ.-правовой системы «КонсультантПлюс».

Монографии, учебники, учебные и научно-практические пособия, методические рекомендации

15. Аверьянова, Т. В. Криминалистика : учебник / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. – 3-е изд., перераб. и доп. – Москва : Норма ; Инфра-М. – 2010. – 944 с. – ISBN 978-5-468-00015-1, ISBN 978-5-16-004096-7.

16. Антонян, Ю. М. Криминология : учебник для вузов / Ю. М. Антонян. – 3-е изд., перераб. и доп. – Москва : Юрайт, 2024. – 388 с. – ISBN 978-5-9916-4891-2.

17. Ахмедшин, Р. Л. Тактика коммуникативных следственных действий / Р. Л. Ахмедшин ; научный редактор Н. Т. Ведерников. – Томск : ТГУ, 2014. – 294 с. – ISBN 978-5-94621-449-0.

18. Алескеров, В. И. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова ; ВИПК МВД России. – Домодедово, 2016. – 166 с.

19. Белкин, Р. С. Курс криминалистики. В 3 т. Т. 3. Криминалистические средства, приемы и рекомендации / Р. С. Белкин. – Москва: Юристъ, 1997. – 480 с. – ISBN 5-7357-0201-7.

20. Белкин, Р. С. Курс криминалистики : учебное пособие для вузов / Р. С. Белкин. – 3-е изд., доп. – Москва : ЮНИТИ-ДАНА ; Закон и право, 2001. – 837 с. – ISBN 5-238-00198-3.

21. Бердникова, О. П. Особенности первоначального и последующего этапов расследования мошенничества в сфере компьютерной информации : учебное пособие / О. П. Бердникова. – Екатеринбург : Уральский юридический институт МВД России, 2019. – 56 с. – ISBN 978-5-88437-670-0.

22. Бердникова, О. П. Особенности расследования мошенничества в сфере компьютерной информации : учебное пособие / О. П. Бердникова, Р. А. Дерюгин. – Екатеринбург : Уральский юридический институт МВД России, 2021. – 84 с.

23. Волчецкая, Т. С. Криминальные и криминалистические ситуации / Т. С. Волчецкая // Криминалистика : учебник / под редакцией Н. П. Яблокова. – 4-е изд., перераб. и доп. – Москва : Норма ; ИНФРА-М, 2016. – 752 с. – ISBN 978-5-91768-114-6, ISBN 978-5-16-004320-3.

24. Возгрин, И. А. Введение в криминалистику: история, основы теории, библиография / И. А. Возгрин. – Санкт-Петербург : Юридический центр Пресс, 2003. – 473 с. – ISBN 5-94201-183-4.

25. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2024. – 490 с. – ISBN 978-5-534-17464-9.

26. Гавло, В. К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений / В. К. Гавло ; Национальный исследовательский Томский государственный университет. – Томск, 1985. – 333 с.

27. Гармаев, Ю. П. Незаконная деятельность адвокатов в уголовном судопроизводстве : учебник / Ю. П. Гармаев. – Москва : Экзамен, 2005. – 512 с. – ISBN 5-472-00343-1.

28. Гармаев, Ю. П. Основы методики расследования коррупционных преступлений : курс лекций / Ю. П. Гармаев. – Улан-Удэ : Изд-во Бурятского гос. ун-та, 2018. – 49 с.

29. Гармаев, Ю. П. Проблемы создания криминалистических методик расследования преступлений. Теория и практика / Ю. П. Гармаев, А. Ф. Лубин. – Санкт-Петербург : Юридический центр Пресс, 2006. – 301 с. – ISBN 5-94201-401-9.

30. Гаврилин, Ю. В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : научно-практическое пособие / Ю. В. Гаврилин. – Москва : Академия управления МВД России, 2021. – 72 с. – ISBN 978-5-907187-86-3.

31. Дубоносов, Е. С. Оперативно-розыскная деятельность : учебник и практикум для вузов / Е. С. Дубоносов. – 7-е изд., пераб. и доп. – Москва : Юрайт, 2023. – 420 с. – ISBN 978-5-534-15604-1.

32. Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учебное пособие / А. А. Балашова [и др.] ; под редакцией Ю. В. Гаврилина, А. В. Победкина. – Москва : Академия управления МВД России, 2021. – 140 с. – ISBN 978-5-907187-68-9.

33. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / В. В. Гончар [и др.] ; Московский университет МВД России имени В.Я. Кикотя. – Москва, 2021. – 332 с. – ISBN 978-5-9694-1011-4.

34. Криминалистика / под редакцией В. А. Образцова. – Москва : Юрист, 1995. – 592 с. – ISBN 5-7357-0056-1.

35. Криминалистика. В 5 т. Т. 5. Методика расследования преступлений: учебник для вузов / И. В. Александров [и др.]; под общей редакцией И. В. Александрова. – Москва : Юрайт, 2023. – 242 с. – ISBN 978-5-534-08441-2.

36. Кудрявцев, В. Н. Объективная сторона преступления : учебное пособие / В. Н. Кудрявцев. – Москва : Госюриздат, 1960. – 244 с.

37. Лунеев, В. В. Курс мировой и российской криминологии. В 2 т. Т. 1. Общая часть. В 3 кн. Кн. 3 : учебник для вузов / В. В. Лунеев. – Москва : Юрайт, 2023. – 413 с. – ISBN 978-5-534-03998-6.

38. Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации, предусмотренных статьей 159.6 Уголовного кодекса Российской Федерации : методические рекомендации / С. Н. Миронов [и др.]. – Казань : КЮИ МВД России, 2017. – 65 с.

39. Ушаков, А. Ю. Особенности квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей : методические рекомендации / А. Ю. Ушаков, А. Г. Саакян, Р. С. Поздышев, М. А. Степанова. – Нижний Новогород : Нижегородская академия МВД России, 2020. – 61 с.

40. Рассолов, И. М. Право и Интернет. Теоретические проблемы / И. М. Рассолов. – 2-е изд., перераб. и доп. – Москва : Норма, 2009. – 384 с. – ISBN 978-5-91768-003-3.

41. Россинская, Е. Р. Настольная книга судьи: судебная экспертиза / Е. Р. Россинская, Е. И. Галяшина. – Москва : Проспект, 2021. – 464 с. – ISBN 978-5-392-33068-3.

42. Россинская, Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е. Р. Россинская. – Москва : Норма ; ИНФРА-М, 2011. – 736 с. – ISBN 978-5-468-00327-5, ISBN 978-5-16-004546-7.

43. Ростовцев, А. В. Электронные носители информации в уголовном судопроизводстве : учебное пособие / А. В. Ростовцев, Р. А. Кокорев, Е. Д. Берестенко ; Московский областной филиал Московского университета МВД России имени В.Я. Кикотя. – Старотеряево, 2021. – 70 с.

44. Старков, О. В. Криминология. Теория и практика : учебник для вузов / О. В. Старков. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2024. – 641 с. – ISBN 978-5-9916-3718-3.

45. Шмонин, А. В. Методология криминалистической методики: монография / А. В. Шмонин. – Москва : Юрлитинформ, 2010. – 415 с. – ISBN 978-5-93295-646-5.

46. Яблоков, Н. П. Криминалистика : учебник / Н. П. Яблоков. – 2-е изд., перераб. и доп. – Москва : Норма, 2009. – 400 с. – ISBN 978-5-468-00171-4.

Диссертации и авторефераты диссертаций

47. Боровских, Р. Н. Теоретические основы и прикладные аспекты расследования преступлений в сфере страхования: дис. … д-ра юрид. наук : 12.00.12 / Боровских Роман Николаевич. – Москва, 2018. – 455 с.

48. Гаспарян, Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : дис. … канд. юрид. наук : 12.00.12 / Гаспарян Гурген Зорикович. – Москва, 2020. – 300 с.

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

50. Григорян, Г. Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации : дис. … канд. юрид. наук : 12.00.08 / Григорян Гарик Рафикович. – Самара, 2021. – 243 с.

51. Ефремова, М. А. Уголовно-правовая охрана информационной безопасности : дис. … д-ра юрид. наук: 12.00.08 / Ефремова Марина Александровна. – Москва, 2017. – 427 с.

52. Зуйков, Г. Г. 46 Криминалистическое учение о способе совершения преступления : автореф. дис. ... д-ра юрид. наук / Зуйков Георгий Георгиевич. – Москва, 1970. – 31 с.

53. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. … канд. юрид. наук : 12.00.12 / Коломинов Вячеслав Валентинович. – Иркутск, 2017. – 211 с.

54. Маилян, А. В. Совершенствование методики расследования хищения с использованием электронных средств платежа: дис. … канд. юрид. наук : 12.00.12 / Маилян Ани Варужановна. – Ростов-на-Дону, 2021. – 245 с.

55. Мазуров, И. Е. Методика расследования хищений, совершаемых с использованием интернет-технологий : дис. … канд. юрид. наук : 12.00.12 / Мазуров Игорь Евгеньевич. – Казань, 2017. – 188 с.

56. Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук : 12.00.09 / Мещеряков Владимир Алексеевич. – Воронеж., 2001. – 386 с.

57. Милашев, В. А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. … канд. юрид. наук : 12.00.09 / Милашев Вадим Александрович. – Москва, 2004. – 21 с.

58. Поляков, Н. В. Особенности методики расследования незаконного обналичивания и транзитирования денежных средств : дис. ... канд. юрид. наук : 12.00.12 / Поляков Николай Владиславович. – Красноярск, 2021. – 241 с.

59. Русскевич, Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-телекоммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук : 12.00.08 / Русскевич Евгений Александрович. – Москва, 2020. – 521 с.

60. Тагиров, Р. А. Первоначальный этап расследования мошенничества в сфере кредитования : дис. … канд. юрид. наук : 12.00.12 / Тагиров Руслан Амирович. – Уфа, 2022. – 236 с.

61. Чумаков, А. В. Особенности методики расследования мошенничества при получении выплат : дис. … канд. юрид. наук : 12.00.12 / Чумаков Алексей Вадимович. – Калининград, 2018. – 238 с.

62. Шевченко, Е. С. Тактика производства следственных действий при расследовании киберпреступлений : дис. … канд. юрид. наук : 12.00.12 / Шевченко Елизавета Сергеевна. – Москва, 2016. – 249 с.

63. Фролов, М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации : дис. ... канд. юрид. наук : 12.00.08 / Фролов Михаил Дмитриевич. – Москва, 2018. – 211 с.

64. Южин, А. А. Мошенничество и его виды в российском уголовном праве : дис. …канд. юрид. наук : 12.00.08 / Южин Андрей Андреевич. – Москва, 2016. – 328 с.

Научные статьи, тезисы докладов

65. Аминев, Ф. Г. Особенности использования специальных знаний как составной части методики расследования преступлений, связанных с экстремизмом и терроризмом / Ф. Г. Аминев // Правовое государство: теория и практика. – 2017. – № 3 (49). – С. 130–137.

66. Андриенко, Ю. А. Отдельные аспекты использования информационных технологий и работы с электронными носителями информации в доказывании по уголовным делам / Ю. А. Андриенко // Вестник Сибирского юридического института МВД России. – 2018. – № 3 (32). – С. 99–105.

67. Борисов, В. В. Об особенностях фиксации информационных следов в практике защиты информации / В. В. Борисов // Известия ЮФУ. Технические науки. – 2009. – № 5 (94). – С. 164–168.

68. Белицкий, В. Ю. Мошенничества и возможные критерии их криминалистической классификации / В. Ю. Белицкий // Вестник Восточно-Сибирского института МВД России. – 2021. – № 4 (99). – С. 176–188.

69. Белова, Н. В. Место совершения дистанционных хищений (проблемы практики применения) / Н. В. Белова, А. В. Белов // Судебная власть и уголовный процесс. – 2021. – № 2. – С. 68–73.

70. Бессонов, А. А. О некоторых возможностях современной криминалистики в работе с электронными следами / А. А. Бессонов // Вестник университета имени О. Е. Кутафина (МГЮА). – 2019. – № 3 (55). – С. 46–52.

71. Бердникова, О. П. Ситуационная характеристика последующего этапа расследования мошенничества в сфере компьютерной информации / О. П. Бердникова // VII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии» : материалы международной научно-практической конференции, Калининград, 14 декабря 2018 года / Калининградский филиал Санкт-Петербургского университета МВД России. – Калининград, 2019. – С. 121–123.

72. Бертовский, Л. В. Понятие, объект и предмет криминалистики / Л. В. Бертовский, В. А. Образцов // Пробелы в российском законодательстве. – 2016. – № 4. – С. 228–233.

73. Бородин, А. И. Исследование остаточных артефактов Viber и Telegram в операционной системе Windows / А. И. Бородин, Р. Р. Вейнберг, Д. В. Писарев, О. В. Литвишко // Бизнес-информатика. – 2019. – Т. 13, № 4. – С. 39–48.

74. Головин, А. Ю. Базовые криминалистические классификации преступлений / А. Ю. Головин // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 2-2. – С. 31–40.

75. Шигуров, А. В. Проблемы правового регулирования изъятия электронных носителей информации и копирования с них информации при

производстве следственных действий / А. В. Шигуров, Н. А. Подольный // Юридическая наука и практика : Вестник Нижегородской академии МВД России. – 2020. – № 1 (49). – С. 169–174.

76. Васюков, В. Ф. Тактические проблемы проведения осмотра места происшествия при расследовании мошенничества в сфере компьютерной информации / В. Ф. Васюков // Право и образование. – 2017. – № 2. – С. 103–110.

77. Гармаев, Ю. П. Преимущественная борьба с «мелкими» коррупционными преступлениями как проблема практики и криминалистической науки / Ю. П. Гармаев // Lexrussica. – 2023.– № 76 (3). – С. 63–71.

78. Гармаев, Ю. П. Концепция «судебная перспектива по уголовному делу» и криминалистическая ситуалогия / Ю. П. Гармаев // Вестник Бурятского государственного университета. – 2013. – № 2. – С. 177–181.

79. Гайнельзянова, В. Р. Возможности судебной компьютерно-технической экспертизы при расследовании преступлений в сфере компьютерной информации / В. Р. Гайнельзянова // Вестник Уфимского юридического института МВД России. – 2021. – № 1 (91). – С. 144–149.

80. Гудкова, М. А. Актуальные вопросы информационно-аналитических исследований / М. А. Гудкова // Расследование преступлений: проблемы и пути их решения. – 2018. – № 3 (21). – С. 155–160.

81. Давыдов, В. О. О некоторых аспектах практики реализации криминалистического предупреждения преступлений экстремистской направленности в информационно-телекоммуникационном пространстве / В. О. Давыдов // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности : сборник научных статей по материалам международной научно-практической конференции, Москва, 26 мая 2023 г. / Академия управления МВД России. – Ч. 1. – Москва, 2023. – С. 199–206.

82. Давыдов, В. О. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий /

В. О. Давыдов, И. В. Тишутина // Криминалистика: вчера, сегодня, завтра. – 2020. – № 2 (14). – С. 81–91.

83. Дубоносов, Е. С. Оперативно-розыскное мероприятия «Получение компьютерной информации»: содержание и проблемы проведения / Е. С. Дубоносов // Известия Тульского государственного университета. Экономические и юридические науки. – 2017. – № 2-2. – С. 24–30.

84. Дубинин, А. С. Получение компьютерной информации как самостоятельное оперативно розыскное мероприятие / А. С. Дубинин, А. В. Серов // Вестник Воронежского института МВД России. – 2018.– № 3. – С. 170–175.

85. Жукова, Н. А. К вопросу об использовании специальных знаний в оперативно-розыскной деятельности / Н. А. Жукова, Р. Е. Черкашин // Гуманитарный научный вестник. – 2021. – № 7. – С. 168–171.

86. Жижина, М. В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) / М. В. Жижина, Д. В. Завьялова // Актуальные проблемы российского права. – 2022. – Т. 17, № 5 (138). – С. 149–158.

87. Зуев, С. В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий / С. В. Зуев // Законность. – 2018. – № 4. – С. 58–60.

88. Зеленский, В. Д. О процессуальных и организационных формах использования специальных знаний в расследовании / В. Д. Зеленский // Общество и право. – 2012. – № 1 (38). – С. 210–212.

89. Иванов, П. О. Использование специальных компьютерных знаний при расследовании преступлений: проблемные вопросы подготовки экспертов / П. О. Иванов // 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 года. – Красноярск : Красноярский государственный аграрный университет, 2022. – С. 291–294.

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

91. Ищенко, Е. П. Виртуальное пространство как объект криминалистического познания / Е. П. Ищенко // Криминалистика и судебно-экспертная деятельность в условиях современности : материалы Международной научно-практической конференции: в 2 томах, Краснодар, 26 апреля 2013 года / редколлегия С. В. Пахомов, Д. А. Натура, Л. А. Рычкалова ; Краснодарский университет МВД России. Т. 1. Краснодар, 2013. – С. 16–23.

92. Камнев, Р. Г. Соотношение места, времени и обстановки совершения преступления / Р. Г. Камнев // Вестник Волгоградского государственного университета. – 2006. – № 8. – С. 127–136.

93. Осипенко, А. Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие / А.Л. Осипенко // Вестник Нижегородской академии МВД России. – 2017. – № 4 (40). – С. 181–188.

94. Кардашевская, М. В. Электронная платежная система как элемент обстановки преступления / М. В. Кардашевская, Ю. В. Гаврилин // Академическая мысль. 2020. № 2 (11). С. 21–23.

95. Коломинов, В. В. Установление места совершения преступления в процессе расследования мошенничества в сфере компьютерной информации / В. В. Коломинов // Криминалистические чтения на Байкале – 2015 : материалы Международной научно-практической конференции, Иркутск, 18–19 июня 2015 года / ответственный редактор Д. А. Степаненко ; Российский государственный университет правосудия, Восточно-Сибирский филиал. – Иркутск, 2015. – С. 264–268.

96. Комаров, И. М. Правовые и криминалистические проблемы расследования мошенничества в сфере компьютерной информации / И. М. Комаров // Преступность в сфере информационных и

телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2015. – № 1. – С. 12–15.

97. Кравец, Е. Г. Комплекс специальных знаний, необходимых при расследовании хищений, совершаемых с использованием вредоносных компьютерных программ / Е. Г. Кравец, Н. В. Шувалов // Юридическая наука и правоохранительная практика. – 2020. – № 3 (53). – С. 119–126.

98. Куемжиева, С. А. Понятие следственной ситуации и ее роль в определении средств и методов отдельного расследования / С. А. Куемжиева // Вестник Краснодарского университета МВД России. – 2015. – № 4(30). – С. 191-195.

99. Куликова, И. Е. Особенности проведения некоторых оперативно-разыскных мероприятий при раскрытии мошенничеств, совершаемых с использованием средств мобильной связи и методов социальной инженерии / И. Е. Куликова // Российский следователь. – 2022. – № 7. – С. 70–74.

100. Кузьмин, М. Н. К вопросу проведения тактики следственных действий по уголовным делам, связанным с мошенничеством в сфере компьютерной информации / М. Н. Кузьмин, Е. В. Пахомова // Юристъ-Правоведъ. – 2022. – № 3 (102). – С. 69–72.

101. Лантух, Э. В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э. В. Лантух, В. С. Ишигеев, О. П. Грибунов // Всероссийский криминологический журнал. – 2020. – Т. 14, № 6. – С. 882–890.

102. Малыхина, Н. И. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети Интернет / Н. И. Малыхина, С. В. Кузьмина // Вестник Томского государственного университета. – 2021. – № 462. – С. 238–247.

103. Мадянов, А. В. Использование методов профайлинга и верификации в ходе предварительного расследования / А. В. Мадянов, Н. Ю. Васильева, С. Н. Болховитина // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3-2. – С. 329–333.

104. Муравьев, К. В. Современные возможности судебно-компьютерной экспертизы и меры по совершенствованию практики ее назначения при расследовании преступлений, связанных с незаконным оборотом наркотических средств «дистанционным» способом / К. В. Муравьев, М. Г. Ермаков // Вестник Восточно-Сибирского института МВД России. – 2019. – № 3 (90). – С. 182–192.

105. Меркулова, М. В. О некоторых проблемах осмотра персонального компьютера / М. В. Меркулова // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика : сборник статей XVIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае». Вып. 16 / ответственные редакторы С. И. Давыдов, В. В. Поляков ; Алтайский государственный университет. – Барнаул : Изд-во Алт. ун-та, 2020. – С. 153–156.

106. Науменко, О. А. Криминалистические аспекты исследования цифровых объектов при расследовании преступлений / О.А. Науменко, В. Д. Халин // Общество и право. – 2023. – № 3 (85). – С. 76-81.

107. Науменко, О. А. Проблемы в расследовании уголовных дел о мошенничестве, совершенном с использованием информационной среды / О. А. Науменко // Вестник Краснодарского университета МВД России. – 2019. – № 3 (45). – С. 60–64.

108. Науменко, О. А. О криминалистическом прогнозировании мошенничеств в сети Интернет / О. А. Науменко // Вестник Краснодарского университета МВД России. – 2021. – № 4 (54). – С 72–76.

109. Осипенко, А. Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие / А. Л. Осипенко // Юридическая наука и практика : Вестник Нижегородской академии МВД России. – 2017. – № 4 (40). – С. 181–188.

110. Выявление и раскрытие хищений денежных средства с лицевых счетов банковских карт граждан : отчет о НИР / Т. В. Попова, А. А. Васильченко, А. В. Котяжов, М. В. Дульцев. – Москва : Академия управления МВД России, 2017. – 115 с.

111. Перякина, М. П. Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства / М. П. Перякина, С. В. Унжакова, Н. Э. Шишкина // Сибирский юридический вестник. – 2019. – № 3 (86). – С. 81–85.

112. Поляков, В. В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. – 2013. – № 2-1 (78). – С. 114–116.

113. Першин, А. Н. «Техническое противодействие» расследованию преступления: понятие и содержание / А. Н. Першин, М. В. Бондарева // Российский следователь. – 2022. – № 7. – С. 7–11.

114. Першин, А. Н. Осмотр сетевых информационных ресурсов – новый вид следственного действия? / А. Н. Першин // Российский следователь. – 2020. – № 1. – С. 13–16.

115. Сааков, Т. А. Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора / Т. А. Сааков // Законы России: опыт, анализ, практика. – 2020. – № 4. – С. 96–103.

116. Семикаленова, А. И. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики / А. И. Семикаленова, И. А. Рядовский // Актуальные проблемы российского права. – 2019. – № 6 (103). – С. 178–185.

117. Соколов, А. Б. Организационно-тактическая деятельность следователя на подготовительном этапе проведения обыска / А. Б. Соколов, А. П. Мясников, О. В. Сергеева // Криминалистика: вчера, сегодня, завтра. – 2021. – № 4 (20). – С. 77–87.

118. Скоробогатов, К. С. Использование специальных знаний при расследовании мошенничества в сфере компьютерной информации / К. С. Скоробогатов // Пермский период : сборник материалов IX Международного

научно-спортивного фестиваля курсантов и студентов образовательных организаций, Пермь, 16–20 мая 2022 года. Том 1 / Пермский институт Федеральной службы исполнения наказаний. – Пермь, 2022. – С. 296–298.

119. Сидорова, К. С. Алгоритм действий следователя при расследовании мошенничеств, совершаемых дистанционным способом / К. С. Сидорова // Закон и право. – 2020. – № 12. – С. 230–233.

120. Скобелин, С. Ю. Использование специальных знаний при работе с электронными следами / С. Ю. Скобелин // Российский следователь. – 2014. – № 20. – С. 31–33.

121. Смушкин, А. Б. Виртуальные следы в криминалистике / А. Б. Смушкин // Законность. – 2012. – № 8 (934). – С. 43–45.

122. Флеров, О. В. Цифровой след человека в Интернете: основные гуманитарные подходы / О. В. Флеров // Образовательные ресурсы и технологии. – 2018. – № 4 (25). – С. 79–82.

123. Харина, Е. А. Некоторые аспекты квалификации мошенничества в сфере компьютерной информации / Е. А. Харина // Российский следователь. – 2022. – № 6. – С. 38–41.

124. 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.

125. Харина, Е. А. Личность типичного преступника, совершившего мошенничество в сфере компьютерной информации / Е. А. Харина // Российский следователь. – 2023. – № 9. – С. 53–57.

126. Харина, Е. А. К вопросу о криминалистической характеристике мошенничества в сфере компьютерной информации / Е. А. Харина // Российский следователь. – 2023. – № 11. – С. 11–15.

127. 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.

128. 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.

129. Шурыгина, Д. С. Особенности криминалистической характеристики потерпевших по компьютерным преступлениям / Д. С. Шурыгина, В. В. Поляков // Проблемы правовой и технической защиты информации. – 2018. – № 6. – С. 162-166.

130. Щербаченко, А. К. Типичные версии о мошенничестве, совершенном группой лиц, и их место в системе базовой методики их раскрытия и расследования / А. К. Щербаченко // Философия права. – 2020. – № 1 (92). – С. 165–169.

131. Яблоков, Н. П. Криминалистическая классификация преступлений в методике расследования и ее виды / Н. П. Яблоков // Вестник Московского университета. Серия 11, Право. – 2015. – № 5. – С. 40–51.

Судебная практика

132. Приговор Братского городского суда Иркутской области от 19 декабря 2016 г. № 1-558/2016. – URL: https://sudact.ru/regular/doc/g09gU4WUC15J/ (дата обращения: 15.07.2022).

133. Приговор Кировского районного суда г. Екатеринбурга от 08 февраля 2022 г. № 1-1. – URL: https://kirovsky--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=2&name_op=doc&number=352801331&delo_id=1540006&new=0&text_number=1 (дата обращения: 10.10.2023).

134. Приговор Кировградского городского суда Свердловской области от 05 августа 2016 г. № 1-105/2016. – URL: https://sudact.ru/regular/doc/b2ynlm3ERQJ9 (дата обращения: 15.12.2022).

135. Приговор Кизилюртовского городского суда Республики Дагестан от 11 июня 2014 г. № 1-49/2014. – URL:https://sudact.ru/regular/doc/7Mcxk2HXGclB/ (дата обращения: 07.08.2022).

136. Приговор Октябрьского районного суда г. Барнаула Алтайского края от 20 апреля 2017 г. по уголовному делу № 1-18/2017 // Архив Октябрьского районного суда г. Барнаула Алтайского края.

137. Приговор Октябрьского районного суда г. Владимира от 04 июня 2019 г. № 1-95/2019. – URL: https://sudact.ru/regular/doc/v59eyhN7lzJq/ (дата обращения: 25.07.2022).

138. Приговор Приволжского районного суда г. Казани Республики Татарстан от 09 ноября 2018 г. № 1-588/18. – URL: https://sudact.ru/regular/doc/o3PSlcynw8Lv (дата обращения: 02.08.2022).

139. Приговор Промышленного районного суда г. Самары от 30 августа 2016 г. по делу № 1-478/2016. – URL: https://sudact.ru/regular/doc (дата обращения 13.08.2022).

140. Приговор Уссурийского районного суда Приморского края от 06 июня 2017 г. № 1-513/2017. – URL: https://sudact.ru/regular/doc/P8NIXBB0caLC (дата обращения: 13.08.2022).

141. Приговор Центрального районного суда г. Тюмени от 3 сентября 2018 г. № 1-18/2018 1-528/2017. – URL: https://sudact.ru/regular/doc/rui CsHOBEBUQ (дата обращения: 15.07.2022).

142. Приговор Якутского городского суда Республики Саха (Якутия) от 26 августа 2019 г. № 1-681/2019. – URL: https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения: 08.08.2022).

143. Уголовное дело № 1-675/2019 // Архив Советского районного суда г. Красноярска.

144. Уголовное дело № 1-414/15 // Архив Индустриального районного суда г. Барнаула.

145. Уголовное дело № 1-675/2019 // Архив Советского районного суда г. Красноярска.

Статистические и иные аналитические материалы, электронные информационные ресурсы

146. Выступление В. В. Путина на расширенном заседание коллегии МВД. – URL: http://www.kremlin.ru/events/president/news/70744 (дата обращения: 01.11.2023).

147. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России. – URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения: 11.12.2022).

148. Официальный сайт МВД России. Статистика и аналитика. – URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 01.11.2023).

149. Официальный сайт Судебного департамента при Верховном суде Российской Федерации. – URL: https:// http://www.cdep.ru/ (дата обращения: 19.02.2023).

150. Обзор отчетности Банка России об инцидентах информационной безопасности при переводе денежных средств. – URL: http://www.cbr.ru/analytics/ib/review_3q_2022 (дата обращения: 11.12.2022).

151. Отчет об утечке данных за 1 полугодие 2022 года. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (дата обращения: 08.01.2023).

152. Антоненков, Д. «Идет невидимая война. Мы стали ее участниками». Обвиняемые рассказывают историю группы хакеров Lurk / Д. Антоненков. – URL: https://66.ru/news/internet/248291/ (дата обращения: 01.07.2022).

153. Братья по кибероружию. – URL: https://blog.group-ib.ru/brothers/ (дата обращения: 29.12.2022).

154. Большое банковское ограбление: APT-кампания Carbanak. – URL: https://securelist.ru/bolshoe-bankovskoe-ograblenie-apt-kampaniya-carbanak/25106/ (дата обращения: 04.01.2023).

155. Дропология. Как вербуют дропов, чему обучают и как используют. – URL: https://teletype.in/@osintology/dropologiya (дата обращения: 04.11.2022).

156. В Испании задержан лидер «самой успешной» хакерской группировки Carbanak. – URL: https://www.vedomosti.ru/technology/articles/2018/03/26/754928-ispanii-hakerskoi (дата обращения: 03.02.2023).

157. Киберугрозы для АСУ и промышленных предприятий в 2022 году. – URL: https://securelist.ru/threats-to-ics-and-industrial-enterprises-in-2022/103980 (дата обращения: 08.11.2022).

158. Корпоративный фишинг и спам в 2022 году: все чаще атакуют HR-специалистов и бухгалтеров. – URL: https://www.kaspersky.ru/about/press-releases/2022_korporativnyj-fishing-i-spam-v-2022-godu-vsyo-chashe-atakuyut-hr-specialistov-i-buhgalterov (дата обращения: 22.01.2023).

159. Нефедова, М. Арестован лидер хакерской группы Cobalt (она же Carbanak) / М. Нефедова. – URL: https://xakep.ru/2018/03/27/cobalt-arrests (дата обращения: 04.01.2023).

160. Русскевич, Е. А. Мошенничество в сфере компьютерной информации: вопросы квалификации [видеозапись круглого стола Павел Яни, Е.А. Русскевич] // YouTube. 15 февраля 2021. – URL: https://youtu.be/knpXHRh2xQc (дата обращения: 15.08.2022).

161. Роскомнадзор подтвердил факт утечки данных из МТС-банка. – URL: https://www.vedomosti.ru/finance/articles/2023/10/19/1001370-roskomnadzor-podtverdil-fakt-utechki-dannih-iz-mts-banka (дата обращения: 29.10.2023).

162. Стоянов, Р. Охота на Lurk / Р. Стоянов. – URL: https://securelist.ru/the-hunt-for-lurk/29220 (дата обращения: 20.12.2022).

163. Стоянов, Р. Русскоязычная финансовая киберпреступность: как это работает / Р. Стоянов. – URL: https://securelist.ru/russkoyazychnaya-finansovaya-kiberprestupnost-kak-eto-rabotaet/27338 (дата обращения: 04.02.2023).

164. Суд дал хакерам от 10 до 13 лет по делу о взломе билетных баз РДЖ и S7. – URL: https://www.rbc.ru/society/25/12/2019/5e00c7bf9a794770d60099a0 (дата обращения: 04.08.2022).

165. Сценарии логических атак на банкоматы. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/atm-vulnerabilities-2018 (дата обращения: 08.01.2023).

166. ТОП-5 самых защищенных и безопасных мессенджеров 2023 года. – URL: https://trashexpert.ru/software/security/best-secure-and-encrypted-messaging-apps (дата обращения: 08.01.2023).

167. Управление «К» МВД РФ заблокировало два популярных «кардерских» ресурса. – URL: https://habr.com/ru/news/650321 (дата обращения: 24.01.2023).

168. Фигурантам уголовного дела о неправомерном обороте средств платежей предъявлены обвинения. – URL: https://мвд.рф/mvd/structure1/Upravlenija/убк/Publikacii_i_vistuplenija/item/28647999 (дата обращения: 24.01.2023).

169. Хакеры-близнецы Попелыши сели в тюрьму со второго раза. – URL: https://news.rambler.ru/crime/40132145-hakery-bliznetsy-popelyshi-seli-v-tyurmu-so-vtorogo-raza/ (дата обращения: 28.12.2022).

170. Шульмин, А. Банковский троянец Lurk: специально для России / А. Шульмин, М. Прохоренко. – URL: https://securelist.ru/bankovskij-troyanec-lurk-specialno-dlya-rossii/28708 (дата обращения: 20.12.2022).

171. Что такое Emolet и как от него защититься. – URL: https://www.kaspersky.ru/resource-center/threats/emotet (дата обращения: 12.12.2022).

172. Экскалация киберугрозы: Group-IB проанализировала ключевые тренды развития киберпреступности. – URL: https://www.group-ib.ru/media-center/press-releases/gib-2021-2022-report (дата обращения: 11.12.2022).

173. 10 громких преступлений, за которыми стояли русские хакеры. – URL: https://vc.ru/flood/92374-10-gromkih-prestupleniy-za-kotorymi-stoyali-russkie-hakery (дата обращения: 02.02.2023).

174. Cobalt (хакерская группа). – URL: https://ru.wikipedia.org/wiki/Cobalt_(хакерская_группа) (дата обращения: 12.01.2022).

175. Group-IB: несмотря на арест лидера, группа Cobalt продолжает атаки на банки. – URL: https://www.group-ib.ru/media-center/press-releases/gib-cobalt-activity (дата обращения: 04.01.2023).

ПРИЛОЖЕНИЯ

Приложение 1

АНАЛИТИЧЕСКАЯ СПРАВКА
по результатам анкетирования сотрудников правоохранительных органов, занимающихся выявлением, раскрытием, расследованием мошенничества в сфере компьютерной информации

Анкетирование проводилось среди 1240 сотрудников правоохранительных органов, занимающихся выявлением, раскрытием, расследованием мошенничества в сфере компьютерной информации: 215 оперуполномоченных (далее о/у), 612 следователей, 413 дознавателей, в 67 субъектах Российской Федерации: 1) Алтайский край – 13 чел. (13 следователей); 2) Амурская область 15 чел. (14 следователей, 1 о/у); 3) Архангельская область – 67 чел. (33 следователя, 30 дознавателей, 4 о/у); 4) Байконур – 4 чел. (1 следователь, 3 дознавателя); 5) Белгородская область – 5 чел. (5 о/у); 6) Брянская область – 6 чел. (6 дознавателей); 7) Владимирская область – 1 чел. (1 следователь); 8) Волгоградская область – 2 чел. (1 дознаватель, 1 о/у); 9) Воронежская область – 9 чел. (8 следователей, 1 о/у); 10) город федерального значения Севастополь – 1 чел. (1 о/у); 11) Еврейская автономная область – 24 чел. (22 следователя, 2 о/у); 12) Забайкальский край – 12 чел. (12 о/у); 13) Ивановская область – 49 чел. (16 следователей, 28 дознавателей, 5 о/у); 14) Иркутская область – 146 чел. (143 следователя, 3 о/у); 15) Кабардино-Балкарская Республика – 22 чел. (17 следователей, 5 о/у); 16) Калининградская область – 2 чел. (2 дознавателя); 17) Камчатский край – 3 чел. (3 о/у); 18) Карачаево-Черкесская Республика – 4 чел. (4 дознавателя); 19) Кемеровская область (Кузбасс) – 1 чел. (1 о/у); 20) Кировская область – 10 чел. (10 о/у); 21) Костромская область – 4 чел. (2 следователя, 2 о/у); 22) Краснодарский край – 8 чел. (8 о/у); 23) Красноярский край – 4 чел. (4 о/у); 24) Курганская область – 57 чел. (7 следователей, 44 дознавателя, 6 о/у); 25) Курская область – 6 чел. (1 следователь, 4 дознавателя, 1 о/у); 26) Москва – 1 чел. (1 о/у); 27) Московская область – 63 чел.

(3 следователя, 56 дознавателей, 4 о/у); 28) Ненецкий автономный округ – 19 чел. (11 следователей, 5 дознавателей, 3 о/у); 29) Нижегородская область – 6 чел. (2 следователя, 3 дознавателя, 1 о/у); 30) Новгородская область – 3 чел. (1 следователь, 2 о/у); 31) Новосибирская область – 54 чел. (47 следователей, 7 дознавателей); 32) Омская область – 1 чел. (1 следователь); 33) Оренбургская область – 12 чел. (9 следователей, 3 о/у); 34) Орловская область – 11 чел. (4 следователя, 4 дознавателя, 3 о/у); 35) Пензенская область – 7 чел. (7 о/у); 36) Псковская область – 5 чел. (5 следователей); 37) Республика Адыгея (Адыгея) – 42 чел. (33 следователя, 3 дознавателя, 6 о/у); 38) Республика Башкортостан – 11 чел. (2 следователя, 9 о/у); 39) Республика Бурятия – 11 чел. (1 следователь, 10 о/у); 40) Республика Коми – 14 чел. (7 следователей, 7 о/у); 41) Республика Крым – 35 чел. (25 следователей, 8 дознавателей, 2 о/у); 42) Республика Марий Эл – 2 чел. (2 о/у); 43) Республика Мордовия – 10 чел. (10 следователей); 44) Республика Северная Осетия – Алания – 6 чел. (6 о/у); 45) Республика Татарстан – 1 чел. (1 следователь); 46) Республика Тыва – 27 чел. (20 следователей, 7 дознавателей); 47) Республика Хакасия – 4 чел. (1 дознаватель, 3 о/у); 48) Ростовская область – 5 чел. (5 следователей); 49) Рязанская область – 1 чел. (1 о/у); 50) Самарская область – 77 чел. (50 следователей, 21 дознаватель, 6 о/у); 51) Саратовская область – 1 чел. (1 о/у); 52) Ставропольский край – 65 чел. (23 следователя, 42 дознавателя); 53) Тамбовская область – 5 чел. (5 о/у); 54) Тверская область – 11 чел. (5 дознавателей, 6 о/у); 55) Томская область – 1 чел. (1 о/у); 56) Тульская область – 4 чел. (4 о/у); 57) Тюменская область – 63 чел. (58 дознавателей, 5 о/у); 58) Удмуртская Республика – 21 чел. (21 дознаватель); 59) Ульяновская область – 7 чел. (2 следователя, 5 дознавателей); 60) Хабаровский край – 27 чел. (19 следователей, 1 дознаватель, 7 о/у); 61) Ханты-Мансийский автономный округ – Югра – 52 чел. (29 следователей, 11 дознавателей, 12 о/у); 62) Челябинская область – 11 чел. (11 о/у); 63) Чеченская Республика – 38 чел. (20 следователей, 14 дознавателей, 4 о/у); 64) Чувашская Республика – Чувашия – 23 чел. (19 дознавателей, 4 о/у); 65) Чукотский автономный округ – 1 чел. (1 о/у); 66) Ямало-Ненецкий автономный округ – 3 чел. (3 о/у); 67) Ярославская область – 4 чел. (4 следователя).

1. Укажите Ваш регион	
2. Укажите Вашу должность	
Следователь	612 (49,4 %)
Дознаватель	413 (33,3 %)
Оперуполномоченный	215 (17,3 %)
3. Укажите Ваш стаж работы в правоохранительных органах	
До 5 лет	389 (31,4 %)
От 5 и более лет	851 (68,6 %)
4. Приходилось ли Вам выявлять, раскрывать, расследовать преступления, предусмотренные ст. 159.6 УК РФ (Мошенничество в сфере компьютерной информации)?	
Приходилось	240 (19,4 %)
Не приходилось	1000 (80,6 %)
5. В связи с исключением «обмана и злоупотребления доверием» из числа обязательных признаков деяния, предусмотренного ст. 159.6 УК РФ, считаете ли Вы верным отнесение этого преступления к одному из видов мошенничества?	
Да	683 (55,1 %)
Нет	230 (18,5 %)
Затрудняюсь ответить	327 (26,4 %)
6. Укажите, какие преступления являются сопутствующими при совершении мошенничества в сфере компьютерной информации? *(Возможно указание нескольких вариантов ответа)*	
ст. 272 УК РФ (Неправомерный доступ к компьютерной информации)	1098 (88,5 %)
ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ)	655 (52,8 %)
ст. 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей)	349 (28,1 %)
ст. 274.1 УК РФ (Неправомерное воздействие на критическую информационную инфраструктуру РФ)	144 (11,6 %)
ст. 274.2 УК РФ (Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования)	223 (18 %)
Затрудняюсь ответить	9 (0,7 %)
Другое, *из них, в том числе: ст. 137 УК РФ, ст. 138 УК РФ, ст. 174 УК РФ, ст. 183 УК РФ, ст. 187 УК РФ.*	7 (0,5 %)
7. Укажите, какие виды имущества наиболее часто становились предметами мошенничества в сфере компьютерной информации? *(Возможно указание нескольких вариантов ответа)*	
Наличные денежные средства	264 (21,3 %)
Безналичные денежные средства	1057 (85,2 %)
Электронные денежные средства	596 (48,1 %)
Криптовалюта	345 (27,8 %)
Цифровая валюта	182 (14,7 %)
Денежные суррогаты (премиальные мили, игровая валюта и т.п.)	99 (8 %)
Затрудняюсь ответить	10 (0,8 %)
Другое	5 (0,4 %)

8. Укажите источники получения информации о мошенничестве в сфере компьютерной информации *(Возможно указание нескольких вариантов ответа)*	
От потерпевших физических лиц	1128 (91 %)
От потерпевших юридических лиц	578 (46,6 %)
В результате расследования других преступлений	295 (23,8 %)
В результате проведения ОРМ	378 (30,5 %)
В результате добровольной явки преступника с повинной	85 (6,9 %)
В результате инициативного выявления мошенничества в сфере компьютерной информации	193 (15,6 %)
Агентурный аппарат	101 (8,1 %)
Затрудняюсь ответить	12 (0,9 %)
Другое	4 (0,3 %)
9. Укажите, возможно, ли инициативное выявление мошенничества в сфере компьютерной информации оперативными сотрудниками?	
Да	709 (57,2 %)
Нет	140 (11,3 %)
Затрудняюсь ответить	391 (31,5 %)
10. Укажите наиболее распространенные способы подготовки мошенничества в сфере компьютерной информации *(Возможно указание нескольких вариантов ответа)*	
Получение специальных познаний в сфере компьютерной информации	774 (62,4 %)
Приобретение соответствующих компьютерных, технических, аппаратных средств, необходимых для совершения преступления	688 (55,5 %)
Приискание соисполнителей	308 (24,8 %
Приискание соответствующих вредоносных программ, баз данных и т.п.	566 (45,6 %)
Открытие банковских счетов, регистрация электронных кошельков и т.п., в том числе на подставных лиц	803 (64,8 %)
Изучение организации работы юридического лица, в отношении которого планируется совершение преступления	242 (19,5 %)
Регистрация в различных мессенджерах, обеспечивающих конспиративность общения	596 (48,1 %)
Регистрация SIM-карт на подставных лиц	736 (59,4 %)
Аренда серверов, в том числе, расположенных на территории других государств	489 (39,4 %)
Получение сведений о логинах, паролях	578 (46,6 %)
Создание «фишинговых» сайтов	614 (49,5 %)
Затрудняюсь ответить	8 (0,6 %)
Другое	3 (0,2 %)
11. Укажите, проведение каких наиболее распространенных действий, осуществляется при проверке сообщения о совершении мошенничества в сфере компьютерной информации? *(Возможно указание нескольких вариантов ответа)*	
Получение объяснений	948 (76,5 %)
Проведение осмотра места происшествия, предметов, документов	731 (59 %)
Направление запросов, получение необходимых выписок, истребование документов	998 (80,5 %)
Назначение и производство судебных экспертиз	442 (35,6 %)
Проведение различного рода проверок, ревизий	174 (14 %)
Получение образцов для сравнительного исследования	120 (9,6 %)
Исследование документов и предметов	519 (41,9 %)

Проведение ОРМ	637 (51,4 %)
Затрудняюсь ответить	28 (2,2 %)
Другое	3 (0,2 %)
12. Укажите, какие носители цифровых следов наиболее часто изымаются в ходе раскрытия и расследовании рассматриваемых преступлений? *(Возможно указание нескольких вариантов ответа)*	
Смартфоны, сотовые телефоны, радиостанции	1045 (84,3 %)
Системные блоки персональных компьютеров, мониторы и другие периферийные устройства	848 (68,4 %)
Ноутбуки, планшеты, цифровые блокноты	823 (66,4 %)
Сканеры, принтеры	80 (6,5 %)
Смарт-часы и браслеты	60 (4,8 %)
Жесткие диски	710 (57,3 %)
USB-накопители, компакт-диски, карты памяти и другие накопители информации	719 (58 %)
Модемы, серверы	372 (30 %)
Видеотехника, фототехника	119 (9,6 %)
Затрудняюсь ответить	6 (0,5 %)
Другое	3 (0,2 %)
13. Укажите, какие ОРМ, наиболее часто проводятся при раскрытии, расследовании мошенничества в сфере компьютерной информации? *(Возможно указание нескольких вариантов ответа)*	
Опрос	683 (55,1 %)
Наведение справок	734 (59,2 %)
Сбор образцов для сравнительного исследования	136 (11 %)
Проверочная закупка	90 (7,3 %)
Исследование предметов и документов	594 (47,9 %)
Наблюдение	200 (16,1 %)
Отождествление личности	105 (8,5 %)
Обследование помещений, зданий, сооружений, участков местности и транспортных средств	292 (23,5 %)
Контроль почтовых отправлений, телеграфных и иных сообщений	297 (24 %)
Прослушивание телефонных переговоров	502 (40,5 %)
Снятие информации с технических каналов связи	739 (59,6 %)
Оперативное внедрение	107 (8,6 %)
Контролируемая поставка	41 (3,3 %)
Оперативный эксперимент	69 (5,6 %)
Получение компьютерной информации	809 (65,2 %)
14. Укажите наиболее распространенные способы совершения мошенничества в сфере компьютерной информации *(Возможно указание нескольких вариантов ответа)*	
Осуществление хищений у юридических лиц их сотрудниками посредством неправомерного доступа к информационной инфраструктуре	579 (46,7 %)
Осуществление хищений со счетов клиентов кредитных организаций посредством неправомерного воздействия вредоносных компьютерных программ на их компьютерные устройства (как правило, смартфоны, сотовые телефоны)	830 (66,9 %)
Посредством установления контроля за работой компьютерных устройств юридических лиц через предустановленное вредоносное программное обеспечение	352 (28,4 %)

Посредством неправомерного внесения вредоносными компьютерными программами изменений в платежные поручения юридических лиц	363 (29,2 %)
Посредством осуществления несанкционированного управления работой банкомата	190 (15,3 %)
Посредством создания и использования «фишинговых» сайтов	593 (47,8 %)
Затрудняюсь ответить	14 (1,1 %)
Другое	17 (1,3 %)
15. Согласны ли Вы с тем, что по уровню специальных познаний в сфере информационно-телекоммуникационных технологий, всех преступников рассматриваемых деяний можно условно разделить на: 1. «Матерых», высококвалифицированных специалистов; 2. Опытных специалистов; 3. Специалистов среднего уровня; 4. «Бытовых» преступников?	
Да	945 (76,2 %)
Нет	151 (12,2 %)
Затрудняюсь ответить	139 (11,2 %)
Другое	4 (0,3 %)
16. Укажите наиболее типичные следственные ситуации первоначального этапа расследования	
Имеется информация о способе совершения преступления, личности преступника, а также выявлены следы преступления	251 (20,2 %)
Имеется информация о способе совершения преступления, выявлены следы преступления, при этом сведения о личности преступника отсутствуют	658 (53,1 %)
Имеется информация о способе совершения преступления, при этом объем выявленных следов незначительный, сведения о личности преступника отсутствуют	630 (50,8 %)
Имеется информация о способе совершения преступления, выявлены следы преступления, имеются сведения о личности преступника, однако его местонахождение неизвестно	249 (20,1 %)
Затрудняюсь ответить	7 (0,5 %)
Другое	1 (0,1 %)
17. Укажите типичные следственные и процессуальные действия при расследовании мошенничества в сфере компьютерной информации *(Возможно указание нескольких вариантов ответа)*	
Осмотр места происшествия	569 (45,9 %)
Допрос	1007 (81,2 %)
Обыск	662 (53,4 %)
Выемка	785 (63,3 %)
Очная ставка	186 (15 %)
Получение образцов для сравнительного исследования	203 (16,4 %)
Изъятие электронных носителей информации	887 (71,5 %)
Осмотр предметов (документов)	887 (71,5 %)
Контроль и запись переговоров	299 (24,1 %)
Наложение ареста на имущество	374 (30,2 %)
Назначение экспертизы	842 (67,9 %)
Затрудняюсь ответить	3 (0,2 %)
Другое	2 (0,1 %)

18. Какие виды судебных экспертиз наиболее часто назначаются при раскрытии, расследовании мошенничества в сфере компьютерной информации? *(Возможно указание нескольких вариантов ответа)*	
Компьютерно-техническая	1206 (97,3 %)
Судебно-бухгалтерская	213 (17,2 %)
Дактилоскопическая	88 (7,1 %)
Почерковедческая	92 (7,4 %)
Экспертиза реквизитов документов	233 (18,8 %)
Судебно-психиатрическая	75 (6 %)
Другие виды экспертиз	111 (9 %)
19. Испытывали ли Вы трудности при назначении судебных компьютерно-технических экспертиз?	
Да	232 (18,7 %)
Нет	444 (35,8 %)
Не приходилось назначать	564 (45,5 %)
20. Укажите типичные следственные ситуации последующего этапа расследования	
Собранных по делу *доказательств достаточно*, при этом подозреваемый *признает* свою вину в совершении преступления	466 (37,6 %)
Собранных по делу *доказательств достаточно*, при этом подозреваемый *отрицает* свою вину в совершении преступления	412 (33,2 %)
Собранных по делу *доказательств достаточно*, подозреваемый *частично признает* свою вину в совершении преступления, при этом отрицает совершение сопутствующих преступлений	256 (20,6 %)
Собранных по делу *доказательств достаточно*, подозреваемый *частично признает* свою вину в совершении преступления, при этом отрицает совершение преступления в составе организованной преступной группы, организованного преступного сообщества	240 (19,4 %)
Собранных по делу *доказательств недостаточно*, при этом подозреваемый *признает* свою вину в совершении преступления	125 (10,1 %)
Собранных по делу *доказательств недостаточно*, при этом подозреваемый *отрицает* свою вину в совершении преступления	327 (26,4 %)
Собранных по делу *доказательств недостаточно*, при этом подозреваемый *частично признает* свою вину, при этом отрицает совершение сопутствующих преступлений	107 (8,6 %)
Собранных по делу *доказательств недостаточно*, при этом подозреваемый *частично признает* свою вину, при этом отрицает совершение преступления в составе организованной преступной группы, организованного преступного сообщества сопутствующих преступлений	138 (11,1 %)
Затрудняюсь ответить	40 (3,2 %)
Другое	17 (1,6 %)
21. С какими трудностями Вы сталкивались в ходе выявления, раскрытия, расследования мошенничества в сфере компьютерной информации? *(Возможно указание нескольких вариантов ответа)*	
Несвоевременное сообщение о преступлении, в результате чего частичная или полная утрата цифровых следов преступления	684 (55,2 %)
Сложности в установлении схемы совершения преступления и похищенных денежных средств из-за дробления, перенаправления похищенного на различные банковские счета, электронные кошельки, перевода в криптовалюту и т.п.	608 (49 %)
Сложности в определении размера похищенного	93 (7,5 %)

Сложности в установлении места совершения преступления в результате использования VPN-сервисов, программ-ремейлеров, анонимайзеров, управляющих серверов, расположенных на территории других государств	714 (57,6 %)
Совершение преступления из-за пределов РФ, отсутствие должного взаимодействия с правоохранительными структурами других государств	584 (47,1 %)
Недостаточный объем следовой картины преступления в результате работы вредоносных компьютерных программ	247 (19,9 %)
Сложности в установлении преступников в результате использования для общения мессенджеров, затрудняющих идентификацию пользователей, содержание разговоров, переписки	458 (36,9 %)
Сложности в установлении преступников в результате использования банковских и иных платежных карт, расчетных счетов, электронных кошельков и т.п., как правило, оформленных на подставных лиц	531 (42,8 %)
Отсутствие специальных познаний и должной квалификации лиц, производящих выявление, раскрытие, расследование преступления	284 (22,9 %)
Отсутствие методических рекомендаций по выявлению, раскрытию и расследованию мошенничества в сфере компьютерной информации	192 (15,5 %)
Длительный срок проведения экспертиз	216 (17,4 %)
Длительный срок получения ответов на запросы от кредитно-финансовых организаций, провайдеров и т.п.	582 (46,9 %)
Трудности в привлечении специалистов, обладающих соответствующими познаниями	242 (19,5 %)
Затрудняюсь ответить	53 (4,2 %)
Другое	6 (0,5 %)
22. Укажите типичные ошибки, допускаемые оперативными сотрудниками при выявлении и раскрытии мошенничества в сфере компьютерной информации *(Возможно указание нескольких вариантов ответа)*	
Ошибки в ходе проведения ОРМ	2803 (22,6 %)
Проведение не всего необходимого комплекса ОРМ	585 (47,2 %)
Недостаточное акцентирование внимания на проведении негласных ОРМ	215 (17,3 %)
Отсутствие нацеленности в раскрытии организованного мошенничества в сфере компьютерной информации	287 (23,1 %)
Установление не всех членов преступного объединения	283 (22,8 %)
Нераскрытие сопутствующих преступлений	210 (16,9 %)
Утечка информации о проведении проверочных действий	78 (6,3 %)
Уделение недостаточного внимания консультациям со специалистами	166 (13,4 %)
Ошибки в ходе обнаружения, изъятия, осмотра электронных носителей информации	246 (19,8 %)
Ошибки в ходе оформления результатов ОРД	145 (11,7 %)
Ошибки отсутствуют	218 (17,6 %)
Затрудняюсь ответить	21 (1,7 %)
Другое	5 (0,4 %)
23. Укажите типичные ошибки, допускаемые следователем (дознавателем) при расследовании мошенничества в сфере компьютерной информации *(Возможно указание нескольких вариантов ответа)*	
Неправильная квалификация преступных деяний	208 (16,8 %)
Несвоевременность проведения неотложных следственных действий	489 (39,4 %)
Ошибки в ходе изъятия, осмотра электронных носителей информации	242 (19,5 %)
Тактические ошибки подготовки, проведения следственных и иных действий	214 (17,3 %)
Ошибки при составлении процессуальных документов	115 (9,3 %)

Утечка информации относительно проведения следственных действий, что влечет утрату следов преступления	62 (5 %)
Нераскрытие сопутствующих преступлений	206 (16,6 %)
Установление не всех денежных счетов, задействованных в преступной схеме	277 (22,3 %)
Отсутствие нацеленности на раскрытие организованного мошенничества и изобличение всей преступной иерархии	168 (13,5 %)
Недостаточное взаимодействие с оперативными подразделениями	241 (19,4 %)
Уделение недостаточного внимания консультациям со специалистами, наряду с отсутствием специальных познаний в сфере компьютерной информации и опыта расследования таких уголовных дел	232 (18,7 %)
Упущение ошибок, допущенных оперативными сотрудниками при оформлении результатов ОРД	163 (13,1 %)
Ошибки отсутствуют	218 (17,4 %)
Затрудняюсь ответить	17 (1,3 %)
Другое	3 (0,2 %)
24. Чем, по вашему мнению, объясняется низкая раскрываемость организованного мошенничества в сфере компьютерной информации? *(Возможно указание нескольких вариантов ответа)*	
Высокий уровень организации преступления, в результате чего оставление незначительной следовой картины	694 (56 %)
Отсутствие у низовых исполнителей и подставных лиц информации об организаторах преступного объединения и/или других его членах в силу соблюдения конспиративности, использования в процессе общения друг с другом технических средств связи, исключающих или затрудняющих идентификацию	423 (34,1 %)
Сокрытие исполнителями информации об организаторах преступного объединения и/или других его членах	230 (18,5 %)
Использование в преступной деятельности высококачественных вредоносных компьютерных программ, оставляющих незначительный объем цифровых следов и/или способных к самоуничтожению	508 (41 %)
Использование в преступной деятельности высокотехнологичных компьютерных, аппаратных, технических средств и устройств, способствующих не изобличаемому совершению, а также сокрытию преступления	441 (35,6 %)
Уделение недостаточного внимания проведению комплекса ОРМ	182 (14,7 %)
Уделение недостаточного внимания консультациям со специалистами	132 (10,6 %)
Отсутствие единой базы данных цифровых следов	424 (34,2 %)
Отсутствие должной квалификации лиц, производящих выявление, раскрытие, расследование преступления	325 (26,2 %)
Отсутствие методических рекомендаций по выявлению, раскрытию и расследованию организованного мошенничества в сфере компьютерной информации	256 (20,6 %)
Затрудняюсь ответить	15 (1,2 %)
Другое	19 (1,5 %)
25. Как вы считаете, обладание преступниками соответствующими компьютерными устройствами, программно-аппаратными и другими техническими средствами, может ли являться одним из элементов обстановки мошенничества в сфере компьютерной информации?	
Да	934 (75,3 %)
Нет	83 (6,7 %)

Затрудняюсь ответить	223 (18 %)
26. Как вы считаете, нужна ли отдельная криминалистическая методика расследования мошенничества в сфере компьютерной информации?	
Нужна	995 (80,2 %)
Не нужна, так как имеются методики расследования других видов мошенничества	111 (9 %)
Затрудняюсь ответить	134 (10,8 %)
27. Как Вы считаете, более эффективно способствовать борьбе с данного вида преступлениями может методика, ориентированная на расследование:	
«Бытового» мошенничества	242 (19,5 %)
Организованного мошенничества	997 (80,4 %)
Другое	1 (0,1 %)

Приложение 2

Лист интервьюирования практических работников

1. Испытывали ли Вы трудности при выявлении, раскрытии, расследовании мошенничества в сфере компьютерной информации? Если да, то какие?

2. Какие меры могли бы способствовать более эффективному выявлению, раскрытию, расследованию рассматриваемых преступлений?

3. Укажите, совершаются ли вместе с деянием, предусмотренным ст. 159.6 УК РФ, другие сопутствующие преступления. Если да, то какие?

4. Укажите, возможна ли классификация типичных преступников по объему специальных познаний в сфере ИТТ. Если да, то какие группы Вы могли бы выделить?

5. Укажите характерные черты личности типичного преступника рассматриваемой категории преступлений.

6. Укажите, отличается ли следовая картина рассматриваемой преступной деятельности в зависимости от категории преступника.

7. Укажите, может ли являться дополнительным элементом его обстановки обладание соответствующими компьютерными устройствами, с помощью и посредством которых совершается мошенничество в сфере компьютерной информации.

8. Необходимо ли создание частной криминалистической методики расследования мошенничества в сфере компьютерной информации?

Приложение 3

АНАЛИТИЧЕСКАЯ СПРАВКА

по результатам интервьюирования практических работников

1. 80 % экспертов испытывали трудности при выявлении, раскрытии, расследовании мошенничества в сфере компьютерной информации. Среди наиболее актуальных эксперты отметили: низкую квалификацию сотрудников в данном направлении деятельности; недостаточную материальную оснащенность соответствующими техническими средствами и современным программным обеспечением; длительный срок получения ответов на запросы из банковских организаций, операторов сотовой связи; регистрация SIM-карт на вымышленные установочные данные либо полное отсутствие данных об абоненте; отсутствие единой базы данных со сведениями о цифровых следах данной преступной деятельности.

2. Среди мер, которые могли бы способствовать более эффективному выявлению, раскрытию, расследованию рассматриваемых преступлений, эксперты отметили: увеличение штата сотрудников, занимающихся выявлением, раскрытием, расследованием данным преступлений, повышение их квалификации; обеспечение сотрудников необходимыми техническими средствами, компьютерными устройствами, соответствующим программным обеспечением; заключение соглашений об электронном документообороте для ускорения получения ответов на запросы; создание единой базы данных цифровых следов; создание единого информационного поля с представителями банковских организаций, операторами сотовой связи, где сотрудники могли бы консультироваться по всем возникающим вопросам.

3. 50 % экспертов отметили, что одновременно с преступлением, предусмотренным ст. 159.6 УК РФ, совершаются сопутствующие преступления. По мнению экспертов, преимущественно ими являются преступления, предусмотренные главой 28 УК РФ «Преступления в сфере компьютерной

информации». Также сопутствующими преступлениями в данной сфере являются преступления, предусмотренные ст. 183, ст. 187 УК РФ.

4. Эксперты указали на возможность подразделения преступников исследуемой противоправной деятельности в зависимости от уровня обладания специальными познаниями в сфере ИТТ. При этом отметили следующие группы типичных преступников: высококвалифицированные специалисты, опытные преступники, специалисты среднего уровня, «бытовые» или «случайные» преступники.

5. Опрошенные эксперты указали, что высококвалифицированные специалисты обладают глубокими познаниями и большой степенью уверенности, к объекту посягательства относятся избирательно, способны сознанием охватить всю ситуацию и ее возможные исходы. Опытные преступники, как правило, не являются разработчиками компьютерных программ, однако могут заниматься их модификацией; избирательность объекта преступного посягательства не принципиальна; в социальной среде их можно определить как психологов. Специалисты среднего уровня обладают соответствующими познаниями на уровне уверенных пользователей. Характеризуются устойчивой увлеченностью к такого рода деятельности, при этом отсутствует должное усердие; их особенностью является иллюзорное представление о совершении резонансных преступлений; преобладает фрагментарное видение ситуации. «Бытовые», «случайные» преступники характеризуются обывательским уровнем соответствующих познаний, неуверенностью в своих действиях; в общении эмоциональны, преобладает хвастовство.

6. Эксперты указали, что в зависимости от уровня обладания преступниками познаниями в сфере ИТТ следовая картина их преступной деятельности (преимущественно это касается цифровых следов) существенно отличается. В зависимости от понижения уровня таких познаний следовая картина носит все более явный, обозримый характер.

7. Опрошенные эксперты указали, что обладание соответствующими компьютерными устройствами, с помощью и посредством которых совершается

мошенничество в сфере компьютерной информации, может являться одним из дополнительных элементов.

8. На вопрос «Необходимо ли создание частной криминалистической методики расследования мошенничества в сфере компьютерной информации?» опрошенные эксперты ответили утвердительно. Свою позицию по данному вопросу объясняли специфичностью рассматриваемой преступной деятельности, относительной новизной криминализованного преступного деяния и его невысоким криминалистическим исследованием.