МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра уголовно-правовых дисциплин

Рекомендовано к защите в ГЭК
Заведующий кафедрой,
канд. юрид. наук, доцент,
заслуженный юрист РФ
_____ В.И. Морозов
04 июня 2022 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистерская диссертация

РАССЛЕДОВАНИЕ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

40.04.01 Юриспруденция
Магистерская программа «Магистр права»

Выполнил работу
студент 2 курса
очной формы обучения — Рябцев Кирилл Антонович

Научный руководитель
канд. юрид. наук,
доцент — Вассалатий Жанна Васильевна

Рецензент
Заместитель прокурора
Тюменской межрайонной
природоохранной прокуратуры — Бугаев Иосиф Александрович

Тюмень
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

С начала XXI века информационно-коммуникационные технологии получили беспрецедентное развитие по всему миру, что, соответственно, открыло новые полезные возможности для удобства жизни человечества. В то же время, стремительное развитие повлекло и появление новых возможностей в совершении преступлений. Среди подобного рода явлений заметное место занимают всевозможные мошенничества.

Действительно, во всем мире отмечается колоссальный рост хищений, совершаемых с использованием информационных технологий. Представители преступной сферы, используя новые возможности, применяют новые способы и методы совершения преступлений, в том числе преступлений с привлечением информационных технологий - киберперступлений.

Статистика подтверждает серьёзность возникшей ситуации. В 2021 году в России зарегистрировано около 518 тыс. киберпреступлений, что на 1,4% больше, чем годом ранее, но сразу в 1,8 раза превосходит показатель 2019 года. В структуре киберпреступности доминировали мошенничества (статьи 159, 159.3, 159.6 Уголовного кодекса РФ) и кражи (пункт «г» части 3 статьи 158 УК РФ), которые в сумме составили 80 % от общего числа преступлений рассматриваемого вида [Состояние преступности…].

Порой совершение хищений с использованием информационных технологий происходит в совокупности со специальными составами главы 28 УК РФ. В них входят ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»; ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

Для дальнейшего ориентирования в теме научно-исследовательской работы следует провести анализ определений понятия «информационные технологии».

В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» «информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов».

Согласно научной работе советского и российского учёного Мизина И.А. и др., «термин "информационные технологии" появился в конце 70-ых годов XX века и его стали широко применять в связи с использованием современной электронной техники для обработки информации».

В настоящий момент в понятие информационных технологий (далее – ИТ) мы можем включить микроэлектронику, разработку и производство компьютеров и программного обеспечения, связь и телефонию, мобильные сервисы, обеспечение доступа в интернет, обеспечение информационных ресурсов интернета, средств вычислительной техники и связи.

Учитывая разнообразие определений, встречающихся как в нормативных документах, учебных материалах, так и в других источниках, наиболее верным видится следующее определение: ИТ - совокупность методов и технических средств поиска, сбора, хранения, обработки, предоставления и распространения графической, текстовой, цифровой, аудио- и видео- информации, а также все технологии и отрасли, на основе которых обеспечиваются перечисленные процессы.

В частности, уголовная ответственность за хищение с использованием информационных технологий в настоящее время предусмотрена тремя статьями: п. «г» ч. 3 ст. 158 УК РФ содержит особо квалифицированный состав – кража с банковского счета, а равно в отношении электронных денежных средств, ст. 159.3 УК РФ устанавливает ответственность за мошенничество с использованием электронных средств платежа, а также ст. 159.6 УК РФ.

Ежегодно киберпреступности удаётся осваивать новые изощрённые способы совершения преступных действий, которые чаще всего являются бесконтактными. Данная особенность ежедневно ставит перед сотрудниками

органов дознания и предварительного следствия весьма сложные задачи в разоблачении преступных деяний и фиксировании доказательств.

Только с недавнего времени такие понятия как IP-адрес, MAC-адрес, сетевой протокол, домен, сетевые мосты, фишинг, хостинг, VPN и многие другие, стали более узнаваемы и понимаемы сотрудниками правоохранительных органов, в связи с чем «виртуальные следы» стали доступней в понимании лиц, осуществляющих уголовное преследование. Тем не менее, обнаружение, фиксация и сохранение информации «виртуальных следов» остаётся для большинства сотрудников неподъёмной задачей.

Вызванная сложность происходит по ряду причин. В их числе:

1) Латентность преступления;
2) Сложность в квалификации разновидности преступлений;
3) Специфика данной категории преступлений;
4) Стремительное совершенствование информационных технологий, с использованием которых и совершаются преступления;
5) Сокрытие или уничтожение материальных и виртуальных следов преступления;
6) Недостаточная степень профессиональной подготовки субъектов расследования;
7) Как правило, высокая профессиональная подготовка преступников;
8) Недостаточность или же отсутствие координации совместных усилий правоохранительных органов с государственными и негосударственными структурами;
9) Редкое обновление методических рекомендаций;
10) Удалённость и трансграничный характер преступления;
11) Отсутствие единой практики фиксации цифровой информации;
12) Особенности технических процессов выявления информации, и иные факторы, способствующие возникновению проблем расследования данных преступлений.

Перечисленное обосновывает актуальность рассматриваемой темы, ее теоретическое и практическое значение, а самое главное – требует от ученых и исследователей больших усилий по всестороннему изучению проблем, связанных с расследованием рассматриваемого вида преступлений.

Особый интерес у практиков вызывает алгоритм следственных действий, комплекс тактических операций и комбинаций, от качества проведения которых зависит весь процесс расследования.

Цель диссертационного исследования - разработка комплекса тактикокриминалистических рекомендаций, направленных на повышение эффективности расследования хищений, совершаемых с помощью информационных технологий. Для реализации данной цели разработан комплекс следующих задач:

-рассмотрение элементов криминалистической характеристики хищений, совершаемых с использованием информационных технологий;

-изучение особенностей возбуждения уголовного дела о хищениях, совершаемых с использованием информационных технологий;

-изучение особенностей первоначального и последующих этапов расследования уголовных дел о хищениях, совершаемых с использованием информационных технологий;

-разработка алгоритма следственных действий в типовых ситуациях по делам о хищениях, совершаемых с использованием информационных технологий на первоначальном и последующем этапах расследования;

Объект исследования - теория и практика расследования хищений, совершаемых с использованием информационных технологий.

Предмет исследования - закономерности деятельности правоохранительных органов в сфере расследования хищений, совершаемых с использованием информационных технологий; нормы уголовно-процессуального
законодательства Российской Федерации, посвященные указанной

проблематике, материалы монографий, научных статей, а также учебная литература, затрагивающая расследование киберпреступлений.

Методологическую основу данной диссертации составляют формально-юридический, сравнительно-правовой, диалектический, логический и системно-правовой методы научного познания.

Нормативная база исследования включает в себя Конституцию Российской Федерации, действующее уголовное, уголовно-процессуальное и оперативно-розыскное законодательство, иные федеральные законы, подзаконные нормативные акты, регулирующие полномочия правоохранительных органов, различных учреждений, организаций, связанные с предоставлением услуг связи и возможностью контроля за информацией, передаваемой с помощью средств телекоммуникации, а также иные источники, связанные с темой исследования.

Теоретической основой данной научной работы выступают труды российских учёных: Р.С. Белкина, А.Ф. Волынского, А.В. Варданяна, Г.Г. Зуйкова, Е.П. Ищенко, А.Н. Колесниченко, А.М. Ларина, В.А. Образцова, Е.Р. Россинской, М.С. Строговича, С.А. Шейфера и других исследователей.

По своей структуре настоящая диссертация состоит из введения, двух глав, каждая из которых разбита на соответствующе параграфы, заключения, а также списка использованных источников.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. ПОНЯТИЕ И ОБЩИЕ ПОЛОЖЕНИЯ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Криминалистическая характеристика преступлений является одним из основных элементов методики расследования. Данное понятие изначально представил советский учёный-криминалист Колесниченко А. Н., относив его к наиболее существенным положениям, общих для всех частных методик.

На сегодняшний день научная литература может предложить достаточный объём исследовательского материала по текущему вопросу. Одним из таких является труд профессора Белкина Р.С., который определял «криминалистическую характеристику как результат научного анализа определенного вида преступной деятельности (вида или рода преступления), обобщения его типичных признаков и особенностей. Кроме того, криминалистическая характеристика обладает ориентирующим значением, чему служат вероятностные зависимости между её элементами». К тому же, изучив исследование Бессонова А.А., можно прийти к выводу, что криминалистическая характеристика определяет отправные особенности для методики расследования.

В ходе настоящей научно-исследовательской работы были проанализированы уголовные дела, связанные с хищением, совершаемым с использованием информационных технологий, в частности ст. 159.6 УК РФ. При проведении исследования подтвердилось, что криминалистическая характеристика крайне значима для расследования преступлений, а её чёткое толкование придаёт значительный темп в расследовании преступлений. Между тем, данная категория преступлений является достаточно специфичной и явно

отличается от иных преступлений, что, предположительно, вызвано цифровизацией и информатизацией общества.

На сегодняшний день информация является не только одной из главных ценностей человека, но и объектом хищений. С каждым днём предприятия, организации и учреждения всё больше применяют современные информационные технологии, с помощью которых осуществляется передача данных и информации, сохранность которых напрямую влияет на деятельность. Всё перечисленное так или иначе имеет отношение к глобальной сети Интернет.

С развитием автоматизированных систем пропорциональный рост приобретают и сами технологии для неправомерного доступа к данным и информации, что не может пользоваться криминальным интересом. Согласно анализу, количество и причиняемый вред от подобных хищений в последнее время только растут.

Статистика только подтверждает динамичный рост и масштабы текущей проблемы. За 2020 год было зарегистрировано свыше 510 400 преступлений, совершённых с использованием информационно-телекоммуникационных технологий, данный показатель на 73,6% больше, чем в 2019 год (294 409 преступления), что в свою очередь на 68,5% больше, чем в 2018 году (174 674), что на 92,8% выше показателей 2017 года (90 587). К тому же, по данным Генпрокуратуры РФ, раскрываемость киберпреступлений в России находится на отметке ниже 25%.

По заявлению начальника главного организационно-аналитического управления Генпрокуратуры Андрея Некрасова «За последние годы число преступлений, совершенных с использованием информационно телекоммуникационных технологий или в сфере компьютерной информации, возросло до масштабов, позволяющих говорить о них как об угрозе национальной безопасности», с чем трудно не согласиться.

Значительное увеличение численности хищений, совершаемых с использованием информационных технологий, и их усиливающийся рост организованности «стали причиной создания в практике органов внутренних дел

специализированных подразделений, предназначенных для борьбы с таким типом преступлений: профильных органов дознания; отделений (отделов) «К»; следственных подразделений - отделений (отделов) расследования хищений», совершаемых с использованием информационных технологий. Эти меры требуют организации тесного сотрудничества и взаимодействия между сотрудниками данных отделов внутренних дел [Мазуров].

Криминалистическая характеристика хищений, совершаемых с использованием информационных технологий имеет существенное значение и роль в расследовании обозначенной категории преступлений, а также выступает совокупностью «базовой информации, которая получена на основании анализа практической, оперативно-розыскной и экспертной деятельности».

Основные элементы криминалистической характеристики хищений, совершаемых с использованием информационных технологий:

1. Жертва преступления;
2. Личность преступника;
3. Способы осуществления хищений, совершаемых с использованием информационных технологий;
4. Место, время, обстоятельства, которые способствуют осуществлению хищений с использованием информационных технологий;
5. Механизмы следообразования хищений, совершаемых с использованием информационных технологий;
6. Цели и мотивы хищений;
7. Подлежащие выяснению обстоятельства.

Необходимо выделить следующие криминалистические особенности хищений, совершаемых с использованием информационных технологий:

1. Модификация, кодировка и преобразование получают моментальное пространственное распространение всеми существующими носителями в места с доступом в сеть Интернет;
2. Возникновение сложностей по изъятию информации, в виде определения изначальных данных их схемы и каналы передачи;

3. Очистка сведений при применении технических средств и устройств;
4. Деактивация информационных устройств с последующим устранением данных;
5. Заморозка информации с помощью материального воздействия, программного обеспечения и технических средств;
6. Преобразование, искажение компьютерных данных с использованием программного обеспечения;
7. Имитация данных на информационные носители, облачные источники информации с последующей рассылкой данных или торговлей сведений.

1.2. СПОСОБЫ СОВЕРШЕНИЯ И СОКРЫТИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Способы реализации преступлений являются базовой частью криминалистической характеристики преступлений. Следует выделить такие элементы как: способы подготовки, совершение преступления, сокрытие следов.

Ссылаясь на собственное мнение, способы реализации хищений, совершаемых с использованием информационных технологий, являются значимыми компонентами данной категории преступлений.

Учитывая исследование Белкина Р.С., способ реализации преступления - это преступные воздействия или же их совокупность, система действий, обращённые на выполнение установленной преступной цели. К тому же, возможно отметить, что способ сокрытия преступлений заслуживает особого места, так как он обособлен и содержит в себе фальсификацию и сокрытие следов преступлений [Белкин, с. 268].

По-нашему мнению, с такой точкой зрения сложно не согласиться, потому как способ сокрытия имеет достаточное влияние на раскрытие данного преступления.

Труды Белкина Р.С. в частности, могут наводить на мысль, что в случае установлении истины способы совершения и сокрытия преступлений являются базисными.

Изучив исследования Зуйкова Г.Г., вполне очевидно заметить, что учёный-криминалист рассматривал способ преступления в виде подготовки, совершения преступления, а также дальнейшего сокрытия следов. Учитывая мнение учёного, акцентирование происходит на психофизических особенностях определённой личности, в том числе условиям окружающей среды, что, в свою очередь, имеет влияние на осуществление преступлений [Зуйков, Белкин, с. 67].

Совокупность сведений, квалифицирующих характерные способы для совершения данных хищений, является главным компонентом криминалистической характеристики.

К вышеупомянутым способам следует отнести:

1. Проникновение напрямую в помещение в месте нахождения компьютерного снабжения, доступ к компьютерно-техническим аппаратам и информации;

2. Дистанционный доступ к компьютерно-техническим устройствам с использованием внешних, удалённых устройств для последующего изъятия данных;

3. Кодирование входной или выходной информации, команд управления и доступа, затруднение проникновения;

5. Модифицирование компьютерных программ, производство вредоносных программных обеспечений для удаления сведений, а также вывода устройства из строя;

6. Разработка спама, в равной степени сведений для продвижения рекламы и информации;

7. Неправомерное распространение сведений, программного обеспечения, правовых систем, книжных издательств, включающих компьютерные данные.

8. Комплексные способы.

В 53 % неправомерных инцидентах были применимы типовые способы получения доступа к компьютерным носителям и информации, равно к стороннему имуществу. Одними из учащённых способов: временное, а также постоянное изъятие компьютерной информации, с использованием мошенничества (обмана, введения в заблуждение и легендирования, производства несуществующих документированных данных), кражи, грабежа или разбоя; обращение в свою или иную пользу; повреждение различными способами или уничтожение данных, также применяя специализированные технические средства (магнит и электромагнитное поле), разработанных для уничтожения компьютерных данных.

Специфичные следы при применении таких средств:

1. Отметины инструментов или орудий взлома;
2. Одорологические следы;
3. Обнаруженное повреждение, уничтожение и/или модификация сигнальных (охранных) приспособлений, замков, запирающих устройств;
4. Фиксирование автоматическими системами охраны и доступа в помещения, которые содержат фото или видеофиксацию;
5. Отпечатки пальцев на технических приборах, магнитных носителях и различных проводах либо вспомогательных механизмах; следы соединительных проводов, материалов для изоляции, капельки припоя, флюса, канифоли;
6. Механическое сдавливание, надрезы, приклеивание сторонних предметов, проколы и проплавления изоляции на проводах компьютерно-технических устройств;
7. Признаки фальсификаций первичных документов, отражающих компьютерную информацию.

В 27 % преступлений, совершенных с использованием информационных технологий, были применены методы на основе средств дистанционного доступа к компьютерам и охраняемой информации. Одни из методов совершения преступления:

1) Компьютерно-технические средства в условиях прямой близости или дистанционного копирования, кодирования, модификации, ликвидации компьютерных данных с технического оборудования в целях передачи и обработки информации;
2) Вредоносные программы, посредством которых совершаются. В этом числе: вирусы, «троянский конь», «временная» и «логическая» бомбы, а также «троянская матрёшка»;
3) Программно-технические средства, производство которых направлено на хищение в случае использования интернет-технологий («генераторы паролей», «код-грабберы»);

4) Средства электросвязи для хищений с использованием информационных технологий;
5) Стандартные и транзитные программные обеспечения.

Специализированные орудия силовых структур, правоохранительных органов и спецслужб нередко используются и в самих преступлениях. Данные органы уполномочены: осуществлять перехват информации в случае применения средств разведки; оказывания воздействия на данные с помощью программ и технических средств с целью уничтожения информации или же её искажении в процессе передачи, хранении и обработки; контролирование электронных сообщений.

На 43% приходятся следующие способы хищений с использованием специализированных интернет-технологий:

1. Бесконтактный (пассивный) перехват - дистанционное осуществление перехвата электромагнитных излучений, которые испускают при работе компьютерно-технические средства (перехватывание акустических, электромагнитных, оптических сигналов и т.д.)
2. Контактный (активный) перехват в процессе подготовки к хищениям с использованием интернет-технологий. Данный способ совершается с помощью непосредственного подключения к компьютерным устройствам и системам, их сети или к специализированным техническим и радиоэлектронным средствам.
3. Использование вредоносных программ по внедрению различными способами в систему или сеть устройства. Применяются программы следующего вида:

1) Разведывательного направления: «троянский конь», «троянская матрешка» и другие;
2) «Компьютерный вирус», «временная» либо «логическая бомба» с помощью которых происходит повреждение средств хранения, передачи и обработки, а также уничтожение компьютерных данных для сбора сведений.

Типичными являются следы в виде показаний мониторинговой (регистрирующей) аппаратуры (пеленгующих и радиосканирующих устройств, компьютеризированных анализаторов для проводных сетей электросвязи);

12 % хищений на модификациях входных и (или) выходных данных, а также управляющих команд применяемых в случае экономических преступлений. Возможны варианты изменения системной информации, а также подмены документации после обработки документов.

Данные способы применяются в случае несоответствия специальным требованиям: в случаях недостаточного контроля службы безопасности, что может повлечь фальсификацию, которая совершается из корыстных побуждений (использование информации и документов на физических и электронных носителях). Вышеупомянутые способы также могут применяться и в иных преступных посягательствах: хищения денежных средств и ведение двойной, так называемой «чёрной», бухгалтерии. Попарное сравнение сведений может помочь обнаружить характерные следы способов хищений.

13 % приходятся на несанкционированное изменение программы и внедрение программных вредоносных средств, подразумевающими сбой технических средств и оборудования, что может принести результат в виде потери контроля над информацией и последующей возможности совершения хищения.

Другие 2 % включают распространение незаконных носителей, содержащих в себе информацию и данные охраняемые законом, оборот и распространение которых преследуется по закону. В их числе можно встретить секретные материалы, а также вредоносные программы. Под распространением данных машинных носителей понимается непосредственная передача третьим лицам. Например, неправомерное распространение контрафактных программ к компьютерно-технических средствам, повреждение и уничтожение баз данных и прочих объектов авторского права, находящихся на различных информационных носителях.

Использование различных комбинаций по получению данных является костяком для осуществления хищений.

Опираясь на настоящее исследование, в практически в 79% эпизодов хищений, совершаемых с использованием информационных технологий, происходит подготовка к преступлению, изучение места совершения преступлений, рассмотрение вероятности взлома, настройка программного обеспечения, приобретение дополнительного оборудования.

Справедливым будет сказать о том, что преступниками данной категории преступлений используются попытки обнаружения самого безопасного внедрения в компьютерно-техническое устройство. К тому же, преступники заинтересованы в полном или частичном уничтожении, или удалении виртуальных признаков взлома данных. Более половины устанавливают наблюдение за деятельностью потерпевшего с компьютерно-техническим устройством, проводят изучение особенности работы пользователя, жертвы, находят ошибки, слабости и пробелы, а также усваивают современную методическую литературу и способы получения информации.

1.3. ЛИЧНОСТЬ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО ХИЩЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Личность преступника является многогранной, специфичной и особенной частью криминалистической характеристики хищений, совершаемых с использованием информационных технологий.

Личность преступника являет собой важнейший элемент криминалистической характеристики хищений, совершаемых с использованием информационных технологий.

Особенностью данного элемента личности характерных преступников, совершаемых с использованием информационных технологий, принято находить в значительной степени профессиональной подготовки, а также в мастерство проведения анализа, группировки материала и умозаключения выводов. Между тем, нередко можно встретить наличие технического образования.

Согласно данному исследованию, хищения, совершаемые с использованием информационных технологий, приходятся в большей степени на долю мужчин. Данную категорию преступлений в исполнении женщин возможно встретить лишь в единичных эпизодах. Следует заметить высокий процент наличия высшего технического образования задержанных, он составляет 81%. В ходе данной работы было определено, что приблизительно 13% задержанных имеют два высших образования. Данный факт наводит на мысль, что хищения с использованием информационных технологий, а также области с применением интернет-технологий и в сфере интернет-технологий в современном мире реализовывают профессионалы, по каким-то обстоятельствам недооцененные окружающими.

Следует заметить, что явное опасение вызывает наличия тесных связей зарубежных и российских преступников, контакты которых явно включают обмен собственным опытом.

В подготовке, совершении и сокрытии хищений, совершаемых с использованием информационных технологий, между участниками происходит распределение ролей. Чаще всего распределение ролей имеет следующий вид:

Первая подгруппа с помощью разработки системы технических устройств с целью негласного получения данных неправомерно получает конфиденциальные сведения

Вторая подгруппа занимается обработкой полученных и систематизацией данных, а также разрабатывает планы преступной деятельности группы.

Третья подгруппа ответствена за перевод похищенных денежных средств на счета в офшоры, а также переводы и распределение данных и денежных средств.

Четвертая подгруппа занимается устранением следов преступления, формированием алиби и поиском сообщников.

Деятельность пятой подгруппы связана со специалистами по информационным технологиям в зарубежных государствах, обеспечивая преступную группу необходимыми материалами и орудиями, применяемых в процессе подготовки и осуществления хищений, совершаемых с использованием информационных технологий.

При анализе социального статуса лиц, осуществивших хищения, совершаемых с использованием информационных технологий, следует уделить внимание, что большая часть совершаемых преступлений не находит отражения в статистических данных. Скорее более подробно происходит анализ происшествий, привлекающих повышенное внимание.

Согласно нашим данным, все лица, совершивших хищения с использованием информационных технологий, имеют собственные особенности, например, наличия собственного «ника» известным в компьютерных и глобальных сетях. Происходит перераспределение ролей в различных направлениях преступной деятельности. Исключительно такие лица знают координаты руководителя и имеют возможность с ним общаться. Общение часто происходит с применением определенных каналов для связи.

Обычно ни рядовые члены группы, ни заместители руководителя того, с кем общаются, не знают в лицо. Так гарантируется максимальная скрытность, анонимность и безопасность лидера.

Возможность подобной ситуации проявляется посредством существования мобильных средств, а также функционирующих сегодня систем цифровой электросвязи: сотовая радиотелефонная и спутниковая связь, компьютерная сеть Интернет.

В абсолютном большинстве случаев (97%) преступники, совершавшие хищения с применением интернет-технологий, были служащими государственных организаций или учреждений, применяющих компьютерные технологии в собственных производственных процессах, при этом из них 30% непосредственно имели отношение к использованию компьютерной техники. С точки зрения исследователя интересным является та ситуация, что на каждую 1000 хищений, совершаемых с применением интернет-технологий, лишь 7 осуществляются программистами- профессионалами.

В соответствии с данными нашего исследования, преступник из числа работников организации - образцовый служащий, который получил соответствующее образование. Обычно указанные лица никаких преступлений раньше не совершали. Часто они являются руководителями различного уровня, которые обладают определенными распорядительными функциями, однако не отвечают непосредственно за конкретные участки.

К моменту осуществления хищений при помощи интернет-технологий преступники по уровню образования имели: 40% - высшее; 40% - среднее специальное; 20% - среднее.

Гораздо чаще хищения при использовании информационных средств применяются преступными группами с устойчивым составом, которые обладают мобильностью, основательной технической оснащенностью и имеют четкое разделение функций, корыстной мотивацией, а также детальной системой по сокрытию следов совершенных преступлений. Высококвалифицированные профессионалы, имеющие специальные знания в сфере негласного получения и

защиты информации, а также входящие в преступные группировки, представляют собой наибольшую опасность для определения и раскрытия преступных деяний. Кроме того, значительная часть хищений с применением информационных технологий, совершённых вышеуказанными субъектами, остаются латентными.

Распределение согласно возрастам у лиц, совершавших хищения с применением интернет-технологий, отображает тенденции к накоплению данного типа криминала среди молодых людей.

Большая часть опрошенных имеет высшее образование, полученное в технических вузах, или закончили техникумы.

Обратившись к результатам работы, представляется возможным сделать вывод, согласно которому около половины имеют образование специализированных физико-математических школ. Наличие отметки о службе в вооружённых силах РФ у 47% обследованных. Около 70% из 360 человек состояли в браке, из которых у 67% в благоприятных семейных отношениях, у других брак был на грани расторжения; у остальных 6% было расторжение брака. Оставшиеся обследуемые никогда не состояли в брачных отношениях. У 78% преступных субъектов хищений с использованием информационных средств, были дети.

Так как хищения с использованием информационных средств носят достаточно распространённый характер, они относятся к категории более опасных и латентных видов преступных посягательств, имеющих возможность перехода в более тяжкие преступления. Данное состояние проблемы объясняется тем что хищения, совершаемые с использованием информационных технологий, имеют недостаточное изучение в лице отечественных исследователей.

Вышепредоставленные сведения предоставляют возможность предположить типичный портрет субъекта преступного посягательства, осуществляемого с использованием информационных средств. Таким образом, перед нами представляется молодой мужчина в возрасте 25-35 лет, имеющий высшее образование, обладающий активностью в социальных, а также трудовых

отношениях, при этом состоящий в браке, по месту жительства и работы имеет положительную характеристику, к тому же является ранее судимым (около 85% опрошенных).

1.4. ИНЫЕ ЭЛЕМЕНТЫ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Обстановка совершения преступлений также относится к категории криминалистической характеристики хищений, совершаемых с использованием информационных средств. Данный элемент содержит социально-психологические, материальные и производственные факторы окружения, связанных с совершением преступного посягательства.

Окружающая среда может существенно влиять на создание иных элементов криминалистической характеристики хищений, совершаемых с использованием информационных технологий, с помощью определения особенности поведения лиц, совершивших преступное деяние и их жертв.

Важнейшим компонентом в подготовке к хищениям, осуществляемых с использованием информационных средств, являются объективные предпосылки. В эти предпосылки входит: род занятия или вид деятельности (информационная, финансовая, коммерческая, хозяйственная, производственная, управленческая, посредническая, топливно-энергетическая, услуги и др.); формы собственности физических лиц либо компаний, правовой режим определенных типов имущества вместе с информацией и включающих её ресурсы; вид используемых компьютерных устройств, телекоммуникаций и связи, включая тактико-технические особенности и конструктивное несовершенство; учет и системы отчетности; назначение и структура организации производственных процессов, характер востребованных ресурсов и производимой продукции, в том числе интеллектуальную; кадровое и материально-техническое обеспечение; порядок реализации и выпуска продукции; наличие необходимых помещений и оборудования; погодные условия; наличие и техническое состояние средств, связанных с учётом, защитой и охраной информации и т.д.

Субъективными условиями являются следующие факторы социально-психологического и организационно-управленческого характера:

1) Несоблюдение установленных технических режимов обработки информации, регламентных работ, технического обслуживания, учёта, хранения, расходования и распределения ценностей;
2) Несовершенство самих правил;
3) Недостатки или отсутствие средств, осуществляющих защиту данных; несоблюдение принципов работы с компьютерными данными, находящихся под охраной закона; неосновательное использование совокупности программных и технических компонентов (СВТ) в поставленных технологических операциях и процессах; некачественная организация производственных процессов, одновременное наличие ручных и автоматизированных этапов обработки документации; некорректные межличностные взаимоотношения руководителей и работников.

Значительное влияние на обстановку осуществления хищений, совершаемых с использованием информационных средств, а также возможного её формирования, в частности оказывают субъективные факторы.

Считается правильным, что при расследовании хищений, совершаемых с использованием информационных средств, является необходимым проведение анализа, исследование мотивов, а также определение целей данного вида преступлений. С учётом проведённого анализа представляется несколько групп мотивов:

1. Попытки показа личных интеллектуальных способностей;
2. Цели, имеющие исследовательский характер;
3. Реализация мести к администрации или другим работникам, в связи с бестактными межличностными отношениями;
4. Расшатывание обстановки государства и её субъектов, преследуя политические цели;
5. Нарушение целостности валютных систем;
6. Нелегальное завладение недвижимостью, денежными средствами, ценными бумагами, незаконное получение кредитов, товаров,

материальных ценностей, привилегий, услуг, квот, льгот, и, стратегического сырья, а также энергетических или топливно-сырьевых ресурсов;

7. Неправомерная деятельность, направленная на дисфункционирование компании, учреждения или системы, объясняющаяся политическими планами, устранением конкурентов, а также вымогательства;
8. Цели сокрытия других преступлений и правонарушений.

Местами осуществления хищений, совершаемых с использованием информационных технологий могут выступать предприятия, организации, учреждения и системы возможного использования компьютерных средств и иных технологических процессов. По итогу, возможно наличие нескольких мест совершения преступных деяний, как и в местах достаточно удалённых между собой, так и имеющих расположение других государств и континентов.

Стремительное развитие информационных технологий, их широкий круг действия, а также использование СВТ, представляют возможность осуществления преступных посягательств из нескольких мест в независимости от их удалённости. [8]

Удачным примером может служить уголовное дело, осуществление расследования которого происходило совместно правоохранительными органами России и США. Уголовной ответственности подлежали 13 граждан России и Нидерландов, будучи в преступном сговоре похитившие денежные средства в крупном размере. Данные средства были принадлежностью «City Bank of America», находившегося в Нью-Йорке. Неправомерными действиями преступной группировки протяжённостью несколько месяцев 2012 года были преодолены несколько рубежей защиты от неправомерного доступа, воспользовавшись оборудованием, находившимся в Санкт-Петербурге. После, находясь в системе управления денежными средствами банка, путём ввода недостоверной информации, были осуществлены десятки переводов денежных средств. Переводы совершались со счетов клиентов банка на счета лиц преступной группы, проживающих в разных странах: Швейцарии, Нидерландах,

Германии и других. Итоговая сумма хищения составила 10 700 952 государственной валюты США.

Следующим элементом криминалистической характеристики преступлений представляются обстоятельства, подлежащие выяснению в рамках уголовного дела, связанного с расследованием хищений, совершаемых с использованием современных информационных средств [Мазуров].

Содержание научной литературы говорит нам о важности выяснения обстоятельств, установление которых даёт гарантию целенаправленности профессиональной судебной, прокурорской и следственной деятельности.

Следующим элементом криминалистической характеристики является «предмет доказывания, что представляет из себя обстоятельства, подлежащие доказыванию по уголовному делу» (ст. 73 УПК). Установление обстоятельств в дальнейшем и будет определять направление, ход и цели дальнейшей следственной деятельности в расследовании хищений, совершаемых с использованием информационных технологий, о чём в частности говорится в научной литературе.

Определение перечня обстоятельств доказывания происходит в соответствии с нормами уголовно-процессуального законодательства и уголовным законом РФ.

Немаловажным будет установление круга обстоятельств, подлежащих доказыванию в конкретном уголовном деле, что потребуется в целях исключения возможных пробелов в процессе расследования и определении чётких границ предела исследования.

Доказыванию подлежит, совершено ли хищение вменяемым физическим лицом, достигшим шестнадцатилетнего возраста; содержится ли в действиях лица состав преступления: объект, субъект преступления, объективная и субъективная стороны.

Мотивом и целью преступлений могут выступать различные объекты. Мотив может представлять собой получение прибыли, месть самореализацию и проч. Цель преступления может заключаться в получении прибыли.

Обстоятельства, которые подлежат доказыванию во время производства по уголовному делу, перечисляются в УПК России, ст. 73, но приводятся они только в общем виде. Необходимо четко разграничивать круг обстоятельств, которые подлежат установлению для каждого уголовного дела, — предметы доказывания, а также круг доказательств, которые необходимы для определения данных обстоятельств, — объемы или пределы доказывания. В то время как предмет доказывания закон (в общих чертах) предусматривает по каждому делу, круг доказательств, требуемых для установления его, определяются следователем и судом согласно внутреннему своему убеждению [Мазуров].

Детализация обстоятельств напрямую зависит от типа совершаемого преступления. В нашем случае внимание будет сосредоточено на мошенничестве в сфере компьютерной информации.

Время осуществления преступления, совершаемого с использованием информационных технологий, устанавливается с учётом способа, объективной даты и времени преступления. Порой точность даты и времени не достигается, так как по истечении определённого времени потерпевшим и свидетелями могут быть забыты детали события совершения преступления.

Кроме того, следует определить место совершения хищения: в местах, указанных свидетелями, потерпевшими, иными лицами, или в другом (разных местах). Данное действие объясняется дальнейшей территориальной подследсвенности, то есть расследования хищения определённым органом предварительного следствия или дознания. Но порой определение подследсвенности является сложной задачей (преступник находится на расстоянии тысяч километров от своей жертвы, другой стране или континенте). Определение места производства предварительного следствия происходит на основании статьи 152 УПК РФ, что позволит обеспечить соответствие процессуальным срокам в условиях появившихся территориальных вопросах.

Выяснение места и времени осуществления данной категории преступлений может помочь установить: продолжительность преступных

деяний, способствовавшие обстоятельства; соучастников хищений; вероятных свидетелей хищения.

Обстоятельства, относящиеся к механизму хищений, указывают, какие следы оставлены предполагаемым преступником, степень причинённого вреда, состояние психики потерпевшего в момент совершения преступления [Мазуров].

При этом, установление устройств (персональные компьютер, смартфоны и др.), используемых в целях совершения хищения, как правило представляет крайне полезную информацию для расследования. Не менее важным на месте хищения является: найденная аппаратура и её принадлежность; количество соучастников; материальные и виртуальные следы, их особенность и характеристика.

Исследуя обстоятельства, связанные с личностью преступника, не стоит обделять роль и самого потерпевшего. Требуется выяснить степень знакомства потерпевшего и подозреваемого либо потерпевшего с кругом общения и соучастников подозреваемого. Знаком ли потерпевший с подозреваемым либо нет, знаком ли он с кем-либо из окружения или соучастников подозреваемого.

Сведения же о личности обвиняемого помогут установить количество и роль его соучастников. С учётом анализа уголовных дел, предстоит установить следующие обстоятельств о личности преступника: ФИО; дата и место рождения; где проживает; семейное положение; образование и уровень знаний; опыт работы с современными технологиями; наличие заболеваний (в том числе вменяемость/невменяемость); наград, а также наличие судимости.

Вместе с тем, доказыванию подлежат, предусмотренные уголовным законом (ст.61, 63 УК РФ), смягчающие либо отягчающие наказание обстоятельства.

В процессе также следует выяснить цели и мотивы осуществлённого хищения; наличие со стороны потерпевшего провокационных действий и в связи с чем; что способствовало совершению преступления; каков моральный и материальный вред преступления, его размер и значение.

Лицо, совершившее хищение с использованием информационных технологий, при наличии невменяемости (медицинского или юридического критерия) и вовсе не подлежит уголовной ответственности, но в последствие к нему могут быть применены принудительные меры медицинского характера, посредством назначения судебно-психиатрической экспертизы.

Таким образом, обстоятельства, подлежащие доказыванию, и их определение вносят значительный вклад в процесс раскрытия хищений, совершаемых с использованием информационных технологий. Данные обстоятельства взаимосвязаны, соответственно определение одного из них позволяет более полно исследовать другие, связанные с ним обстоятельства [Мазуров].

ГЛАВА 2. ВОЗБУЖДЕНИЕ УГОЛОВНОГО ДЕЛА, ПЕРВОНАЧАЛЬНЫЕ И ПОСЛЕДУЮЩИЕ ЭТАПЫ РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

2.1. ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА ПО ХИЩЕНИЯМ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

По итогам анализа источников юридической литературы, материалов уголовных дел, а также иных отечественных и зарубежных источников становится очевидным, что расследование хищений, совершаемых с использованием информационных технологий, и его успех, зависят от оперативности начала расследования, являющегося предварительным. Особо значимым моментом в этом процессе представляется возбуждение уголовного дела, которое является начальной стадией уголовного процесса. Данная стадия определяется уголовной и правовой природой незаконных деяний, спецификой способов, с содействием которых совершаются эти посягательства. Стоит обратить должное внимание на сложность исследования начальной доказательной базы, используя изучение учетные и технологические материалы. Документация, содержащая такие материалы, возможна в форматах повышенной сложности.

Эффективная работа следственных органов постоянно подвластна оперативности реагирования на сообщение о правонарушении либо поданное заявление. Также считается немаловажным своевременное возбуждение уголовного дела, имеющее правовую обоснованность. Практическое наблюдение показывает, что запоздалое начало процесса расследования является результатом достаточно быстрой утрате доказательств, имеющих особую степень важности. Безнаказанность правонарушителей является одним из последствий такой задержки. В случаях значительного увеличения сроков

предварительного расследования велик рост наиболее негативных последствий. По утверждению Р.С. Белкина, в зависимости от того насколько удачным будет расследование преступления, зависит систематически точный подход к расследованию и от оперативности реагирования, способности организовать имеющиеся в распоряжении следственных органов силы и средства, в целях борьбы с преступностью [Белкин, с. 267]. Также важным будет и верная организация взаимосвязанных действий между следственными подразделениями.

Оживлённое участие в данной деятельности принимают органы дознания, службы экспертов и безопасности, представленные частными охранными структурами. Данная необходимость вызвана обеспечить приобретение наиболее полной информации о преступном посягательстве. Полученные материалы, включающие информацию, способны представлять максимальное значение для криминалистов.

Ключевые этапы деятельности следователя и дознавателя на начальной стадии расследования:

1. Оценка поступившей к сотрудникам информации о преступлении;
2. Проверка поданных заявлений и полученных сообщений. В ситуациях отсутствия и недостатка необходимых данных в первичной информации, которые могут указать на признаки преступления данного вида;
3. Принятие и оформление в соответствии с процессуальными требованиями важных решений о необходимости возбуждения уголовного дела.

Данная деятельность подлежит регулированию уголовно-процессуальным законодательством и нормативными актами данного ведомства. Но присутствуют некие особенности.

Наиболее частым поводом и основанием для возбуждения уголовного дела о хищении, совершённого с использованием информационных технологий, являются:

1. Заявление от потерпевшего, от граждан, которые являются физическими лицами, от представителей юридических лиц.

2. Обнаружение органом дознания признаков совершения противозаконного деяния в ходе:

- проверки поступившего из оперативных источников сообщения о том, что правонарушение совершено или готовится его совершение;

- выполнения оперативно-технических мероприятий;

- изучения контрольных и ревизионных материалов, а также других проверок, связанных с документацией;

- задержании подозреваемых на том месте, где было совершено преступление, с поличным.

3. Обнаружение признаков правонарушения сотрудником следственных органов или прокуратуры во время расследования уголовных дел о других преступлениях.

В зависимости от того, что включает в себя первичная информации о свершившемся событии, сотрудник следственных органов может в порядке ст. 144 УПК РФ еще до возбуждения уголовного дела провести начальную проверку фактов, которые содержатся в сообщении о правонарушении. Подобная проверка не может считаться начальной стадией предварительного расследования. Но ее часто проводят при совершении хищений с использованием компьютерных технологий. Сроки проведения такой проверки регламентированы действующим уголовно-процессуальным законом (ч. 1 и 3 ст. 144 УПК РФ). Существует необходимость составления плана проверки, которая будет проведена до начала следствия. План должен включать определенные позиции:

1. Получение затребованной документации, которая свидетельствует о том, что свершившееся событие противоправно. Эти документы могут отражать несоответствие закону проведенной операции в сфере краж, которые были совершены с использованием компьютерных технологий информации;

2. Исследование, подтверждающее правильно формирование комплекта документов и их содержания. Данные документы являются подтверждением противоправности совершенного действия;
3. Исследование баз данных, файлов, машинного носителя информации, программ для компьютерно-технических устройств, как возможных орудий для совершения преступления;
4. Изучение технологии использования документов для хищений, которые совершаются с использованием компьютерных технологий. Использование информации в определенном процессе или отдельной операции;
5. Консультации со специалистами.
6. Иные проверочные действия, не являющиеся следственными.

Учитывая данные, которые были получены в результате проверки имеющихся материалов по делу, проведенной до начала следствия, может быть принято решение о возбуждении, отказе в возбуждении уголовного дела.

Данное решение должно быть принято на основании установленных сведений и документов:

1. Заявление потерпевшего (либо его представителя) в устном или письменном виде;
2. Объяснение обстоятельств преступления (время, место, предмет преступных действий).
3. Оригиналы или копии документов, подтверждающих право собственности, владения или пользования предметом хищения. Например, договор банковского счёта.
4. Рапорт уполномоченного лица об обнаружении признаков преступления с приложением материалов ОРМ и проверок.
5. Заключение специалиста о предварительном изучении вещественных доказательств.
6. Идентификационные данные субъекта противоправного действия.

7. Протокол осмотра места преступного посягательства, МНИ, сервера сети, в целях подтверждения фактов заявителя.

Для принятия какого-либо процессуального решения требуется достоверность полученных документов и сведений.

Успех расследования хищений, совершаемых с использованием информационных технологий, напрямую зависит от навыков и решительности следователя, а также его взаимодействия с грамотным специалистом из отдела «К». Данный спецорган относится к Управлению специальных технических мероприятий и может участвовать в проверке материалов, а также задержании правонарушителя.

От скорости принимаемых решений зависит, будут ли реализованы попытки сокрытия следов преступления. К тому же, недостаточная оперативность может привести к утечке конфиденциальной информации и потере идентификационных признаков предметов преступления.

Немаловажным являются и консультации высококвалифицированных специалистов области информационных технологий.

Получение консультаций происходит от следующих лиц:

1. Сотрудник научно-исследовательского центра;
2. Специалист компьютерно-технической экспертизы;
3. Работник службы безопасности, отвечающий за защиту технических каналов информации;
4. Сотрудник учебного заведения.

2.2. ОСОБЕННОСТИ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Обязательной частью первоначального этапа расследования хищений, совершаемых с использованием информационных технологий, выступают планирование, выдвижение, а также рассмотрение версий.

Расследование хищений, совершаемых с использованием информационных технологий, основано на планировании, последующим этапом которого является возбуждение уголовного дела на основе полученной информации.

Основой построения плана являются планирование, построение и выдвижение версий. Построение плана зависит от разработки версий и их проверки.

По утверждению Р.С. Белкина «Криминалистическая версия - это обоснованное предположение относительно отдельного факта или группы фактов, имеющих или могущих иметь значение для дела, указывающее на наличие и объясняющее происхождение этих фактов, их связь между собой и содержание и служащее целям установления объективной истины».

Следственная версия является одним из видов криминалистической версии.

Для формирования версий требуется учёт практики хищений и сравнение следов, обнаруженных в процессе следственных действий, в разрешение которых требуется профессиональная практика. В случае отсутствия сведений, используемых для толкования отдельных фактов преступления, мотив носит неоспоримый вклад.

Получив первичную информацию о хищениях, с помощью интернет - технологий следователь выдвигает общие версии. Первичная информация, такая как заявление потерпевшего, осмотр места преступления, проведение опроса свидетелей и пострадавшего, а также данные подсудимого (подозреваемого)

способствует дальнейшему выдвижению общих версий. Данная информация является вспомогательной в выдвижении версий и определении целей хищения.

Осмотр места происшествия является одной из составляющей в расследовании данной категории преступлений.

Планирование дальнейших действий, выбор приёмов и средств выполнения качественного сбора и оценки доказательств является одной из главных задач формирования плана расследования.

Основой для планирования расследования являются ранее совершённые хищения, сведения о которых были получены с помощью оперативно-розыскных мероприятий и процессуальных действий. Получение полных или поверхностных фактических данных напрямую влияет на формирование задач, версий, определение путей и способов расследования данной категории преступлений. Планирование на всём протяжении расследования является непрерывным процессом.

Полнота теоретических знаний, а также практический опыт выступают ядром вынесения верных решений. К обратной стороне успеха может привести ошибочное применение тактических приёмов, а также отсутствие чёткой последовательности действий. В этом случае на помощь приходит планирование, которое включает в себя точную организацию и совокупность определённых действий, что положительно влияет на результат выявления преступных лиц и событий преступных действий.

Дальнейшие направления следствия зависят от следственной ситуации, которая в свою очередь влияет на тактику и последовательность начальных следственных действий.

В такой же зависимости находятся и оперативно-розыскные и организационные мероприятия в процессе расследования хищений, совершаемых с использование информационных технологий.

Для исследования особенностей тактических решений на различных этапах деятельности следователя при расследовании хищений, совершаемых с

использованием информационных технологий, стоит сделать акцент на типовых ситуациях:

1) Проверки сообщения о хищении (от сообщения о неправомерном действии до возбуждения уголовного дела или его отказа);
2) Первоначального этапа расследования (начиная с возбуждения уголовного дела до предъявления обвинения);
3) Последующего этапа расследования (от предъявления обвинения до окончания предварительного расследования).

Определение типовых следственных ситуаций указанных этапов основывается на анализе более 50 приговоров по уголовным делам о хищениях, совершённых с использованием информационных технологий. Приговоры на территории Самарской, Московской, Оренбургской, Кемеровской, Оренбургской, Ленинградской, Белгородской, Томской, Ульяновской, Свердловской, Челябинской областей, Приморского края и Республики Хакасия в промежутке 2014-2021 годов уголовных дел.

Необходимо обратить внимание на то, что при совершении преступлений данной категории в виртуальном киберпространстве, существует вероятность «стирания границ» преступных посягательств. Что даёт возможность одновременно совершать преступления, включая в это разные регионы.

Данная специфическая особенность прослеживается в примере из следственной практики сотрудников Следственного управления и Уголовного розыска МВД России по Республике Тыва.

Так, при раскрытии серии дистанционных мошенничеств, совершённых с использованием информационных систем, сотрудниками МВД по Республике Тыва было установлено, что жителем Республики Башкортостан было совершено несколько эпизодов преступления. Он, предлагая интернет-пользователям несуществующие товары, а далее требуя оплату и получив денежные средства, переставал выходить на связь. При этом обман происходил как жителей Тувы, так и жителей других отдалённых регионов Российской Федерации [Полицейские…].

В этой связи процессы совершения и расследования мошенничества наименее подвержены влиянию географических и иных факторов, связанных со спецификой различных регионов, что позволяет отметить универсальность рассматриваемых типовых следственных ситуаций и алгоритма действий следователя на различных этапах при расследовании рассматриваемых преступлений.

При проверке сообщения о преступлении могут быть выделены ситуации в зависимости от источника и объема информации:

1) Сведения о хищении получены из заявления потерпевшего; данных, чтобы принять процессуальное решение, недостаточно.

Данный случай потребует проведения следующих проверочных действий. В них может входить: получение объяснений от заявителя и лиц в качестве возможных свидетелей; Истребование выписки банковского счета потерпевшего; Осмотр места происшествия, компьютерных и иных устройств с привлечением специалистов в области информационных технологий. Проведение осмотра по месту нахождения компьютерного оборудования потерпевшего, акцентируя внимание на обнаружение и фиксацию цифровых следов. Такими следами могут выступать, как и сами следы движения денежных средств, так и пользовательские данные потерпевшего и преступника, их обмен сообщениями, содержание журнала браузеров, отчёты и статистика антивирусной программы и лог-файлы (файлы с записями событий). В протоколе осмотра следует отразить картину расположения устройств, их описание, включая серийные номера, индивидуальные характеристика (например, IP и MAC адреса), внешнее состояние устройств и наличие на них материальных следов. Также потребуется внесение сведений подключения устройств к сети Интернет, вида связи сети. Немаловажным будет содержание информации о том, включено ли на момент осмотра компьютерное или иное устройство; описание запущенных процессов. Кроме того, в протоколе должен быть указан порядок проводимых действий, фиксация цифровых следов при помощи скриншота

экрана, скопированные файлы и способ их копирования. При изъятии компьютерных и сетевых устройств, в целях недопущения утраты значимых следов, может потребоваться координирование специалиста информационных технологий.

2) Сведения о хищении получены в результате ОРД; данных, чтобы принять процессуальное решение, достаточно.

Данный случай потребует рассмотрения достаточности результатов ОРД; наличия сведений о месте, времени и обстоятельствах преступления; наличие сведений о лицах, совершивших преступление; местоположение вещественных доказательств.

Чаще всего на практике мы можем наблюдать ситуацию недостаточности информации. В зависимости от достаточности сведений, будет принято итоговое процессуальное решение об отказе или возбуждении уголовного дела.

На первоначальном этапе расследования хищения в зависимости от содержания исходной информации могут быть следующие типовые ситуации:

1) Потерпевшие, свидетели и способ хищения установлены, обнаружены цифровые следы, но данные о субъекте преступления отсутствуют.

Отдельными следами в данной ситуации могут выступать, например, следы вывода денежных средств, следы соединений абонентов, следы незаконного доступа. Установление информации о лице противоправных действий с помощью обнаруженных цифровых следов является направлением расследования.

Видится следующая последовательность следственных действий:

1. Допросы потерпевших и последующее выяснение наличия у потерпевшего персонального компьютера и иных устройств с доступом к сети Интернет, а также может ли кто-то располагать доступом к устройству помимо потерпевшего. Есть ли у потерпевшего учётная запись в социальных сетях, только ли потерпевший располагает данными для доступа к этой учётной записи. Уточняется наличие банковских счетов, наименование банков, а также услуги «Онлайн-банк». Известны ли реквизиты банковского счёта

третьим лицам, были ли потерпевшим произведены платежи, где, куда и в каких целях и каким способом. Также следует выяснить способ взаимодействия с преступником (переписка или голосовая связь). После этого стоит установить были ли у мошенника характерные особенности речи; наличие в прошлом потерпевшего идентичных неправомерных действий; установлены ли на его устройствах программы защиты, а также иные программы после установки которых, была зафиксирована подозрительная активность.

2. Изучение выписок движения денежных средств;

3. Запрос у банков и кредитных организаций данных держателя счёта/карты, на которые были перечислены денежные средства;

4. Запрос сведений о владельце доменного имени мошеннического сайта;

5. Направление запроса оператору связи о лице владельца абонентского номера;

6. Запрос провайдеру интернет-соединения, в целях получения сведений об абоненте или абонентском устройстве (дата, время записи сессии, IP-адрес маршрутизатора, вид соединения и остальные параметры);

Отсутствие необходимого и оперативного содействия по вышеперечисленным запросам способно сталкивать следственных работников в расследовании данной категории хищений с определёнными трудностями.

7. Допросы свидетелей, обладающих криминалистически значимой информации ввиду своего профессионального статуса (сотрудники банков и кредитных организаций, представители регистратора доменных имён, провайдеры хостинга и иные);

8. Назначение и проведение необходимых экспертиз;

9. Поручение о проведении ОРМ, в целях установления лиц преступного посягательства.

10. Принятие мер для задержания преступных лиц.

2) Потерпевшие, свидетели и способ хищения установлены; цифровые следы не обнаружены, данные о субъекте преступления отсутствуют.

В этой ситуации, ввиду неосторожных или умышленных действий, допускается возможность уничтожения виртуальных следов преступления. К таким последствиям может привести: очистка истории интернет-браузера, удаление сообщений диалога; удаление сайта мошеннических действий либо аккаунтов социальных сетей; технические особенности работы устройства (автоматические процессы удаления данных; повреждение устройства); использование программного обеспечения, вспомогательной функцией которого является сокрытие активности вредоносных программ.

Таким образом, для дальнейшего выявления цифровых следов, с помощью которых будет возможно установить преступный элемент, потребуется применить специальные знания и технические средства.

Видится следующий алгоритм расследования:

1. Допрос потерпевших, с целью выяснения информации, оставшейся в их памяти, а также возможных действиях, которые могли привести к уничтожению цифровых следов. Запомнившейся информацией может быть, как визуальное оформление и доменное имя мошеннического сайта, так и данные из переписки с преступником.

Примером, может служить следующее уголовное дело. В Тюменской области, в ходе расследования мошенничества, где вспомогательным инструментом в совершении неправомерных действий выступал интернет-магазин, сайт которого на момент расследования оказался заблокирован. В последствие было решено провести допрос потерпевших. Полученная из памяти потерпевших информация о наименовании интернет-магазина, адресе, контактных данных на сайте способствовала установлению подозреваемых [Приговор Ленинского районного суда г. Тюмени…].

1. Направление запроса регистратору доменного имени. Ответ на запрос должен содержать сведения доменного имени и аннулирования домена мошеннического сайта.
2. Направление запроса оператору связи, в целях установления сведений о соединениях потерпевших (зная ориентировочные дату и время).

3. Допросы свидетелей или их представителей по полученным ответам на запросы следователя.
4. Выемка и осмотр устройств потерпевших. Применяются специальные технические средства при взаимодействии специалиста.

Данные следственные действия должны сопровождаться использованием специальных программных и технических средств, цель которых состоит в обнаружении и последующем изъятии утраченных цифровых следов. Например, программа «NetAnalysis» и программный комплекс «UFED». С помощью комплекса «UFED» извлекаются удалённые пароли и файлы. Первая программа отвечает за поиск, сбор и восстановление следов в интернет-браузере.

При этом не помешает обратиться и к блокираторам записи. Их польза применения выражается в возможности просмотра файлов устройства, без опасности внесения изменений (например, «SUMURI PALADIN»).

5. Назначение компьютерных и иных экспертиз. Проведение судебной компьютерной экспертизы поможет ответить на вопросы: наименования марки, модели; технических характеристик устройства; наличия информации в памяти устройства; промежутки времени подключения к сети Интернет; задействованные ресурсы; сведения о способах проведения платежей и другие. В определении перечня вопросов приемлемо согласование с экспертом или специалистом информационной области.

В случае обнаружения в ходе осмотра переписки потерпевшего и лица, совершившего хищение, может проводиться судебная автороведческая экспертиза текстов электронных сообщений. В некоторых случаях при расследовании хищений, совершаемых с использованием информационных технологий, возможно проведение психологической, комплексной психолого-психиатрической, психолингвистической экспертиз. Также при разрешении данной следственной ситуации необходимо проведение ранее обозначенных действий, направленных на установление личностных особенностей преступника.

3) Потерпевшие, свидетели и способ хищения установлены, обнаружены цифровые следы; имеются некоторые данные о субъекте преступления кроме его местонахождения.

На данном этапе расследования могут быть известны персональные данные преступного лица. Их получение зависит от конкретного источника. Допустим, похищенные средства были перечислены на банковский счёт или карту, принадлежащих лицу, совершившему хищение с использованием информационных технологий.

В данной ситуации акцентирование внимание должно происходить на проверке достоверности имеющихся персональных данных (иных сведений), а также дальнейшего установления местонахождения преступного элемента.

Дальнейшая деятельность может сопровождаться следующими следственными и иными действиями:

1. Допросы потерпевших и свидетелей установления достоверности сведений и месте нахождения лица, совершившего преступление.
2. При наличии предполагаемого номера абонента противоправных действий следует сделать запрос оператору связи, для дальнейшего получения сведений о лице, которому принадлежит данный номер телефона. Последующим действием будет направление поручения о проведении ОРМ.
3. Проверка и истребование сведений потенциального мошенника, используя базы информационного центра и главного информационно-аналитического центра МВД РФ. Дальнейший круг действий зависит от наличия или отсутствия судимости. Если лицо ранее судимо, потребуется его характеристика, дактилоскопическая карта и фотографии.
4. Направление поручения органам дознания о проведении мероприятий по розыску мошенника.
5. Задержание и допрос подозреваемых.
6. Осмотр мест расположения оборудования и устройств, с помощью которых и совершалось хищение, совершаемое с использованием

информационных технологий. В процессе этого следственного действия отдельное внимание стоит обращать на обнаружение: специальной технической литературы; реквизитов банковских и кредитных карт; адреса социальных сетей, электронных почт их паролей; договоры представления различных услуг (например, подключение домашнего или корпоративного интернета); распечатки проработанных диалогов и пр. Осмотр устройств, их аксессуаров и иной вспомогательной техники должен быть проведён тщательнейшим образом, ведь на данных предметах могут находиться следы биологического происхождения.

Также при проведении осмотра важным будет провести следующие действия: изучить внешний вид устройства (модель, повреждения и прочее), комплектующие устройства (жёсткий диск, сетевая карта, процессор), уточнить тип операционной системы, IMEI, MAC и IP-адреса устройства.

Чтобы определить сведения о мобильном телефоне, при возможности следует зайти в настройки данного девайса. В них может содержаться интересующая информация об устройстве, например, IMEI (или комбинация «*#06#)», IP и MAC-адреса, модель, операционная система, прошивка, а также серийный номер. В случае неработоспособности устройства уникальный идентификационный номер может находиться на задней крышке или под аккумулятором мобильного телефона.

Кроме того, при осмотре мобильных устройств следует изучить информацию о взаимодействии абонентов (СМС и ММС-сообщения, телефонная книга), возможно оставшиеся следы преступления, посредством просмотра WEB-браузера (вкладки, закладки, история просмотров, электронная почта, социальные сети).

При осмотре WEB-страниц все проводимые следственные действия, должны быть занесены в протокол. Прибегая к помощи специалиста устанавливаются информация о домене, проверяется верное отображение подлинного сайта, а также его содержание. При обнаружении значимой информации, она отражается в протоколе.

Дополнительным методом фиксирования в ходе осмотра выступает снимок экрана (от англ. screenshot) с помощью нажатия на клавиатуре комбинации «Win + PrtSc».

Кроме того, целесообразно сделать акцент на вложениях электронной почты. В них могут находиться изображения, видеозаписи, текст и иные документы, имеющие значение для успешного расследования. По итогу осмотра электронной почты в протоколе должно быть отображено содержание и данные текстовых сообщений (тема, дата, время, электронные адреса отправителя и получателя, начало и конец текста сообщения). Значимая информация заносится дословно.

Учитывая вышесказанное, первоначальный этап расследования уголовных дел данной категории преступлений основан на собирании и исследовании всевозможных и всеполных значимых доказательств, а также установлении лиц, причастных к совершению хищений, совершаемых с использованием информационных технологий.

2.3 ОСОБЕННОСТИ ПОСЛЕДУЮЩЕГО ЭТАПА РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В отличии от ранее рассмотренного первоначального этапа расследования хищения, последующий отличается количеством необходимых сведений, являющихся доказательством. К тому же, на этом этапе происходит проверка и закрепление ранее полученных доказательств.

Далее будут рассмотрены типовые ситуации в зависимости от степени признания вины обвиняемого и достаточности доказательств.

1) В первой ситуации обвиняемым даны показания по поводу обстоятельств и соучастников неправомерных действий, вину признаёт, доказательства подтверждают вину.

Данная ситуация представляется перед следователем в позитивном ключе. В основном деятельность следователя при этой типовой ситуации состоит в систематизации ранее полученных доказательств по делу, а также принятии дальнейших решений, ответственных за окончание предварительного расследования.

В данном случае видится проведение следующих следственных действий:

1. Допрос обвиняемого с целью уточнения информации по поводу обстоятельств и отдельных эпизодов преступной деятельности (подготовка, как совершалось преступление, способы сокрытия, а также данные су участников и их роли в преступных действиях).

Допрос в данной ситуации подлежит особой подготовке. В данном случае отдельно изучаются биография и особенности личности допрашиваемого лица. Социальные сети могут выступать источником получения дополнительных личностных данных преступника. Достаточно важным будет изучить друзей и группы пользователя. Тем самым будет установлен круг общения, опубликованные записи, комментарии, которые могут стать свидетельством отношения лица к определённым социальным явлениям и событиям.

Отдельного внимания перед допросом заслуживает изучение специальной литературы, в целях обладания знаниями в сфере информационных технологий, а также верная постановка вопросов с помощью консультаций специалистов IT-сферы.

При проведении допроса обвиняемого, посредством общих вопросов, должно быть установлено: обладает ли он навыками в сфере информационных технологий; есть ли у него опыт работы с определённым программных обеспечением; где работает и в какой должности; в чём состоит мотив и цель совершения преступления; в какое время возник умысел совершения неправомерных действий. Следующей задачей допроса будет детализация имеющихся сведений о способе хищения и оставшихся в процессе совершения следов преступления.

Кроме того, при допросе обвиняемого следует задать вопросы, ответ на которые будет содержать сведения о дате создания мошеннического сайта, продолжительности его функционирования. К тому же, стоит выяснить с помощью каких технических средств производилось создание сайта, какие при этом были использованы программы; на какое доменное имя зарегистрирован мошеннический сайт; какие товары предлагались к продаже; какими способами осуществлялась реклама и продвижение предложенных товаров; каким образом происходило взаимодействие с покупателями (номер телефона и адрес электронной почты); способ и реквизиты оплаты; какие были предприняты попытки сокрытия данного преступления.

Если при совершении преступления были использованы социальные сети, то предстоит выяснить какими способами происходил подбор паролей и логинов жертв хищения.

Допрос лица, совершившего хищения с применением вредоносных программ, осуществляется посредством выяснения следующей информации: создана ли вредоносная программа самостоятельна или же была позаимствована, какой язык программирования (например, JAVA) использовался; что составляло

функциональность программы; код данной программы; каким способом распространялась вредоносная программа.

2. Очная ставка, в случае возникновения противоречий в показаниях;
3. Обыск или выемка при выяснении ранее неизвестных сведений, полученных в ходе допроса;

При проведении обыска или выемки выяснению подлежит: вид вычислительной техники; обладает ли техника программой защиты от несанкционированного доступа. Между тем, потребуется установить: тип и место источников электропитания, расположение подачи электропитания. Также при производстве обыска и выемки является обязательным участие понятых и специалистов. В ходе производимого следственного действия, в данном случае обыска, следователю надлежит внимательно следить за поведением обвиняемого, заранее узнав и изучив особенности личности обвиняемого, что вероятно повысит эффективность наблюдения.

В некоторых источниках научной литературы содержатся рекомендации, суть которых направлена на привлечения понятых, обладающих специальными знаниями в сфере информационных технологий. Это объясняется тем, что понятое лицо, задача которого удостоверить факт и ход проводимых следственных действий, должен осознавать цель и содержание событий. Однако, следовать данным рекомендациям представляется достаточно сложной задачей, так как расширенный поиск понятых при необходимости проведения срочных следственных действий, порой не видится возможным.

При расследовании хищений, совершаемых с использованием сети Интернет, проводя обыск в помещении обвиняемого, следует ограничить его свободное передвижении, а также использование им электронных средств.

По окончании обыска или выемки для отображения результатов проведённых следственных действий составляется протокол и изымаются предметы, имеющие значение для дела. Необходимо зафиксировать место и обстоятельства обнаруженного оборудования, документов и иных предметов; факт добровольной выдачи или принудительного изъятия предметов, при этом

отражая их перечень и описание (например, номерной знак предмета). При обнаружении файлов потребуется сделать их копии, указав информацию о накопителе и наименование и объём файлов.

4. Проверка показаний на месте для уточнения информации о механизме совершения преступления.

1) Во второй ситуации обвиняемый признаёт вину, однако объёма доказательств его вины недостаточно.

В этой типовой следственной ситуации деятельность следователя будет акцентироваться на выявлении новых доказательств, используя следующие действия:

1. Повторные допросы свидетелей, обвиняемого и потерпевших для выявления дополнительных источников доказательств.
2. Проведение исследований и экспертиз на основе специальных знаний.

Так, использование специальных знаний помогло подтвердить вину лица, совершившего хищения с помощью создания интернет-магазина. В Тюменской области, с целью совершения мошенничества, Немошкаловым М.А. был создан интернет-магазин ООО «<данные изъяты>», основным видом деятельности которого являлась торговля бытовыми товарами. Приискав на руководительскую должность ранее знакомого ФИО49, не посвятив последнего в свои преступные планы, руководил преступной деятельностью и принимал организационные решения для реализации преступного умысла. В ходе проведённого допроса Немошкаловым М.А. были даны показания, в которых он и признал свою вину. В целях подтверждения его вины была назначена почерковедческая экспертиза, согласно которой рукописные записи и подписи в документах, причастных к совершению преступления, были сделаны именно Немошкаловым, а не назначенным ранее директором ФИО49. [Приговор Ленинского районного суда г. Тюмени No 1-20/2019 1-718/2018…]

Поручения о проведении ОРМ, в целях получения новых сведений предмета доказывания.

2) В третьей ситуации мы видим, что обвиняемый полностью или частично отрицает его виновность, но достаточность доказательств говорит об обратном.

В приведённой ситуации следует ожидать от обвиняемого противодействия расследованию в виде дачи ложных показаний или отказа давать показания. Основное направление этой ситуации состоит в систематизации ранее полученных доказательств и их источников, поиске новых источников получения доказательств и проверке ранее данных показаний.

В данной ситуации потребуется выполнение следующих следственных действий:

1. Повторный допрос с использованием изменённой тактики.

При расследовании преступных деяний, совершаемых с использованием информационных технологий, наиболее эффективными тактическими приёмами будут являться: замена главного вопроса второстепенными; разъяснение допрашиваемому лицу возможности установления какого-либо факта посредством проведения различных экспертиз; создание впечатления обладания следователем более полной информацией о событиях преступления [Поляков В.В., Ширяев А.В., С. 123–126].

Тактические приёмы при допросе в приведённой ситуации необходимо применять, учитывая индивидуальные особенности допрашиваемого лица. В случае допроса мошенников, совершающих хищения с использованием информационных технологий, обладающих социальной пассивностью в реальной жизни и не имеющих криминальных связей, действующим средством воздействия будет являться разъяснение лицу последствий и тяжести совершённого преступного деяния. Также отдельного внимания заслуживает профессиональная подготовка и уровень знаний допрашиваемого в информационной сфере.

1. Определение роли обвиняемого лица в стадии подготовки, совершения и сокрытия преступных действий; установление других причастных к преступлению лиц.

С учётом вышеизложенной информации можем подвести итог:

1) Проведя анализ судебной практики по хищениям, совершаемых с использованием информационных технологий, были выделены типовые ситуации этапов расследования (при проверке сообщения о преступлении, типовые ситуации первоначального и последующего этапов расследования).
2) Установлено, что на этапе проверки сообщения о совершении хищения, совершаемого с использованием информационных технологий, в зависимости от источника и объема информации, видятся следующие ситуации: а) Сведения о хищении получены из заявления потерпевшего; данных, чтобы принять процессуальное решение, недостаточно. Данный случай потребует проведения следующих проверочных действий. В них может входить: получение объяснений от заявителя и лиц в качестве возможных свидетелей; Истребование выписки банковского счета потерпевшего; Осмотр места происшествия, компьютерных и иных устройств с привлечением специалистов в области информационных технологий. Проведение осмотра по месту нахождения компьютерного оборудования потерпевшего, акцентируя внимание на обнаружение и фиксацию цифровых следов; б) Сведения о хищении получены в результате ОРД; данных, чтобы принять процессуальное решение, достаточно. Данный случай потребует рассмотрения достаточности результатов ОРД; наличия сведений о месте, времени и обстоятельствах преступления; наличие сведений о лицах, совершивших преступление; местоположение вещественных доказательств.
3) Чаще всего на практике мы можем наблюдать ситуацию недостаточности информации. В зависимости от достаточности сведений, будет принято итоговое процессуальное решение об отказе или возбуждении уголовного дела.

На первоначальном этапе расследования хищения в зависимости от содержания исходной информации могут быть следующие типовые ситуации:

a) Потерпевшие, свидетели и способ хищения установлены, обнаружены цифровые следы, но данные о субъекте преступления отсутствуют.

Отдельными следами в данной ситуации могут выступать, например, следы вывода денежных средств, следы соединений абонентов, следы незаконного доступа. Установление информации о лице противоправных действий с помощью обнаруженных цифровых следов является направлением расследования.

b) Потерпевшие, свидетели и способ хищения установлены; цифровые следы не обнаружены, данные о субъекте преступления отсутствуют.

В этой ситуации, ввиду неосторожных или умышленных действий, допускается возможность уничтожения виртуальных следов преступления. Таким образом, для дальнейшего выявления цифровых следов, с помощью которых будет возможно установить преступный элемент, потребуется применить специальные знания и технические средства.

c) Потерпевшие, свидетели и способ хищения установлены, обнаружены цифровые следы; имеются некоторые данные о субъекте преступления кроме его местонахождения.

На данном этапе расследования могут быть известны персональные данные преступного лица. Их получение зависит от конкретного источника. В данной ситуации акцентирование внимание должно происходить на проверке достоверности имеющихся персональных данных (иных сведений), а также дальнейшего установления местонахождения преступного элемента.

Учитывая вышесказанное, первоначальный этап расследования уголовных дел данной категории преступлений основан на собирании и исследовании всевозможных и всеполных значимых доказательств, а также установлении лиц, причастных к совершению хищений, совершаемых с использованием информационных технологий.

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования, следует отметить, что, учитывая цели и задачи, поставленные нами в ходе данной научной работы, нам удалось выявить ряд теоретических и практических проблем, появляющихся в деятельности субъектов расследования хищений, совершаемых с использованием информационных технологий.

Также следует сделать следующие выводы:

1) Нами раскрыто содержание особенностей элементов криминалистической характеристики хищений, совершаемых с использованием информационных технологий, а также закономерность данных элементов. Так, в структуру особенностей можно включить следующие элементы: данные о личностях преступника и потерпевшего, типичные следы преступлений, условия совершения хищений, методы и мотивы преступлений.
2) Был проведён анализ взаимосвязи элементов криминалистической характеристики; выявлена взаимообусловленность элементов криминалистической характеристики, то есть их воздействие друг на друга.
3) Изучив специфику и проблематику возбуждения уголовных дел о хищениях, совершаемых с использованием информационных технологий, был предложен алгоритм действий проверки изначально полученной информации о совершении преступления. Таким образом, алгоритм действий на начальной стадии возбуждения уголовного дела должен выглядеть следующим образом:

1. Беседа с пострадавшим лицом;
2. Осуществление исследований экспертов;
3. Обработка документов с информацией о хищении;
4. Осмотр места происшествия и анализ предметов, относящихся к хищению;

5. Опрос круга общения пострадавшего и преступника.
6. Получение объяснений от преступника.

Успех расследования хищений, совершаемых с использованием информационных технологий, напрямую зависит от навыков и решительности следователя, а также его взаимодействия с грамотными специалистами отдела «К и специалистами в области информационных технологий.

От скорости принимаемых решений зависит, будут ли реализованы попытки сокрытия следов преступления. К тому же, недостаточная оперативность может привести к утечке конфиденциальной информации и потере идентификационных признаков предметов преступления.

4) Мы выделили типовые следственные ситуации, возникающие этапах расследования хищений, задачи данных типовых ситуаций, а также разработали алгоритм следственных действий для каждой ситуации.

В данных типовых ситуациях содержится алгоритм проведения отдельных следственных действий в характерных следственных ситуациях, ряд соответствующих рекомендаций и прочее, учитывая при этом рассмотрение типичных и виртуальных следов.

5) Изучили процесс выдвижения версий и составление плана расследования хищений, совершаемых с использованием информационных технологий.

Следует отметить, что планирование включает в себя точную организацию и совокупность определённых действий, что положительно влияет на результат выявления преступных лиц и событий преступных действий.

Любой следователь в осуществлении практической деятельности в определенной мере обязательно составляет план расследования, продумывает ход следствия и выбирает разные следственные действия, однако при таком неполном осуществлении планирования оно проявляется только как один из организационных методов в работе следователя, отнюдь не обеспечивающий использование всех возможностей планирования.

6) Сформировали рекомендаций проведения следственных действий на начальном и последующих этапах расследования хищений, совершаемых

с использованием информационных технологий. Каждое следственное действие обладает своей функцией, ролью, значением и задачами.

7) Определили возможные причины и условия совершения хищений рассматриваемой категории преступлений.

Стабильная криминогенная обстановка киберпреступлений и их повышенная латентность, порождающая сложности в обнаружении доказательственной базы, в том числе виртуальных следов преступления, мотивируют совершать подобные преступления, осознавая низкую вероятность их выявления.

Недостаточная подготовка сотрудников правоохранительных органов говорит о потребности разработки новых методов в этом направлении.

Между тем, данная категория преступлений является достаточно специфичной и явно отличается от иных преступлений, что, предположительно, вызвано цифровизацией и информатизацией общества.

Решение перечисленных проблем видится в регулярном повышении уровня профессионализма субъектов расследования киберпреступлений, включая хищения, а также постоянном учёте новых способов, характерных следов (виртуальные следы) и действий по маскировке их совершения.

На данной основе необходимо строить частные методики расследования, давать рекомендации по планированию расследования киберпреступлений, а также определять систему необходимых следственных действий или иных мероприятий.

Таким образом, специфичность хищений, совершаемых с использованием информационных технологий, а также динамично меняющиеся условия следственных ситуаций, требуют от следователя высокого профессионального уровня, предельной сосредоточенности при построении алгоритма следственных действий, а также привлечения грамотных специалистов из сферы информационных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 года: с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // КонсультантПлюс: справочно-правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_28399 (дата обращения: 15.04.2022).

2. О государственной судебно-экспертной деятельности в Российской Федерации: Федеральный закон РФ от 31 мая 2001 года № 73-ФЗ: от 01.07.2021 N 273-ФЗ // http://www.consultant.ru/document/cons_doc_LAW_31871 (дата обращения: 17.04.2022).

3. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон РФ от 18 декабря 2001 года №174-ФЗ: ред. от 11.06.2022 N 181-ФЗ // КонсультантПлюс: справочно-правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_34481 (дата обращения: 17.04.2022).

4. Уголовный кодекс Российской Федерации: Федеральный закон РФ от 13 июня 1996 года №63-ФЗ: ред. от 25.03.2022 N 63-ФЗ // КонсультантПлюс: справочно-правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 21.05.2022).

5. Вопросы организации и производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: Приказ МВД России от 29 июня 2005 года №511: ред. от 27.06.2019 // КонсультантПлюс: справочно-правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_55315 (дата обращения: 18.04.2022).

6. О полиции: Федеральный закон № 3-ФЗ: от 7 фев. 2011 г.: от 21.12.2021 N 424-ФЗ// // КонсультантПлюс: справочно-правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 24.05.2022).

2. Учебная и научная литература

7. Алексеева Т.А., Ахмедшин Р.Л., Юань В.Л. Исследование личности обвиняемого посредством анализа материала социальных сетей //Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий : сб. науч. ст. /отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул : Изд-во Алт. ун-та, 2018. Вып. XV. С. 7–14.

8. Ахмедшин Р.Л. Тактика коммуникативных следственных действий. Томск: Издательский Дом Томского государственного университета, 2014. 294 с.

9. Бондарева Г.В. Электронные доказательства в раскрытии и расследовании преступлений // Юристъ-Правоведъ. 2020. № 3 (94). С. 81-85.

10. Быков В.М. Актуальные проблемы уголовного судопроизводства / В.М. Быков. Казань: Познание, 2015. 300 с.

11. Батюк В.И., Галузо В.Н. Проблемы правового регулирования заключения эксперта и заключения специалиста в Российской Федерации // Образование и право. 2018. №7. С. 80-85.

12. Бедняков И.Л. Об определении процессуальных нарушений, влекущих недопустимость использования в доказывании результатов обыска// Вестник Самарского юридического института. 2010. №1. С. 167-169.

13. Белкин Р.С., Зуйков Г.Г. Криминалистика / под ред.. - М.: Юрид. лит., 1968. - 493 с.

14. Боярова М.А. Особенности правового статуса эксперта в рамках уголовного процесса // Известия Института систем управления СГЭУ. 2019. №1(19). С. 34-36.

15. Быков ВМ. Фактические основания производства следственных действий по Уголовно-процессуальному кодексу Российской Федерации // Журнал российского права. 2014. № 6. С. 59-69.

16. Воробей С.Н. Проблемы правовой регламентации процессуального порядка изъятия электронных носителей и копирования содержащейся на них информации // Полицейская и следственная деятельность. 2021. № 2. С. 26-31.

17. Верхотурова С.В., Соболевская С.И. О роли специалиста в уголовном процессе // Юридическая наука и правоохранительная практика. 2021. №1(55). С. 71-81.

18. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4 (44). С. 45.

19. Журба О.Л., Торопов С.А. К вопросу повышения эффективности поисковых действий при производстве обыска // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2018. Т. 3 (69). № 3. С. 132-138.

20. Зеленский, В.Д. Организация расследования преступлений. Криминалистические аспекты / В.Д. Зеленский. - Ростов н/Д, 1989. С 258.

21. Казанцев С.Я., Самитов Э.О. Тактические особенности проведения обыска при расследовании хищений, совершенных с использованием современных интернет-технологий // Вестник Московского университета МВД России. 2016. № 8. С. 145-147.

22. Капустина Л.К. Оценка допустимости и достоверности доказательств в уголовном судопроизводстве // Вестник Санкт-Петербургского университета МВД России. 2020. №1(85). С. 113-118.

23. Клевцов В.В. Проблемные аспекты изъятия электронных носителей информации при расследовании распространения «дизайнерских» наркотиков с использованием сети Интернет // Российский следователь. 2015. № 6. С. 59-62.

24. Когосов А.П. Некоторые актуальные вопросы экспертной деятельности // Вестник Южно-Уральского государственного университета. Серия: Право. 2019. Т. 19. №2. С. 103-107.

25. Колесниченко, А.Н. Научные и правовые основы расследования отдельных видов преступлений: дис. . д-ра юрид. наук / А.Н. Колесниченко. - Харьков, 1967. С. 156.

26. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. ...канд. юрид. наук. М., 2018. 197 с.

27. Коротков А.П., Тимофеев А.В. Прокурорско-следственная практика применения УПК РФ. М., 2005. 607 с.

28. Купряшина Е.А. Источники доказательства и критерии их оценки в уголовном процессе РФ: специальность 12.00.09 Уголовный процесс, криминалистика и судебная экспертиза; оперативно-розыскная деятельность: автореф. дис. канд. юрид. наук. Воронеж, 2007. 23 с.

29. Левченко О.В. Доказательства и процесс уголовно-процессуального доказывания: учебное пособие / Левченко О.В. Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014. 123 с.

30. Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. ... канд. юрид. наук: 12.00.12 / Мазуров Игорь Евгеньевич. - Казань, 2017. - 188 с.

31. Основы уголовного судопроизводства: учебник / М. В. Бубчикова, Т. С. Жиленкова, В. А. Давыдов [и др.]; под ред. В. А. Давыдова, В. В. Ершова. Москва: РГУП, 2017. 444 с.

32. Пешкова К.Т. Доказательство и доказывание в уголовном процессе / К.Т. Пешкова. Москва: Лаборатория книги, 2010. 109 с.

33. Россинская Е.Р. Теория судебной экспертизы (судебная экспертология): учебник / Е.Р. Россинская, Е.И. Галяшина, А.М. Зинин; под ред.

Е.Р. Россинской. 2-е изд., перераб и доп. Москва: Норма: ИНФРА-М, 2020. 368 с.

34. Россинский С.Б. Следственная выемка (изъятие) как «технический» способ собирания доказательств в уголовном процессе // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2021. № 2 (87). С. 101-106.

35. Селина Е.В. Экспертиза как средство доказывания в суде первой инстанции по уголовным делам: специальность 12.00.09 уголовный процесс, криминалистика, теория оперативно-розыскной деятельности: автореф. дис. канд. юрид. наук. Краснодар, 1997. 22 с.

36. Соболевская С.И. Проблемные вопросы комплексной экспертизы в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2019. №1(47). С. 142-150.

37. Строгович М.С. Курс советского уголовного процесса. Том 1. Основные положения науки советского уголовного процесса. М.: Издательство «Наука», 1968. 468 с.

38. Уголовно-процессуальное право: учебник для бакалавриата, специалитета, магистратуры и аспирантуры (адъюнктуры) / под общ. ред. В.М. Лебедева. 3-е изд., перераб. и доп. Москва: Норма: ИНФРА-М, 2021. 936 с.

39. Уголовный процесс. Учебник. / под ред. Булатов Б.Б., Баранов А.М. М.: Юрайт, 2020. 567 с.

40. Хмыз А.И. Профилактика низкого качества заключения эксперта // Вестник экономической безопасности. 2020. №2. С. 233-236.

41. Шейфер С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение. М.: Юрлитинформ, 2018. 229 с.

42. Шутемова Т.В. Проблемы оценки прокурором заключения эксперта по уголовным делам // ГлаголЪ правосудия. 2020. №3(25). С. 25-27.

3. Материалы правоприменительной практики

43. О практике применения судами законодательства о процессуальных издержках по уголовным делам: Постановление Пленума Верховного Суда РФ от 19 декабря 2013 года № 42 // Российская газета. 27.12.2013.

44. О судебной экспертизе по уголовным делам: Постановление Пленума Верховного Суда РФ от 21 декабря 2010 года №28 // Официальный сайт Верховного Суда РФ. URL: https://vsrf.ru/lk/practice/acts (дата обращения: 04.04.2021).

45. Приговор № 1-410/2017 от 19 октября 2017 года Дзержинского районного суда г. Оренбурга // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/dLvBrnx4b4gJ/ (дата обращения: 07.05.2022).

46. Приговор № 1-207\16 от 19 апреля 2016 года Дорогомиловский районный суд г. Москвы // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/jLvtyrfgnx4b6f6/ (дата обращения: 05.05.2022).

47. Приговор № 1-227/2019 от 5 июля 2019 г. по делу № 1-227/2019 Автозаводский районный суд г. Тольятти Самарской области // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/996lESV2gK6u/ (дата обращения: 13.05.2022).

48. Приговор № 1-277/2020 от 30 июля 2020 г. Советский районный суд г. Владивостока // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/4AyuDmz7J9oX/ (дата обращения: 10.05.2022).

49. Приговор № 1-49/2014 от 15 мая 2014 г. Хамовнический районный суд (Город Москва) // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/Qi3HnbaBGg5p/ (дата обращения: 04.05.2022).

50. Приговор № 1-336/2017 от 27 сентября 2017 года Рудничный районный суд г. Кемерово Кемеровской области // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/13Zhhdo4xmLK/ (дата обращения: 08.004.2022).

51. Приговор № 1-221/2017 от 11 мая 2017 года Центральный районный суд г. Челябинска // Судебные и нормативные акты РФ. URL: https://sud-praktika.ru/precedent/256201.html (дата обращения: 09.05.2022).

52. Приговор № 1-89/2017 03 апреля 2017 года Ленинский районный суд г. Ульяновска // Судебные и нормативные акты РФ. URL: https://sud-praktika.ru/precedent/295713.html (дата обращения: 04.05.2022).