Министерство внутренних дел Российской Федерации

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

Кафедра криминалистики

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: Методика расследования мошенничества в сфере компьютерной информации.

Выполнил: Райманов Айдар Сириневич
(фамилия, имя, отчество)
Правовое обеспечение национальной безопасности, 2013 г., 131 уч.гр.
(специальность, год набора, № группы)

Руководитель: старший преподаватель кафедры криминалистики
(ученая степень, ученое звание, должность)
Лихачева Алевтина Андреевна
(фамилия, имя, отчество)

Рецензент: начальник ЭКЦ МВД России по Республике Татарстан, полковник полиции
(должность, специальное звание)
Мухаметзянов Анас Харисович
(фамилия, имя, отчество)

К защите _____
(допущена, дата)
Начальник кафедры _____

Дата защиты: "___" _____20___г. Оценка _____

Казань 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы дипломной работы. Увеличение объема и развитие информационных технологий открывает возможность использования их в различных областях жизнедеятельности. Соответственно данные процессы в значительной мере ускоряют социально-экономическое развитие общества и позволяет взаимообмен информацией, используемой в компьютерных технологиях. Вместе с этим, появилось социально опасное явление, называемое киберпреступностью. Так, действиями киберпреступников базирующихся на разных уровнях экономике России нанесён ущерб в 203,3 млрд. руб., что равно 0,25% объёма ВВП, в 2015 году прямой финансовый ущерб составил 123,5 млрд. (0,15% от ВВП), а затраты на ликвидацию последствий более 79,8 млрд. (0,1% от ВВП). Данные сведения опубликованы в совместном исследовании Group-IB, Фонд развития Интернет-Инициатив (ФРИИ) и Microsoft. В течение четырех кварталов – со II квартала 2015 года по I квартал 2016 года киберпреступники украли около 5,5 млрд. руб., что на 44% больше похищенного за предыдущий отчетный период, сделала вывод Group-IB в исследовании.[1]

Изучая статистику также можно выявить что, число киберпреступности с 2013 года увеличилось в шесть раз. В 2017 году было зафиксировано 67 тыс. IT-преступлений. В 2013 году этот показатель составлял 11 тыс.[2]

На сегодняшний день одной из главных задач государства является защита личности, ее прав и свобод, охрана интересов общества и государства путем быстрого реагирования на преступность, его расследование, изобличение и назначение справедливого наказания виновных лиц; недопущение привлечения невиновных лиц к уголовной ответственности. Именно правоохранительные органы, в чьи обязанности входит обнаружение преступлении, выявление лиц, их совершивших, привлечение виновных в

---

[1] [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Россия (дата обращения: 17.12.2017).

[2] [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Россия (дата обращения: 15.01.2018).

преступлении к ответственности в соответствии с законом Российской федерации. Несомненно, эффективному решению указанных задач будет способствовать использование всех достижений информационных технологий в деятельности органов уголовного преследования.

Важным условием совершенствования деятельности органов уголовного преследования является оптимальное использование интеллектуального потенциала сотрудников указанных органов. Этому должно способствовать эффективное внедрение в практику научно-технических достижений в области криминалистической техники, рациональное использование средств оргтехники, применение передовых технологий. Повышение эффективности работы органов уголовного преследования в современных условиях практически невозможно без внедрения в их деятельность новых информационных технологий, использования современных средств компьютерной техники. Это позволит, во-первых, добиться качественного улучшения информационного обеспечения раскрытия и расследования преступлений и, во-вторых, освободить органы уголовного преследования от выполнения значительного объема технической работы, требующей больших временных затрат.

Повышение эффективности предварительного расследования по уголовным делам о кибермошенничестве невозможно без определения факторов, которые способны оказывать заметное негативное влияние на качество процедуры расследования уголовного дела. Во-первых, это касается несовершенства норм отечественного уголовного права, предусматривающих ответственность за кибермошенничество. Данная проблема предопределяет неизбежное возникновение у правоприменителя сложностей в грамотной квалификации рассматриваемой разновидности мошенничества. Во-вторых, отсутствует в полной мере адекватное сложившейся криминогенной ситуации криминалистическое обеспечение процедуры расследования этой категории уголовных дел (как на уровне криминалистической методики, так и на уровнях криминалистической тактики и техники). В-третьих, степень профессиональной

квалификации субъектов расследования не всегда в полной мере соответствует современным требованиям, что, безусловно, не может не сказаться на качестве предварительного расследования по уголовным делам о кибермошенничестве. В-четвёртых, негативное воздействие оказывает недостаточная координация совместных усилий правоохранительных органов с государственными и негосударственными структурами, специализирующимися на обеспечении безопасности в сфере телекоммуникаций и компьютерной информации.

Если оценивать состояние и тенденции развития отечественного уголовного законодательства, призванного стать основой борьбы с киберпреступностью, то важно отметить, что злободневность и сложность проблемы противодействия криминальной активности в сфере использования компьютерных технологий во многом предопределила направления и динамику совершенствования уголовного законодательства Российской Федерации последнего времени. В этой связи в целом как позитивные можно оценить изменения, произошедшие в Уголовном кодексе РФ (далее – УК РФ) в 2011–2012 гг. В частности, одним из таковых можно считать введение в ст. 272 УК РФ[1] понятия компьютерная информация. Раскрытие законодателем содержания данного термина оказало положительное влияние на процедуру доказывания по уголовным делам, где можно обнаружить подобного рода информацию в качестве составляющей способа преступления. Кроме того, в указанный период законодателем была реализована идея расширения и детализации составов киберпреступлений.

Исходя, из этого в самостоятельную статью УК РФ (ст. 159.6) была выделена такая разновидность киберпреступности, как мошенничество в сфере компьютерной информации, что также оказало позитивное воздействие на практику противодействия кибермошенничеству.

Киберпреступники совершенствуя схемы и способы совершения мошенничества в сфере компьютерной информации, используют достижения

---

[1] "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 30.03.2016) // "Собрание законодательства РФ", 17.06.1996, N 25;

науки, прогрессы компьютерных технологии, расширяют познания применения областей программирования. Для достижения корыстных целей, субъекты противоправного деяния объединяются в группы, не редко данные преступные группы носят межгосударственный характер. При этом от преступного действия потерпевшими становятся не только конкретные физические лица, но и юридические лица, независимо от форм собственности, а также публично-правовые образования (государственные и муниципальные органы, учреждения и организации), в связи с чем повышается ущерб наносимый в целом экономике страны. Перед государством возникла необходимость принятия соответствующих адекватных мер, позволяющих эффективно противодействовать фактам мошенничества, совершаемого в сфере компьютерной информации. Президент РФ В. Путин в ходе выступления на расширенном заседании коллегии Федеральной службы безопасности Российской Федерации (26 февраля 2016 года) поручил ведомству разработать систему защиты от информационных угроз и киберзлоумышленников[1].

Степень разработанности темы исследования. В науке криминалистике состояние данного вопроса характеризуется, с одной стороны, недостаточной научной разработанностью, а с другой — большой реальной значимостью для практики борьбы с преступностью. Это нашло свое отражение в диссертационных исследованиях В.В. Полякова (2011), Шурухнова (2012), И.Г. Иванова (2012), А.И. Усова (2012), А.Н. Яковлева (2013), В.А. Мещерякова (2013), А.А. Васильева (2014), Р.А. Белевского (2014), Л.Н. Соловьева (2015), А.И. Семикаленовой (2015), В.В. Крылова (2015), В.П. Хомколова (2016), Н.Г. Ю.В. Гаврилина (2016), В.Б. Вехова (2016) Г.В. Семенова (2016), А.С. Егорышева (2017), В.А. Милашева (2017), и других ученных.

Проблемы использования специальных познаний при расследовании преступлений в сфере компьютерной информации были рассмотрены в научных работах Е.Р. Россинской, А.И. Усова, В.А. Мещерякова, В.Б. Вехова; в

[1] [Электронный ресурс]. URL: http://portaltele.com.ua/news/officially/2013-02-14-13- 34-52.html (дата обращения: 14.11.2017).

сфере высоких технологий, в научных работах Г.В. Семенова, И.В. Лазаревой. Некоторые аспекты были также затронуты В.И. Вараксиным, Ю.В. Гаврилиным, А.Ю. Головиным, А.В. Гортинским, Н.А. Ивановым, С.П. Кушниренко, М.Ш. Махтаевым,.А.Б. Нехорошевым, Л.Н. Соловьевым, О.В. Тушкановой, М.Н. Шухниным, И.Ю. Юриным, А.Н. Яковлевым и др.

Объектом исследования выступают уголовно процессуальные и криминалистические проблемы современного этапа развития общества при расследовании мошенничества сфере компьютерной информации.

Предметом исследования являются закономерности использования специальных познаний в сфере компьютерной информации и высоких технологий при расследовании преступлений, а также закономерности собирания, исследования, оценки и использования доказательств в расследовании обозначенных преступлений

Целью исследования явилось рассмотрение теоретических и практических вопросов использования специальных познаний в области компьютерной информации и высоких технологий при расследовании мошенничества совершаемых с использованием средств компьютерной техники, разработка научно обоснованных рекомендаций и рациональных способов организации взаимодействия следователя со специалистами и экспертами при применении указанных специальных познаний.

Для достижения указанной цели сформулированы следующие *основные задачи:*

– дать криминалистическую характеристику мошенничества в сфере компьютерной информации как объекта криминалистического анализа

– рассмотреть особенности производства отдельных следственных действий при расследовании мошенничества в сфере компьютерной информации.

При решении указанных задач использовались общие, частные и специальные методы познания, применяемые в криминалистике и других юридических науках: формально-логический, функциональный, сравнение,

анализ и синтез, системно-структурный анализ. Были проанализированы как публикации отечественных авторов, посвященные проблемам применения информационных технологии в деятельности органов уголовного преследования, так и зарубежный опыт по рассматриваемому вопросу.

Структура данной работы состоит из введения, двух глав, четырёх параграфов входящих в них, заключения и списка использованной литературы.

ГЛАВА 1. МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА

§1. Криминалистическая характеристики мошенничества в сфере компьютерной информации

Анализируя криминалистическую характеристику мошенничества в сфере компьютерной информации, следует учесть следующие положения. Под криминалистической характеристикой преступлений в общих чертах понимается «система сведении научной категории о типичных признаках отдельно взятых преступлении имеющие значение для криминалистики, определение которых дает возможность найти путь эффективного расследования, раскрытия и изобличения виновных лиц в их совершении»[1].

Так, В.П. Лавров, криминалистическую характеристику определяет, как систему сведений о признаках определенной категории преступлений, которая позволяет сделать вывод об оптимальных путях их раскрытия и расследования.[2]

Совокупность наиболее характерной, криминалистически значимой информации определённого рода преступлении, способствующих выдвинуть версии о событии преступления и личности преступника, определяющие верную оценку ситуации, возникающие в процессе расследования и раскрытия компьютерных преступлении, обусловливающей применение соответствующих методов, приемов и средств которые составляют понятие криминалистической характеристики.

В криминалистическую характеристику должно быть включено

---

[1] Самойлов А.В. Современное состояние учения о криминалистической характеристике преступлений // Российский следователь. – 2012. – № 22. – С. 5–6.
[2] Лавров В.П. Криминалистика. М.: Норма, 2014. С. 33.

наибольшее число признаков, имеющих криминалистическое значение[1], и данное положение является принципиальным.

Так, А.А. Протасевич и Л.П. Зверянская выделяют следующие криминалистически значимые элементы характеристики киберпреступлений:

– способ совершения преступления;

– способ сокрытия преступления;

– особенности следовой информации;

– особенности обстановки совершения преступления (место совершения преступления, время совершения преступления и др.);

– личностная характеристика преступника;

– особенности непосредственного предмета преступного посягательства[2].

Такую же классификацию элементов криминалистической характеристики давал в своих трудах и Рафаил Самуилович Белкин. Соглашаясь с такой общей структурой, берем её за основу конструирования криминалистической характеристики мошенничества в сфере компьютерной информации, учитывая особенности и специфику данного вида преступного деяния, подвергнется корректированию нами. Так, к существенным и наиболее полным отражающим цели практики элементом криминалистической характеристики мошенничества в сфере компьютерной информации следует отнести в первую очередь:

– способ совершения преступления;

– компьютерные орудия и средства, используемые для совершения преступления;

– место и обстановка совершения преступной деятельности.

Следует рассматривать данные элементы в их взаимосвязи и

---

[1] Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. … д-ра. юрид. наук: 12.00.2013 г.

[2] Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С. 45-47.

взаимообусловленности.

Остановимся на данных элементах криминалистической характеристики мошенничества в сфере компьютерной информации более подробно. Основным из них является способ, точнее способы, совершения преступления мошенничества в сфере компьютерной информации. Как отмечает А.А. Комарова: «Если взять любую форму мошенничества его определяющим признаком выступает способ совершения преступления: обман или злоупотребление доверием, который является единственным способом совершения данного преступления».[1]

При определении понятия мошенничества Р.С. Атаманов, предлагает использовать, кроме «хищения», так же понятие «завладение». Для достижения промежуточных результатов преступник использует способы мошенничества: обман и злоупотребление доверием, а именно введение в заблуждение собственника или владельца предмета посягательства, таким образом, чтобы впоследствии, беспрепятственно получить имущество от жертвы.[2]

Сложный характер способа совершения мошенничества в сфере компьютерной информации имеет полноструктурное строение. В качестве основных его частей можно выделить: подготовка к совершению мошенничества, реализация самого способа совершения, а также действия направленные на сокрытие следов доведенного до конца преступления.

Отдельно следует остановиться на том, что мошенничество в сфере компьютерной информации заключается в том, что на этапе подготовки совершения данного вида деяния злоумышленник направляет свою деятельность на сокрытие следов еще не совершенного преступления. Выражается это в том, что при создании вредоносных программ, через которые будут осуществляться несанкционированные доступы, проникающие в компьютер жертвы без информирования об этом пострадавшего, преступником

---

[1] Комарова А.А. Интернет-мошенничество: проблемы детерминации и предупреждения: монография. М.: Юрлитинформ, 2014. С. 9.

[2] Атаманов, Р.С. Основы методики расследования мошенничества в сети интернет: автореф. дис. … канд. юрид. наук: 12.0012 / Р.С. Атаманов. М., 2012. С. 12.

учитываются настройки анонимного и удаленного (на расстоянии) доступа в программное обеспечение (например Skype и т.п.).

Кроме этого, преступниками разрабатываются соответствующие сайты, на которых пострадавший получает информацию, либо скачивает и устанавливает вредоносную программу через которые преступник осуществляет вовлечение жертву в преступные схемы, все это зависит от выбранного способа совершения преступления.

Аналогично, по схожей схеме в зависимости от способа совершения мошенничества в сфере компьютерной информации подбирают лиц, среди которых будут распределяться роли, также возложение на них определенных обязанностей без распределения которых невозможно совершение с минимальным оставлением следов на компьютере на который будет осуществляться доступ, последующая подготовка определённых орудии и средств (компьютерно-технические средства, провайдер, компьютерная сеть и т.п.), необходимых для совершения мошенничества данного вида.

Особенностью подготовки программы является то что, лица их создающие для заказчика в некоторых случаях могут не знать об истинных целях своей деятельности. Разработав программу лицо может не догадываться о том, что заказчик может использовать ее в качестве вредоносной, причинять вред с помощью неё.[1]

Анализ следственной и судебной практики, а также репрезентативный опрос пользователей ПК и сотрудников правоохранительных органов позволяет констатировать, что на сегодняшний день наиболее распространёнными способами мошенничества в сфере компьютерной информации с использованием компьютерных сетей являются:

– незаконный доступ в учетные записи с использованием регистрационных данных пользователя (appstore, mail, googlemarket и т.п.) с дальнейшим использование в мошеннических целях;

---

[1] Комаров А.А. Интернет-мошенничество: проблемы детерминации и предупреждения: монография. – М.: Юрлитинформ, 2013. С. 31-32.

– осуществление платежных операции на различных интернет-ресурсах (как в российском сегменте сети интернет, так и зарубежом) с последующим обналичиваением имеющихся безналичных средств, либо приобретение различных товаров (для личного пользования, либо с последующей реализацией) в сети интернет (для осуществления транзакции мошенники также имеют в наличии данные о картах пострадавшего);

– размещение ложной информации для привлечения инвесторов (будущую жертву) путем введения их в заблуждение, через специально созданные сайты (либо размещение сообщении с «привлекательным» содержанием на форумах) о возможности получения прибыли за краткосрочный период времени, с заключение договора сделки;

– взлом электронных кошельков (путем рассылки смс-сообщении со ссылкой на вредоносную программу) с последующим хищением безналичных денежных средств, и возможностью распорядиться ими в корыстных целях. (например, покупка товаров в интернет магазинах, либо перевод на другие электронные системы, приспособленные под использование электронных денежных средств «YandexMoney», «Webmoney», «PayPal», «Qiwi» и др.);

– рассылка смс-оферт об инвестировании определенной деятельности бизнесмена посредством перевода денежных средств. В случае одобрения пострадавшим, то есть поступлении акцепта просьба перевести персональные данные (для юридического лица банковские реквизиты, образцы подписей, оттиски печати);

– рассылка спам-сообщении на электронную почту жертв, содержащие вредоносные программы. Рекламные объявление могут содержать различного рода и характера сообщения, которыми заинтересуется пострадавший и перейдет по ссылке присланной на его электронную почту (о приобретении медикаментов и БАДов и способах диет и похудении за месяц на определенный вес; бесплатного или дешевого приобретения услуг и товаров; обогащения за короткий срок времени путем выгодного инвестирования;

– получение у жертвы денег на оплату виртуальных товаров, создание

мошенниками сайтов известных интернет-магазинов;

– проведение лже-торгов через сеть интернет (выставление на продажу несуществующий лот), проведение лже-аукционов (для продажи товара по завышенным ценам аукционного товара, продавцы мошенники-делают самостоятельные ставки тем самым покупатели для приобретения данного товара делают повышенные ставки);

– организация благотворительных акций через Интернет, где предлагается на счета для конкретных лиц (инвалидов, нуждающихся в срочных операциях и т. п.) перечислять денежные суммы. С этой целью также могут создаваться сайты-клоны реальных благотворительных организаций;

В качестве следующего элемента криминалистической характеристики является следы преступной деятельности. Любой преступник, совершая то или иное деяние наказуемое уголовным законом оставляет следы, главной целью деятельности по расследованию преступления является сбор информации о преступном событии. Однако в рассматриваемом нами виде преступной деятельности информация представляет собой специфическую категорию[1].

Нельзя не согласиться с мнением о том, чтобы определить относимость определенной компьютерной информации к доказательствам возможно определить только при воспроизведении информации с использованием специальных технических устройств путем анализа ее содержания и свойств только после данных процедур получить ответ об отнесении к доказательствам. Оценка относимости предполагает, что проверяемая информация соответствует предмету доказывания, и определяет, как они связаны между собой, обстоятельства совершения преступления, какой поставленной версии она соответствует и какой противоречит.[1]

Данное положение служит основой для формирования рассматриваемого элемента криминалистической характеристики мошенничества, совершаемого в сфере компьютерной информации. При этом важное значение имеет соблюдение целостности компьютерной информации, т.е. сохранение ее в полном неизменном

[1] Зигура Н.А., Кудрявцев А.В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. М., 2015. С. 125.

первоначальном виде. Достоверность доказательства производится в ходе следственных действий, при выдвижении следственных версий и принятии процессуальных решений, и определяется совокупностью анализа всего процесса формирования информации, а именно условиями получения, восприятия, фиксации, закрепления, сохранения целостности, анализа содержания и свойств. Оценка компьютерной информации как доказательства с точки зрения их достоверности ставит две проблемы: доказывания правильности этих данных и правильности функционирования программ обработки»[1].

Как подчеркнул А.Г. Волеводз, при расследовании мошенничества в сфере компьютерной информации можно с уверенностью отметить о возможности обнаружения следов, представляющие собой сведения о злоумышленнике оставленные им при прохождении по проводной, радио-, оптической и другим электро- магнитным системам связи, которые в научной литературе носит название «сведения, передаваемые по сетям электрической связи», либо сохраненные в базе данных поставщика услуг как злоумышленнику так и потерпевшему (провайдерами) «исторические данные», переданные сообщения либо о сеансах полученных обманным путем преступником «данные о потоках информации».[2]

Следует учитывать и тот момент, что для качественного достижения целей по обработке и хранению оставленных следов на носителе информации, требует использования соответствующих материальных средств (компьютерно-технических). Именно данное условие дает возможность материально зафиксировать отображенный след на носителе информации. В случае выявления, следов, несущих в себе информацию о киберпреступниках, даже с учетом ее блокирования, уничтожения и т.п. изъятию подлежать компьютерные средства, в том числе жесткий диск, для полного восстановления полной преступной деятельности которая содержится на

---

[1] Протасевич А.А., Зверянская Л.П. Проблемы собирания и оценки компьютерной информации как доказательства // Современная криминалистика: проблемы, тенденции, имена (к 90-летию профессора Р.С. Белкина): сб. материалов 53-х криминалистических чтений: в 3 ч. М.: Академия управления МВД России, 2012. Ч. 3. С. 274-275.

[2] Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. – 2012. – №1. С.4-12.

самой компьютерной информации.

Рассматриваемые виртуальные следы, в том виде, в котором оно описано выше, являются ничем иным, как материальными следами-отображениями.[1] На основании того, что они являются материально зафиксированными, отображаемыми на материальных носителях, что позволяет их обнаружить, используя методы и средства, разработанные наукой криминалистики.

Таким образом, следы оставляемые при совершении мошенничества в сфере компьютерной информации, по нашему мнению, можно разделить на два вида:

– *традиционные следы:* следы, оставляемые преступником в момент реализации своих преступных замыслов в конкретном месте нахождения (сюда можно отнести, внешний облик преступника, который сумел запомнить потерпевший если имело место встреча при подготовительных действиях, либо имело место встреча с провайдером при заключении договора о предоставлении услуг проводимых перед совершением преступления; следы пальцев рук на клавиатуре компьютера, клавишах банкомата, на пластиковых платежных картах; следы оставленные на материальных средствах связи используемые самим преступником)

– *компьютерные следы,* любые действия, направленные на достижение преступной цели через программируемые устройства, итоговое отражение которых остается в электронной памяти (например, осуществление преступником компьютерного доступа, путем использования средств мобильной и интернет связей). Данные следы получают свое отражение:

1) в административных журналах, в журналах безопасности в которых фиксируются действия, как включение, выключение, операции различного рода с использованием памяти компьютера;

2) в реестре компьютера так называемых reg-файлах, записывающие проведенные действия установленными программами на компьютерное устройство (Установка, изменение исходных данных, включая удаление определенной

[1] Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореферат дис. ... канд. юрид. наук: 12.00.09 / В.Ю. Агибалов. Воронеж, 2010; Мещеряков В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков // Библиотека криминалиста. – 2013. – № 5 (10). С. 265-269.

программы и т.д);

3) в log-файлах в которых записываются проделанные действия пользователем Интернет ресурса, локальных сетях и иных сетях;

4) сохраненные последние измененные операции в свойствах файлов (например, даты создания, даты удаления и т.д.)[1].

Традиционно в науке криминалистики *местом совершения* преступления принято понимать – место реализации объективной стороны преступления.[2] Особенностью рассматриваемого нами элемента криминалистической характеристики, является то, что на месте совершения преступления преступник оставляет наибольшее количество значимых для расследования уголовного дела следов. Влияние на восстановление и формирование всей следовой картины как материальных, так и идеальных следов преступления несомненно велико, так как обнаруженные на месте совершения преступления следы обладают максимальной информативностью о противоправном деянии.

Как справедливо подчеркнул Л.Г. Видонов, «главенствующей характеристикой места преступления являются его признаки, определяющие его назначение для людей и отличающие его от окружающей местности и обстановки»[3].

Возможность контроля движения информации в сети Интернет по мнению И.Н. Воробца, является созданная «система адресации в сети интернет» характерной особенностью которой является присвоение каждому без исключения компьютеру, подключаемое к сети, уникального идентификационного номера (IP-адреса). IP-адрес – это набор четырех разделенных точками чисел (например192.168.100.47.). Для удобства работы

---

[1] Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. – 2016. – №11. С. 45-47.

[2] Место преступления, участок местности или помещение, где было совершено преступление. Белкин Р С. Криминалистическая энциклопедия. 2-е изд. доп. М.: Мегатрон XXI, 2000. С. 115. В нашем случае справедливым будет рассмотреть и понятие места происшествия, под которым понимается, участок местности или помещение, где были обнаружены следы события, требующего расследования. Там же. С. 115.

[3] Видонов Л.Г. Криминалистическая характеристика убийств и системы типовых версий о лицах, совершивших убийства без очевидцев. Горький, 2013. С. 11.

числовые адреса заменяются символьными с использованием доменной системы преобразования имен. Символьные имена наделены возможностью преобразовываться в IP-адрес и соответственно имеют свойство обратного действия, то есть присваивать имя домена по числовому адресу, данная операция осуществляется благодаря существующей системе доменов. IP-адрес делятся на два вида:

– статистический;

– динамический.

Доступ к размещенной в сети-Интернет информации, а также ее внутрисетевой обмен осуществляется специализированными организациями так называемыми поставщиками услуг (провайдерами)[1].

При создании компьютерных сетей использовалась система, позволяющая анализировать, с возможностью контролирования процесса перемещения (в определенное запрашиваемое время) информации внутри ее, а также установления источника ее происхождения и конечного получателя передаваемой информации. Данное обстоятельство имеет как негативный аспект, так и позитивный. С одной стороны, негативно отражается на соблюдении законных прав и интересов гражданина, с другой стороны, регулирование и контроль в сети-Интернет позволяет быстро и эффективно реагировать на преступное деяние, совершаемое в сфере компьютерной информации.

Обращая внимание на характерные особенности компьютерной сети, можно определить местом совершения мошенничества в сфере компьютерной информации саму информационно-телекоммуникационную сеть, в которой выполняются функции по вводу, удалению, блокированию, модификации компьютерной информации либо иное вмешательство в среду хранения информации, обработки или передачи компьютерной информации. С другой

[1] Воробец И.Н. Глобальная сеть Интернет, как пространство для совершения преступлений // Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России: доклады междунар. науч.-практ. конф. / под ред. А.М. Кустова, Т.Ю. Прокофьевой. М.: МЭЙЛЕР, 2012. С. 71.

стороны, местом совершения рассматриваемого вида преступлении является место нахождения конкретного компьютера, через который осуществляется неправомерный доступ. Именно на месте нахождения компьютера используемого для совершения мошенничества в сфере компьютерной информации, находится значимый объем информации, характеризующий механизм совершения преступления (способ, орудия и средства, следы и т.п.).

Таким образом, в рассматриваемом преступном деянии местом совершения преступления является местонахождение компьютерно-технических средств, с которого отправляются команды.

С данной точкой зрения согласны также и другие ученые. Указывая на существующие трудности определения места происшествия, научные деятели утверждают, что при совершении данного вида мошенничества путем получения неправомерного доступа к компьютерной информации, может быть несколько мест происшествия:

– рабочее место, рабочая станция – место сбора и обработки информации, ставшей предметом преступного посягательства;

– место постоянного хранения или резервирования информации – сервер или стример;

– место установленных технических средств для неправомерного доступа к компьютерной информации, находящийся в отдаленном месте при стороннем взломе путем внешнего удаленного сетевого доступа;

– место подготовки как программно-технических средств совершения преступления (разработка программ, обеспечивающих взлом, подбор паролей, создание вирусных программ) или место непосредственного использования информации (искажение исходной информации, копирование), полученной в результате неправомерного доступа к информации содержащейся на компьютере жертвы.[1]

«Преступное деяние, – как подчеркивает автор Колоколов Н.А., – считается

[1] Колоколов Н.А. Преступления против собственности: комментируем новеллы УК РФ // Мировой судья. – 2013. – №1. С. 6-15.

законченным с момента получения электронных безналичных денежных средств, и возможности самостоятельно распоряжаться такими деньгами (чужим имуществом)»

Следует отметить также тот факт, кроме телекоммуникационной сети, местом совершения мошенничества является место, «обналичивания» безналичных денежных средств, полученных преступным путем. В зависимости от способа перевода денежных средств жертвы в распоряжение преступника, местами «обналичивания» могут являться банкоматы, интернет-магазины, кассовые залы банков, электронные карты (независимо выпущена она банком либо выпущена электронным кошельком такие как QIWI, WebMoney) и т.п. Надо отметить, что процесс использования преступных денежных средств, полученных путем мошенничества сфере компьютерной информации в целом оказывает воздействие на характер следообразования, который влияет на дальнейшее расследование уголовного дела.

Как достоверно подчеркивает А. Смушкин, для рассматриваемых нами преступлении возможно использование двухуровневой приспособленности программ:

– «стандартные» – программы легкого использования, находящиеся в свободном доступе в сети-Интернет, данные программы не нуждаются в специальных познаниях для их применения, возможно также вариант так называемых вредоносных программ, находящиеся в специальном пространстве, не имеющего свободного доступа участка Интернета, и уже приспособленные для совершения противоправных действии соответственно их использование не предусматривает дополнительного умения и навыков;
– «приспособленные» программы – переделанные под свои нужды злоумышленником учитывая все нюансы и тонкости подготавливаемого преступления, возможен также вариант

самостоятельного написания данной категории программ.[1]

На сегодняшний день киберпреступниками подготовлено и функционирует большое количество программ для совершения преступлении в сфере компьютерной информации. По мнению О.В. Зубань, по скромным оценкам, вредоносные-троянские программы насчитывают несколько миллионов уже функционирующих и действующих на электронных носителях компьютерной информации по всему миру. Такие программы автообновляются, получают инструкции с заранее подготовленных сайтов или каналов IRC, рассылать спам, осуществлять «DDoS-атаки»»[2].

Криминалистическая характеристика мошенничества в сфере компью-терной информации представляет собой систему значимой для криминалистики информации, признаках и свойствах преступления, предусмотренного ст.159.6 Уголовного кодекса Российской Федерации, состоящего из таких элементов как:

– непосредственный предмет преступного посягательства;

– способ совершения преступления, орудия и средства преступления;

– следы и механизм следообразования;

– обстановка совершения преступления, его пространственно-временной континуум, которые характеризуются корреляционной зависимостью между элементами криминалистической характеристики, и особенностью проявления данных видов преступлении в компьютерно-информативной среде, что отличает данный вид преступной деятельности от других видов преступлении предусмотренных УК РФ, и дает возможность для выдвижения типичных версии о событии преступления и личности преступника, определения пути поисковых мероприятии расследуемого уголовного дела.

Таким образом, изложенное выше позволяет констатировать тот факт, что корреляционные (взаимозависимые) связи между элементами

[1] Смушкин А. Виртуальные следы в криминалистике. 2014 г. С. 43-45.
[2] Зубань О.В. Проблема спама и ее решения // Материалы конференции. М., 2013.С. 2-3.

криминалистической характеристики мошенничества в сфере компьютерной информации дают возможность детально просмотреть и анализировать ход изучения положении науки и практики, что дает возможность подготовки сотрудников правоохраняемых структур на высоком уровне, для расследования данного вида преступления.

§2. Механизм совершения преступления, его соотношение с криминалистической характеристикой

Наряду с категорией криминалистической характеристики, в науке криминалистике активно изучается механизм преступления. Связано это с тем, что последнее характеризует функциональную сторону преступления. Д.В.Ким, рассматривает механизм преступления как «взаимодействие элементов криминалистической характеристики преступления, начиная с процесса подготовки, совершения и заканчивая сокрытием преступного деяния, приводящую к образованию следов, имеющих значение для уголовного дела… Криминалистический механизм, включает в себя элементы криминалистической характеристики.[1] Учитывая, что две категории схожи в содержательном аспекте, все же понятия «механизм преступления» и «криминалистическая характеристика» отражают «разные стороны, одной медали». Таким образом, можно смело говорить о том, что, механизм представляет преступление в динамическом состоянии, а криминалистическая характеристика отражает систематизированные результаты научного познания

[1] Ким Д.В. Проблемы теории и практики разрешения криминалистических ситуаций в процессе раскрытия, предварительного расследования и судебного рассмотрения уголовных дел: дис. … д-ра юрид. наук: 12.00.09 / Д.В. Ким. Барнаул, 2009. С. 106-107.

в статичной и завершённой форме научного познания.[1]

На сегодняшний день в науке, ученые-криминалисты под механизмом преступления понимают процесс взаимодействия, как прямых, так и косвенных участников между собой, а также их взаимодействие с материальными объектами, соответствующими орудиями, средствами и иными объектами, связанными с преступным деянием. В литературе справедливо отмечается, механизм преступления сопутствует появлению значимой информации о преступлении, о ее участниках и результатах преступной деятельности лиц.[2]

Целесообразно указать на два основных свойств, характерных механизму преступления. К первому свойству относится системность, включающий взаимосвязь абсолютно всех элементов механизма преступления, в их взаимодействии. Ко второму свойству ученые относят его динамичность, отражающий его функциональную сторону, выражающийся во взаимодействии и взаимосвязи.

Ученый А.М. Кустов, в качестве элементов механизма преступления выделяет:

– деятельность лица, совершающего преступное деяние;

– комплекс действии потерпевшего лица;

– комплекс поступков иных лиц, связанных с преступным событием;

– отдельные элементы обстановки, используемые участниками преступного посягательства.[3]

Понятие «механизм преступления» ориентировано на элементы состава преступления, относящегося к его субъективной стороне. При этом в процессе ретроспективного познания, каковым является расследование преступлений,

---

[1]Айвазова О.В. Криминалистическая характеристика преступлений как систематизированное отражение механизма преступной деятельности: результаты научной полемики // Вестник Томского государственного университета. – 2014. – №389. С. 155.

[2] Челышева О.В. Механизм преступления и криминалистическая характеристика // Вестник криминалистики. Вып. 2. М., 2010. С. 13.

[3] Кустов А.М. Теоретические основы криминалистического учения о механизме преступления. М., 2015. С. 24.

установление элементов субъективной стороны (цели и мотивов преступления, вины и её форм) возможно лишь на основании единственного «объективного материала» – конкретных действий участников преступного события.

Исходя из вышеуказанного, к элементам механизма мошенничества в сфере компьютерной информации, целесообразно будет отнести:

– деятельность лица, совершающего преступление – действия кибер-преступника, совершающего мошенничество в сфере компьютерной информации путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей;

– действия, жертвы в отношении которого совершается мошенничество, предусмотренное статьей 159.6 УК РФ;

– взаимосвязанные действия лиц, косвенно связанных с преступлением мошенничества в сфере компьютерной информации;

– элементы обстановки, используемые участниками преступного собы-тия, включая предмет преступного посягательства.

Данные элементы находятся в постоянном движении и развитии, создавая тем самым систему взаимодействии участников и среды преступления, в которой совершается данное деяние. Полученные сведения и информацию о данных элементах эффективно использовать для раскрытия и расследования данного вида мошенничества. Данные сведения определяют направленность поиска на цель разоблачения преступника.

С вышеуказанной позицией в науке криминалистике согласны также и научные деятели, например, ученый В.К. Гавло, отмечал, что механизм преступления, дает ответы на вопросы о том, как в различной обстановке

происходит взаимодействие компонентов преступления.[1]

Основным элементом системы механизма мошенничества данного вида является субъект преступного посягательства. Еще в своих научных трудах Р.С.Белкин, неоднократно подчеркивал о том, что важное значение имеет любая хоть и типичная информация о личности преступника.[2]

Лицо совершившее криминальные деяния, обладает рядом свойств, а именно:

– биологические;

– физические;

– социальные,

именно данные свойства присущи информации, оставленные преступником на месте происшествия в виде материальных и идеальных следов.[3]

Анализ практической деятельности свидетельствует о том, что преступление, связанное с рассматриваемым видом мошенничества, находится в плотной связи с субъектом преступления. При этом на наш взгляд формированию свойств и качеств личности преступника, совершающего мошенничество в сфере компьютерной информации формируются под воздействием условии социальной среды и носят устойчивый характер.

Таким образом следует отметить тот факт, одним из главных черт механизма совершения мошенничества в сфере компьютерной информации, является то что, преступник для совершения такого вида преступления должен обладать соответствующими компьютерными средствами, а также в его распоряжении должна находиться локальная сеть к которой подключается данная техника.

Характеристика личности, анализированная судебной практикой, показывает, что в 95-ти процентах субъектом мошенничества предусмотренное

---

[1] Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск, 2015. С. 191.

[2] Белкин Р.С. Проблемы, тенденции, перспективы. От теории к практике. М., 1988. С. 178.

[3] Кустов А.М. Криминалистика и механизм преступления: цикл лекций. М.: МПСИ; Воронеж: МОДЕК, 2012. С. 112.

ст. 159.6 УК РФ, являются лица мужского пола, в возрасте от 18 до 36 лет.

В научной литературе предлагается классифицировать всех преступников, в зависимости от уровня и умения пользоваться компьютерной техникой и ее программным обеспечением, в том числе и сложными компьютерно-техническими устройствами. Их различают по следующим основаниям:[1]

1) профессионалы в сфере IT-техники, которые совершают преступную деятельность в чьих распоряжениях находятся уже существующие программы высшего класса, либо которые сами создают уникальные программы для совершения преступления в сфере компьютерной информации;

2) так называемые непрофессиональные злоумышленники компьютерных преступлении, (в ряде случаев имеют специальное образование, а также занимающиеся «самоучкой»). В свою очередь их можно поделить:

– продвинутые пользователи, создающие несложные компьютерные программы, понимающие механику работы компьютерной техники и ее программ;
– уверенных пользователей (знают, как работают компьютерные системы, могут сами устанавливать компьютерные программы).

Система функционирования компьютерной сети имеет свои некоторые особенности, она построена таким образом, что операции, совершаемые при преступном деянии, позволяют завладеть киберпреступнику материальными ценностями, без установления контакта с потерпевшим от мошенничества в сфере компьютерной информации. Например, использование компьютерных сетей при продаже несуществующих товаров через сети-Интернет преступником, жертва может оплатить операцию реальными денежными средствами (оплата товаров и услуг пластиковыми картами, онлайн кошельком и т.п.) такой ложный товарообмен, способствует получению преступником денежных средств при отсутствии взаимодействующего контакта между

[1] Пучкова И.М. Психологические аспекты профессиональной подготовки пользователей ЭВМ: автореф. …канд. психол. наук: 19.00.03 / И.М. Пучкова. М., 2016 г.

продавцом и покупателем. Данный способ позволяет активизации преступных элементов, в целях извлечения материальных средств, с помощью компьютерной сети.

Следует обратить внимание также на тот момент, что все элементы механизма мошенничества в сфере компьютерной информации оказывают взаимовлияние друг на друга. Чем профессиональнее и квалифицированнее разбирается преступник в поставленном вопросе, тем изощрённее приемы и средства применяемые в ходе совершения, более детальный выбор орудии и средств используемые в целях достижения поставленных задач перед преступником.

Также в практической деятельности встречаются случаи, когда более профессиональные пользователи, при помощи модификации компьютерных средств, приобретая расходные материалы в торговых предприятиях, переделывают, приспосабливая программное обеспечение для достижения более высоких результатов от использования технических средств. Связано это с тем, что увеличивается скорость обработки информации для проникновения в компьютерную систему, лиц в отношении которых совершается мошенничество в сфере компьютерной информации.

К элементу механизма мошенничества в рассматриваемом виде преступлении относится поиск жертвы преступного посягательства. Поиск и выбор жертвы зависит от выбранного способа совершения преступником противоправного деяния. Такие способы характерны для организованных преступных групп. Именно организованный характер подчеркивает специфику механизма преступной деятельности мошенников.

«Субъект преступной деятельности (лидер группы), – отмечают ученые, планируя преступление, создает его мысленную модель, затем пытается передать подготовленную модель соучастникам, возможно даже ее фиксация на материальном носителе, что облегчает расследование преступления при обнаружении данной схемы. Затем запланированный план преступником переносится в плоскость решения своих поставленных задач, и начало действии

первоначального этапа, с дальнейшим ее развитием. Также субъекту занимающимся расследованием данного преступления следует учитывать, что на переходном этапе возможна незапланированная смена преступником своих дальнейших действии, которые требуют быстрого принятия решении для реализации запланированного преступного деяния».[1]

Анализ, а также опрос практических работников правоохранительных органов показывает, что при поиске жертв мошенничества рассматриваемого вида, преступники в основном используют для реализации умысла спонтанный подбор лиц, в отношении которых возможно использование имеющихся в наличии компьютерной техники. С дальнейшей рассылкой на адреса компьютерной техники потерпевшего различных предложении, содержащих вредоносные программы.

По мнению, И.Г. Чекунова, блокирование у пользователей программного обеспечения компьютера через сети-Интернет – является типичным способом совершения мошенничества, предусмотренного статьей 159.6 УК РФ.

В конечном итоге у лица на которое направил свой преступный умысел киберпреступник, появляется на экране вирусное окно «баннер», с информационным письмом о том, какие действия необходимо предпринять в дальнейшем, для возвращения в рабочее положение программного обеспечения компьютера. Как правило, в информативном письме указывается о том, что пользователь посетил сайт, отнесенный к запрещенному контенту, и для разблокировки необходимо пополнить баланс конкретного оператора сотовой связи (указывается в самом тексте, то есть преступники не скрывают контактный номер для совершения преступных действии), соответственно данное СМС-сообщение является платным. При этом, после выполнения указанной операции по перечислению денежных средств, необходимо дождаться специального пин-кода, с помощью которого он сможет

[1] Ершов В.А., Костылева Г.В., Милованова М.М. Методика расследования преступлений против жизни и здоровья граждан, совершаемых членами неформальных групп (движений): науч.-практ. пособие. М.: Юрлитинформ, 2017. С. 59.

разблокировать программное обеспечение, зараженное вирусом.[1]

Такой способ навязчивой рекламы называется «Спамминг» – это электронные рекламные сообщения анонимного характера, не запрошенная получателем. Данный способ совершения преступления отличается от других способов тем, что для внедрения в программное обеспечение вирусного рекламного сообщения не требуется согласия адресата, а также потерпевший не может отказаться от получения аналогичных сообщении «баннеров». Аналогом такой рассылки спама в «несетевом» пространстве являются «назойливые» рекламы на бумажном носителе оставляемые в почтовом ящике, а в виртуальном пространстве роль почты играет компьютерная техника, которые получают вирус через интернет-службы.[2]

Следует учитывать, что во всех случаях мошенничество в сфере компьютерной информации направлено на изъятие любых материальных средств потерпевшего, и дальнейшее обращение его в свою пользу. «Непосредственное завладение предметом посягательства, – отмечают О.Э.Згадзай и Л.С. Хафизова, – в большинстве случаев, выполняется преступником после того, как потерпевший введен в заблуждение и согласен с поставленными перед ним условиями, и готов приступит к выполнению действии диктуемые преступником, примером того является, внесение предоплаты лицом введенное в заблуждение. В этой связи следует выделить две формы завладения предметом посягательства:

– ввод регистрационных данных кредитных карт;

– перевод «электронной наличности»,

первый рассматриваемый способ, используется при «фишинге»[3], где «фишеры» ставят перед собой цель именно завладеть регистрационными данными

---

[1] Чекунов И.Г. Квалификация мошенничеств, связанных с блокированием программного обеспечения компьютеров пользователей сети Интернет // Российский следователь. – 2012. – №5. С. 31-32.

[2] Семенов Г.В. Криминалистическая классификация способов совершения мошенничества в системе сотовой связи // ИНФОРМОСТ–Средства связи. М., 2011. №3 (16). С. 37-45.

[3] Фи́шинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

кредитных карт. Второй способ, при переводе электронных денег («Qiwi-кошелек», Яндекс-деньги, AdvCash) характерен при схемах с осуществлением предоплаты потерпевшим преступления (например, при продаже несуществующих товаров). На данной стадии совершения преступления, жертва все еще не знает истинных целей киберпреступника, и не догадывается что в отношении него совершается мошенничество в сфере компьютерной информации.[1]

Ученые-криминалисты отмечают тот факт, что отличительной особенностью интернет-мошенничества является то обстоятельство, что при нем остается мало-следов, и потерпевшие не знают преступников в лицо, по сравнению с «традиционным мошенничеством», при котором возможность выявления и идентификации личности мошенника в разы выше.

Таким образом, мошенничество в сфере компьютерной информации, предусматривает для реализации преступного замысла, путем его обмана и введения в заблуждение, необходимость постоянного воздействия на лицо через компьютерную сеть-Интернет. Для этого преступнику необходимо постоянное воздействие на компьютерные средства потерпевшего.

Воздействие во временном измерении зависит от нескольких факторов: во-первых, в зависимости от длительности времени как входа, так и выхода из сети-Интернет; во-вторых, опытности лица (будущей жертвы) в оказываемых услугах интернет магазинами, оплаты товара и услуг (наличие умении пользования интернет магазинами); в-третьих, наличие у жертвы электронных платежных средств (пластиковых электронных карт; онлайн электронных кошельков платежной системы). Кроме того, возможности киберпреступника введения в заблуждение и обман будут ограничены, в случае информирования потерпевшего об аналогичных преступлениях, совершенных в отношении его близких, от правоохранительных органов, либо с интернет сайтов.

На практике так же известны и такие способы воздействия, при котором

[1] Згадзай О.Э., Хафизова Л.С. Финансовая преступность и мошенничество в сети Интернет. Казань. 2006. С. 158.

установление контакта не обязательно. Такой случай зависит от способа и характера преступной деятельности. Во-первых, злоумышленник должен обладать набором компьютерной техники, на которых обеспечен выход в интернет со всех имеющихся устройств, приспособленных для совершения преступления; во-вторых, такой способ обеспечивается доступом в компьютерные устройства потерпевших без их вмешательства, поскольку программы, атакующие проникают в персональный компьютер и передают (выкачивают) необходимую информацию и отправляют автоматически преступнику. Именно эти обстоятельства позволяют в последующем использовать полученные данные для успешного совершения мошенничества, в отношении потерпевшего. При этом потерпевший не будет информирован, о передаче его компьютерных данных преступнику.

Такое мошенничество осуществляется путем взлома сайтов и DDoS-атаки, которые направлены на вымогательство денег за прекращение атаки, получение информации об обнаруженной уязвимости и ее дальнейшей продажи, выполнение хакерами «заказа конкурентов», шантаж сайта, что в дальнейшем он не будет подвержен атакам.[1]

Следы преступления, также активно скрываются преступниками после совершенного деяния, что вводит в заблуждение правоохранительные органы расследующие преступление. Сокрытие следов преступной деятельности мошенника обеспечивается использованием приспособленных специальных компьютерно-технических средств и сети Интернет.

Данный факт, подчеркивается и А.А. Косынкиным, который отмечает, что киберпреступник, на этапе подготовки к преступлению в сфере высоких технологии, разрабатывает план действии, таким образом, чтобы деяние не стало известно правоохранительным органам и не быть изобличенным.

Активное сопротивление наблюдается со стороны злоумышленника при

---

[1] Шепель В.А. Современные способы мошенничества в сети Интернет // Актуальные проблемы борьбы с преступностью на современном этапе: тез. докл. и сообщ. всерос. науч.-практ. конф. Омск: Омская акад. МВД РФ, 2013. С. 94-97.

раскрытии и расследовании уже выявленных преступлении рассматриваемого вида. Данное обстоятельство приводит к тому, что отдельные обстоятельства остаются не раскрытыми, лица причастные к совершению неустановленными, а причины и условия не выясненными. Такой исход расследования приводит к слабому предупреждению новых, планируемых преступлении схожего характера.[1]

По мнению О.А. Росляковой П.И. Шихова, сокрытие следов преступления может сопровождаться не только традиционными способами (например, дача ложных показании, утаивании, фальсификации документов), так и специальными способами, связанными с компьютерной техникой, и ее программными компонентами:

1) фальсификация и маскировка компьютерных программ, использованные при совершении преступления;
2) маскировка местонахождения при удаленном доступе и последующем получении данных потерпевшего:
   - использование «ремейлеров» («Remailers») – компьютерные устройства с установленными программными компонентами выполняющих функцию перенаправления полученной информации (сообщения) по адресу, указанному отправителем. При этом теряются все возможности выяснения информации об авторе (отправителе) сообщения, программа устроена таким образом, что уничтожаются все данные конечного получателя. В сети-Интернет распространены случаи, когда «ремейлеры» при отправке сообщения подписываются как анонимные пользователи, тем самым скрывают свои данные;
   - использование в программах, созданных для пересылки сообщения, фиктивного или вымышленного электронного адреса отправителя;
   - использование «программ-анонимизаторов», меняющие адреса обратной

[1] Косынкин А.А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования // Российский следователь. – 2012. – №2. С. 2-3.

связи и службу электронной почты злоумышленника. При этом, не теряется возможность правоохранительных органов установить IP-адрес компьютера адресанта.

В настоящее время использование второго электронного почтового адреса, предоставляют множество интернет сайтов, в которых можно умышленно регистрировать любые вымышленные первоначальные данные готовые к свободному использованию в преступных целях;

3) восстановление прежней работоспособности компьютера, которое было до специальной ее подготовки к преступлению;
4) сокрытие присутствия в операционной системе («Rootkit»).

«Rootkit» – программный код или техника, направленная на сокрытие присутствия в системе заданных объектов (процессов, файлов, ключей реестра и т.д.);

5) противодействие расследованию также может выражаться в воздействии на его участников либо уклонении от участия в расследовании.[1]

Указанные обстоятельства могут использоваться злоумышленниками при сокрытии преступлении мошенничества в сфере компьютерной информации и противодействий его расследованию. Такие меры необходимо учитывать при разработке научных положении, практических рекомендации, и соответственно лицу производящим расследование уголовного дела данной категории.

Однако, как показывает следственная и судебная практика, лица совершившие такие преступления и задержанные с поличным, идут на сотрудничество со следствием и заключают досудебное соглашение в 65% изученных уголовных делах.

Таким образом, криминалистические знания о расследовании мошенничества данной категории, источники и их свойства, позволяют создать полную модель механизма совершения мошенничества в сфере компьютерной

[1] Рослякова О.А., Шихов П.И., Расследование преступлений в сфере компьютерной информации и высоких технологий: курс лекций. СПб., 2015. С. 170.

информации. И как отмечает Д.А. Степаненко, следователь, путем логического моделирования основных полученных данных, получает новое выводное знание на основании умозаключения (новую доказательственную базу). Сделанные выводы в своей сущности касаются предмета уголовно-процессуального доказывания, например, они могут определить событие преступления с точки зрения динамических процессов взаимодействия материальных тел-объектов, процесс его возникновения, а также наступившие последствия[1].

Модель механизма преступления, созданная при расследовании преступления, вооружает следователя системным знанием, который способствует эффективному расследованию преступления. В процессе расследования мошенничества в сфере компьютерной информации следователь использует типовую модель преступления и, применяя такие приемы логического мышления, как сравнение и аналогия, сопоставляет полученную информацию с модельной, восполняя при этом недостающие ее звенья за счет выведенных зависимостей между преступной деятельностью субъекта, совокупностью действий, поступков жертвы преступления и лиц, оказавшихся косвенно связанных с преступным событием, а также отдельными элементами обстановки, используемой участниками преступного события.

[1] Степаненко Д.А. Моделирование как метод научного исследования в приложении к решению задач уголовного судопроизводства (некоторые актуальные проблемы): дис. … канд. юрид. наук: 12.00.09 / Д.А. Степаненко. Иркутск,2013. С. 76;

ГЛАВА 2. ОСОБЕННОСТИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Особенности производства отдельных следственных действии при расследовании мошенничества в сфере компьютерной информации

Следственные действия являются общими и универсальными средствами получения доказательств, которые оказывают содействие в расследовании преступлении. Производство следственного действия обусловлено, необходимостью получения информации об обстоятельствах преступного события, которые составляют предмет доказывания.

Расследование мошенничеств в сфере компьютерной информации, в аспекте поисково-познавательной деятельности следователя требует понимания следующих категории понятии «компьютерная информация», «кибернетическое пространство», «виртуальный след».[1]

Под «компьютерной информацией» мы понимаем информацию, представленную в специальном (машинном) виде, предназначенном и пригодном для ее автоматизированной обработки, хранения и передачи, находящуюся на материальном носителе и имеющую собственника или иного законного владельца, установившего порядок ее создания (генерации), обработки, передачи и уничтожения.

«Кибернетическое пространство» при расследовании рассматриваемого вида мошенничества – следует понимать как область нахождения информации, который предусматривает автоматизированную обработку, имеющий существенное значение для расследуемого дела, дающую возможность установления истины по делу, образованная средствами электронно-вычислительной техники, управление которыми осуществлялось через

[1] Степаненко Д.А. К вопросу о поисково-познавательном «инструментарии» следователя // Российское правосудие. – 2012. – №7 (75). С. 98.

конкретное программное обеспечение.

«Виртуальный след» – любое изменение состояния автоматизированной информационной системы (образованного ею «кибернетического пространства»), связанное с событием преступления и зафиксированное в виде компьютерной информации (т.е. информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе и на электромагнитном поле.[1]

Расследование массива уголовных дел мошенничества в сфере компьютерной информации, предусматривает необходимость производства следственных и иных процессуальных действии, предусмотренных и регламентированных уголовно-процессуальным кодексом.

Анализ и репрезентативный опрос сотрудников правоохранительных органов, расследующих мошенничество в сфере компьютерной информации, дает основание сделать неутешительные выводы: отсутствие специального познания компьютерной техники, служит помехой достаточно точно сформировать базу доказательственной информации, что в свою очередь приводит к трудностям квалификации и расследования, рассматриваемых категории уголовных дел. Исключение составляют сотрудники Управления отдела «К» МВД России, которые специализируются по борьбе с преступлениями в сфере информационных технологии, так как их специфика включает в себя знание как технической части компьютерной системы, так и юридическую сторону расследования данных видов преступлении.

Изучив материалы уголовных дел, мы пришли к выводу, что наиболее часто на практике проводятся следующие следственные действия:

- ОМП, осмотр предметов и документов (100% уголовных дел);
- допрос лиц, с конкретным процессуальным положением определенных уголовно-процессуальным законом (100% уголовных дел);
- назначение и производство судебных экспертиз (100% уголовных дел). В

[1] Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра. юрид. наук: 12.00.09 / В.А. Мещеряков. Воронеж, 2012. С. 15, 21.

100% случаев назначалась компьютерная экспертиза; в 60% – дактилоскопическая экспертиза; в 55% случаев – технико-криминалистическая экспертиза документов; 25% – трасологическая экспертиза; в 10% – психологическая экспертиза; в 5% случаев – иные;

- получение образцов для сравнительного исследования (80% уголовных дел);
- предъявление для опознания (25% уголовных дел);
- обыск и выемка (90% уголовных дел);
- очная ставка (85% уголовных дел);
- следственный эксперимент и проверка показаний на месте (65% уголовных дел);
- снятие информации с технических каналов связи (25% уголовных дел);
- прослушивание телефонных и иных переговоров (5% уголовных дел) и др.[1]

Выбор тактико-криминалистических методов производства следственных действии, при расследовании уголовных дел связанных с мошенничеством в сфере компьютерной информации связано с особенностями механизма преступления. Е.С. Шевченко, подчеркивает, что «при производстве вербальных следственных действии, следует учитывать следующие особенности:

- целесообразность привлечения специалистов обладающими знаниями в области телекоммуникационных систем и компьютерной техники;
- интеллектуальном противодействии преступлению (учитывать возможности продолжения преступной деятельности злоумышленником, имеющим доступ к компьютерным программам настроенных под совершение преступления);
- содержании предмета допроса (осведомленность о функциях преступных

[1] [Электронный ресурс]. URL: https://мвд.рф/mvd/structure1/Centri/JEkspertno_kriminalisticheskij_centr (дата обращения: 17.12.2017).

компьютерных программах обнаруженной на конкретном носителе);

- в ограниченности времени и мгновенном изменении обстановки в киберпространстве;
- возможностях использования отдаленно сети Интернет.

Особенности производства невербальных следственных действий включает:

- необходимость последовательного и логичного построения при использовании профессиональных знании и умении информационно-следовой картины преступления;
- применение специальных технико-криминалистических средств»[1]

Среди распространенных вербальных следственных действии немаловажное место занимает *допрос.*

В теории криминалистики давно уже определено понятие допроса. Так, Р.С. Белкин определял допрос как процессуальное (следственное или судебное) действие, заключающееся в получении показаний (информации) о событии, ставшем предметом уголовного судопроизводства, лицах, проходящих по делу, причинах и условиях, способствовавших совершению и сокрытию преступления.[2]

Исходя из специфики мошенничества в сфере компьютерной информации, и содержание механизма противоправного деяния стоит учитывать, что их установление зависит от применения для его реализации специальных орудий и средств – компьютеров, техники к ним, накопителей информации, компьютерных сетей и др.

Выше перечисленные обстоятельства обуславливают, производство допроса с привлечением специалиста в сфере компьютерных технологии. Бесспорным является тот факт, что вопрос о привлечении специалиста остается за следователем. Кроме того, смело можно отметить, на практике встречаются

---

[1] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. …канд. юрид. наук: 12.00.12 / Е.С. Шевченко. М., 2012. С. 10-11.

[2] Белкин Р.С. Криминалистическая энциклопедия. М.: Мегатрон XXI, 2000. С. 62.

случаи, привлечение специалиста может сказаться на качестве достижения поставленного результата. Такой случай связан с отрицательным влиянием присутствия третьих лиц, на установление психологического контакта между следователем и допрашиваемым лицом. Допрос следователем лица с определенным процессуальным положением в качестве подозреваемого или обвиняемого в отдельных случаях давало повод для оказания противодействия расследованию со стороны допрашиваемых лиц. Данный случай связан с тем, что у лица дающего показание складывается убеждение о отсутствии достаточных знании об особенностях совершения преступления, специфике расследования мошенничества в сфере компьютерных информации и некомпетентности следователя в расследовании уголовного дела.

Опрос практических сотрудников следственных органов, участвовавших в данном следственном действии, связанном с преступлением предусмотренным статьей 159.6 УК РФ, отметили что привлечение специалиста дает возможность получить всю исчерпывающую информацию о механизме преступления, доказательственного значения, что оказывает влияние на допрашиваемое лицо. Таким образом, у него отпадает желание в дальнейшем обмануть правоохранительные органы и ввести расследование дела в безвыходное положение.

В другом случае, сотрудники, участвовавшие в опросе отмечали, привлечение специалиста на следственное действие допрос подозреваемого (обвиняемого) негативно сказывалось на результат получения информации о преступлении. В этот момент злоумышленник на основании глубоких знании системы компьютерных технологии и консультационный характер действии следователя, старался давать ложные показания, отрицать совершение преступления, оказывал противодействие расследованию, инкриминируемого ему деяния, что способствовало потере имеющих значение для расследования сведении.

Изложенное свидетельствует о том, что перед проведением допроса, должна предшествовать подготовительная работа к следственному действию, в

которой должно быть установлено отношение подозреваемого (обвиняемого) к расследуемому событию, его характеризующий личность материал, а также тщательно изучены особенности средств и методов использованных преступником для совершения преступления, и именно на подготовительном этапе следователю необходимо активно использовать помощь специалиста.[1]

Приведем следующий пример, подозреваемая в совершении преступления предусмотренного статьей 159.6 УК РФ, гр-ка И., в ходе допроса пояснила, что она не могла совершить мошенничество в сфере компьютерной информации ввиду отсутствия доступа к данной информации. В ходе личной консультации следователя со специалистом данной сферы, были установлены обстоятельства о рабочей деятельности И., которые давали доступ к данной информации и способствовали совершению преступления только гр-ой И. В ходе повторного допроса, гр-ка И., в вопросно-ответной форме призналась в совершении данного преступления, после предъявления железных доказательств о ее виновности.[2]

В ходе подготовки к следственному действию допроса подозреваемого (обвиняемого) следователю следует обратиться к документам полученные до возбуждения уголовного дела (доследственной проверки). Как отмечает Н.Г.Шурухнов: «…Первоначальный допрос во время следствия, по возбужденному уголовному делу, будет являться подтверждением объяснений изложенным до возбуждения мошенничества в сфере компьютерной информации. … Данное мероприятие играет немаловажную роль в получении интересующим следствие информации, так как создает благоприятный исход допроса подозреваемого (обвиняемого) на предварительном следствии. Что касается лиц, дающие ложные показания, то первоначальное их объяснение даст следователю понять, какую позицию хочет занять во время допроса

---

[1] Егоров Н.Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспекты. М.: Юрлитинформ, 2017. С. 197.

[2] Уголовное дело №00234-12 // Архив судебного участка №2 Авиастроительного района г. Казани.

недобросовестный участник следственного действия».[1]

Следует учитывать, что допрос потерпевших и свидетелей по уголовным делам о мошенничестве в сфере компьютерной информации будет отличаться от допроса подозреваемых и обвиняемых, а особенности, связанные с механизмом преступления, будут влиять на выбор тактических приемов допроса.

Необходимо отметить, также, что при допросе потерпевших и свидетелей, выяснению подлежит следующая информация:

- какие конкретно компьютеры, программное обеспечение использовались потерпевшим при работе, на компьютере на который осуществлял посягательство злоумышленник;
- наличие умении и знании у жертвы о программном обеспечении навыков их использования, а также знание характеристик компьютерного устройства;
- наличие программного обеспечения, установленного на компьютер на который посягал преступник;
- оператор (провайдер) оказывающий услуги связи, который подключен к компьютеру, на который посягал преступник;
- через какое время и как узнал потерпевший о том, что стал жертвой мошенничества в сфере компьютерной информации;
- каким образом осуществлялся контакт между допрашиваемым лицом и злоумышленником, если оно имеет место;
- был ли визуальный контакт (в каких условиях, например, видео-звонок через программное средство Skype, либо общение через социальную сеть путем сообщения) между потерпевшим и преступником, сможет ли он его опознать.

Такое следственное действие как *осмотр места происшествия* по преступлениям в сфере компьютерной информации занимает особое место, так

[1] Шурухнов Н.Г. Использование при допросе ранее данных объяснений // Тактические приемы допроса и пределы их использования. М., 2013. С. 50-53.

как особенности его производства следует учитывать при расследовании преступления предусмотренного статьей 159.6 УК РФ.

Осмотр места происшествия, также, как и обыск, выемка, следственный эксперимент относятся к группе невербальных следственных действий. Указанные следственные действия позволяют дознавателю, следователю сформировать мысленный образ материальных объектов, основанный на чувственном образе, не выраженном в вербальной форме. Данная форма информации об значимых сохраненных следах, оставленных на объекте заключается в получении объективных знании лицом ведущим расследование уголовного дела. Как вербальный так и невербальный способ познания имеет большое значение для установления исчерпывающих обстоятельств, входящих в предмет уголовно-процессуального познания.[1]

Во время осмотра места происшествия следователь фиксирует обстановку, следы оставленные преступником, иные фактические данные позволяющие сделать вывод о механизме преступления, что способствует установлению преступника.

В состав объектов следственного осмотра кибернетического пространства, по мнению В.А. Мещерякова, должны быть включены:

- отдельные помещения либо их совокупность в которых расположены компьютерные системы, включая их техническое обеспечение деятельности (электропитание, телекоммуникационная связь и т.п);
- каналы Интернет связи служащие линией для передачи и получения данных (в том числе звуковые волны и электромагнитные поля);
- объекты носителей информации, служащие для обработки, хранения в пригодном состоянии для восприятия компьютерными технологиями;
- непосредственно сама информация (данные с компьютерных носителей информации);
- принятый системный порядок и определенная последовательность

[1] Россинский С.Б. Результаты «невербальных» следственных и судебных действий как вид доказательств по уголовному делу. М.: Юрлитинформ, 2015. – 224 с.

обработки информации на техническом устройстве.

При осмотре места преступления, следователю также следует помнить особенности совершения преступления в «кибернетическом пространстве». К ним следует отнести:

- быстрое изменение состояния, при их огромном количестве;
- отсутствие четких форм проявления исправлении, и недолговечность информационных следов преступления в программном обеспечении компьютера;
- отсутствие идентификационных признаков передаваемого объекта по «кибернетическому пространству»;
- использование специальных программ приспособленных для определенной обработки, имеющихся только у злоумышленника.[1]

Производство осмотра места происшествия по делам о мошенничестве в сфере компьютерной информации преследует своей целью выявление:

- компьютерных следов, а также объектов на которых они могут находиться (например: системный блок, флеш-карта с USB входом и т.п)
- следов оставляемых конкретным лицом, находящимся на месте происшествия (традиционных следов);
- особенности и виды сетей, устройств принципы их функционирования посредством которых совершено мошенничество в сфере компьютерной информации;
- имеющиеся устройства –аудио, –видео фиксации на прилегающей территории, на месте происшествия, а также непосредственно (при наличии) на самом компьютере.

При выявлении следов указывающих на копирование, блокирование, модификацию информации со стороны злоумышленника, то есть направленных на изменение свойств компьютерной информации, обязательному осмотру

[1] Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. …д-ра юрид. наук: 12.00.09 / В.А. Мещеряков. Воронеж, 2001. С. 15-16.

подвергнется как компьютерно-технические устройства, так и их содержание осматриваемое в рамках детального осмотра. При этом, М.Ш. Махтеев, отмечает обязательное приобщение к протоколу осмотра всех необходимых физических характеристик файла (каталога), включая его размещение на машинном носителе, путем распечатки этих данных.[1] В данном случае представляется, что следователю необходимо обладать специальными знаниями (либо привлечь специалиста) для обнаружения файлов содержащих криминалистически значимую информацию. В некоторых случаях на практике встречаются случаи необходимости осмотра не одного технического устройства, а значительного их количества.

Кроме этого, преступники могут использовать различного рода программное обеспечение и средства к ним, которые выполняют функцию по сокрытию следов, которые при попытке обнаружения и изъятия влекут полное ее уничтожение.

В ходе осмотра места происшествия при обнаружении компьютерно-технических средств рекомендуется производить их детальный осмотр, т.к. они могли использоваться в качестве орудии и средств совершения мошенничества в сфере компьютерной информации, установление их особенностей и отличительных признаков. После чего производится изъятие и их упаковка с соблюдением установленных правил с целью последующего тщательного осмотра в кабинете следователя с обязательным привлечением специалиста обладающего знаниями в области компьютерной техники и ее программ.

На практике встречаются случаи, когда на компьютер установлены специальные программы выполняющие функцию защиты вредоносной программы, которые в автоматическом режиме при производстве следственного действия приступают к очистке всей базы вредоносных программ на компьютере, для того чтоб остановить данный казус следователю либо специалисту, необходимо ввести специальный код, при этом целесообразно,

[1] Махтеев М.Ш. Методика расследования компьютерных преступлений: учеб. пособие. М.: РосНОУ, 2017. С. 103.

чтоб преступник выдал данные пароли добровольно, что способствует быстрой остановки функционированию вредоносных программ, что существенно снижает риск дальнейшего нанесения ущерба. В данном случае после данной операции специалист может приступать к копированию имеющей значение для расследования информацию. В противном случае, несвоевременный ввод запрашиваемого кода может привести к потере необходимой для расследования информации.

Согласно действующему законодательству Российской Федерации, по уголовным делам изъятию подлежит та информация, которая имеет отношение к мошенничеству в сфере компьютерной информации, представляется что следователь самостоятельно должен определить ее содержание и скопировать их. Однако при невозможности изъять указанную выше информацию на месте, по причине отсутствия доступа к программному обеспечению компьютера (например, неизвестен пароль, либо в связи со значительным объемом информации) следует изъять компьютер целиком, либо системный блок в отдельности.[1]

При случае изъятия целого компьютера либо системного блока, важно соблюсти целостность значимой для уголовного дела информации, т.е. сохранить в полном первоначальном виде всю информацию. Справедливо заметить, данное требование, возможно, выполнить путем привлечения специалиста, для гарантированного сохранения компьютерной информации.[2]

Случаи применения специальных защитных паролей, как указывают респонденты составляют 75% от всего количества уголовных дел мошенничества в сфере компьютерной информации, из них 97% случаев совершены субъектами преступной деятельности, в составе группы лиц, в том числе организованными группами, также использовались такие приемы в своей

---

[1] Методика расследования налоговых преступлений: учеб. пособие / под общ. ред. А.А. Кузнецова. М.: ЦОКР МВД России, 2017. С. 49.

[2] Протасевич А.А., Зверянская Л.П. Проблемы собирания и оценки компьютерной информации как доказательства // Современная криминалистика: проблемы, тенденции, имена (к 90-летию профессора Р.С. Белкина): сб. материалов 53-х криминалистических чтений: в 3 ч. М.: Академия управления МВД России, 2012. Ч. 3. С. 274.

деятельности.

Выяснение таких точностей как:

- какие операционные системы установлены на каждый отдельный компьютер;
- какое программное обеспечение используется;
- имеются ли отдельные резервные копии оригинальных документов используемых на компьютерах;
- пароли администраторов системы;
- при наличии имена паролей пользователей;
- установленные на компьютер программы защиты и шифрования,

все эти обстоятельства требуют выявления конкретного администратора системы и его обязательный допрос.[1]

Во всех случаях осмотра места происшествия, следователю необходимо учитывать время, прошедшее от момента совершения преступления, до момента осмотра компьютерно-технических средств. Данное положение обусловлено тем, что на практике встречаются случаи, с момента посягательства на компьютер до момента проведения следственных действии проходит значительный промежуток времени, в этот период пользователь, не понимая, что компьютер подвергся преступным действиям со стороны мошенника, начинает перезагружать неоднократно персональный компьютер, скидывать настройки до первоначального состояния, соответственно все это ведет к потере «информационных» следов о преступном посягательстве.[2]

Таким образом, осмотр места происшествия по уголовным делам о мошенничестве в сфере компьютерной информации в значительной степени направлен на выявление криминалистически значимой информации, свидетельствующей о механизме преступления, совершенном конкретным способом,

---

[1] Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / под ред. Ю.В. Гаврилина. М.: ЮИ МВД РФ, 2013. С. 147.

[2] Вражнов А.С. Криминалистический риск при расследовании неправомерного доступа к компьютерной информации: автореферат дис. ... кандидата юридических наук: 12.00.12 / А.С. Вражнов. М., 2015. С. 22.

последовательности определенных действий, субъектов преступной деятельности, об установлении соответствия уже полученной информации выдвинутым версиям. Кроме того, с помощью осмотра выявляются и фиксируются следы, указывающие на причастность к совершенному деянию конкретного лица, изымаются компьютерно-технические средства, имеющие отношение к исследуемому виду мошенничества. Это предопределяет выбор следователем способа, метода и содержания осмотра места происшествия. «Высокая эффективность проведения осмотра места преступления по данному виду правонарушений достигается благодаря усилиям его участников и сопутствующим факторам:

- высокой квалификации следователя и его осведомлённости об основных способах и механизмах совершения киберпреступлений;
- своевременному привлечению к осмотру компетентных специалистов;
- квалифицированному применению технико-криминалистических средств;
- оперативности прибытия следователя на место происшествия;
- неукоснительному соблюдению процессуальных требований и криминалистических рекомендаций в обращении с вещественными доказательствами.

Осмотр места происшествия по киберпреступлениям часто требует от специалистов ситуативной формы организации знаний, и прежде всего – от следователя»[1]

При проведении любого следственного действия, в особенности в результате проведения допроса, следователь получает информацию о точном или предполагаемом местонахождении объектов (предметов) имеющих доказательственное значение для уголовного дела. При получении такой информации, с целью отыскания предметов, о местонахождении которых стало известно из показании полученных при допросе, необходимо произвести такие

[1] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. …канд. юрид. наук: 12.00.12 / Е.С. Шевченко. М., 2012. С. 23-24.

следственные действия как *обыск* или *выемка.*

Производство обыска и выемки может носить неотложный характер, обыск может носить поисковый характер искомого объекта, а выемка производится по результатам определения точного местонахождения предметов. Перед производством таких следственных действий, для облегчения достижения поставленных задач перед следователем, предлагается выдать предметы добровольно. Довольно часто встречаются случаи, когда производство обыска носит неотложный характер, соответственно его производство по указанной категории мошенничества целесообразно проводить незамедлительно, после возбуждения уголовного дела, поскольку обнаружение доказательственной информации по мошенничеству в сфере компьютерной информации способствует оперативному установлению местонахождения злоумышленника.[1]

О данном факте свидетельствует анализированные материалы уголовных дел, примерно 60% случаев следователем были изъяты доказательственные материалы (это компьютерные устройства, их программное обеспечение, носители информации в виде флеш-карт и жестких дисков, смартфоны(телефоны), печати юр. лиц и т.п.), а также документы носящие информацию о причастности конкретных лиц к совершенному мошенничеству в сфере компьютерной информации (записные книжки, распечатанные листы бумаг с изображением банковских карт и его реквизитов, пароли используемые как на компьютере так и в социальных сетях записанные на листы бумаг, бланки документов и т.п.). В 40% случаев в ходе обыска была изъята информация, косвенно указывающая на причастность лица к совершенному преступлению. В данном случае речь идет об ориентирующей информации, содержащаяся в учебной и научной литературе, в которой рассматривались вопросы функционирования локальных сетей, сети Интернет, разработки

[1] Мещеряков В.А. «Виртуальные следы» под «скальпелем Оккама» / Информационная безопасность. Саратов: ГОУВПО «Саратовский юридический институт МВД России. 2016. №1(4). С. 29.

злокачественного оборудования, программно-технических средств, способствующих локальному проникновению на компьютер потерпевшего.

Как показывает практика, во время обыска и выемки необходимо также изымать носители информации, на которых может храниться программное обеспечение и документы указывающие на виновность лица. Такими носителями могут быть USB флеш-накопители, накопители на жестких магнитных дисках, компактные диски (CD-R, CD-RW) иные источники информации и т.п. Такие объекты могут содержать переписку соучастников преступления, похищенные программы официальных версии выпущенных компанией либо их фрагменты, а также на нем могут находиться сами вирусные программы.

Следует признать, что в процессе изъятия информации с электронных носителей следователи сталкиваются с различными значительными трудностями, в основном проблемы возникали с тем, что после изъятия терялась возможность продолжения своей хозяйственной деятельности организациями, компаниями и предпринимателями.

Такое обстоятельство приводило к росту подачи жалоб в государственные ведомства на адрес субъектов, расследующих уголовное дело. В этой связи законодатель определил порядок работы с данными объектами. Так, при производстве обыска и выемки (ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ)[1] изъятие электронных носителей информации производится с участием специалиста. По ходатайству законного владельца изымаемой информации, специалистом может производиться копирование на электронный носитель данной информации в присутствии понятых, оставляя оригинал у владельца, что безусловно способствует продолжению хозяйственной деятельности субъектом у которого изымается данная информация. При копировании специалистом следует учитывать, что данная операция позволяет скопировать

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ// Собрание законодательства Российской Федерации от 24 декабря 2001 г. №52 (часть I) ст. 4921.

искомую информацию без потери ее какой-либо части, представляющий интерес для расследования преступления. В случае невозможности копирования электронной информации целиком, следователю необходимо отклонить ходатайство, учитывая позицию специалиста в области компьютерно-технических средств.[1]

Таким образом, производство следственных и иных процессуальных действий по уголовным делам о мошенничестве в сфере компьютерной информации имеет определенные особенности, которые в полной мере обусловлены механизмом преступной деятельности, а также субъектами его совершившими. Для достижения положительного результата и цели производимого следственного действия следователю необходимо тщательно готовиться к его производству, используя многообразные тактические приемы и помощь специалистов.

§2. Возможности использования компьютерно-технической экспертизы в расследовании мошенничества в сфере компьютерной информации

Необходимо отметить, что данный вид мошенничества обладает своей спецификой, для сбора доказательственной базы необходимо произвести большое количество судебных экспертиз, отдельные из которых присуще только данной категории уголовных дел. Как отмечалось ранее, что для расследования мошенничества в сфере компьютерной информации необходимо использовать специальные знания не только при проведении экспертизы, но и для сбора информации, то есть при проведении следственных действии (осмотре, обыске, выемке) для поиска, обнаружения и изъятия носителей

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

информации необходимые для производства экспертизы. Один из видов экспертиз проводимой по данным категориям уголовных дел является судебные компьютерные экспертизы (СКЭ), которая в настоящее время в теории делятся на следующие разновидности:

– аппаратно-компьютерная экспертиза;

– программно-компьютерная экспертиза;

– информационно-компьютерная экспертиза;

– компьютерно-сетевая экспертиза,

поэтому результаты экспертизы наряду с процессуальными и следственными действиями обладают значительным объемом информации.

Поэтому целесообразно поделить указанные виды экспертиз по задачам ими выполняемые на идентификационные и диагностические. Они зависят от объектов, представленных на исследование. Например, к идентификационным задачам аппаратно-технической экспертизы относится установление групповой принадлежности и сопоставление конкретных аппаратных средств между собой по общим и частным признакам. Диагностические задачи шире, и предусматривает решение следующих задач при его производстве, это определение видов и свойств аппаратных средств, их технические и функциональные характеристики, а также определение исправности технических средств и т.п.

При решении вопроса идентификационного характера программно-компьютерная экспертиза устанавливает тождество используемых программ в компьютере лицензионным версиям (официальная версия выпускаемых продуктов программного характера). К диагностическим задачам следует отнести, данного вида экспертизы как определение основных характеристик операционной системы, исследование функциональных настроек и свойств программного обеспечения, а также решение вопроса о фактическом установлении и изменении данных программ.

При производстве информационно-компьютерной экспертизы в ходе идентификационных задач отождествляются содержание файлов с данными

файлов, а также документов исходными компонентами которых являются данные программы компьютера, кроме этого устанавливается источник происхождения информации предоставленной на материальном носителе информации. При решении диагностических задач устанавливается свойство, характеристика, какое первоначальное состояние было у информации предоставленной на исследование на технических устройствах.

Несколько иные возможности компьютерно-сетевой экспертизы, в ходе которой можно определить свойства и характеристики аппаратных средств и программного обеспечения, установить место и роль, а также функциональное назначение исследуемого объекта в сети. Также можно выявить свойства и характеристики вычислительных сетей, установить их архитектуру, различные конфигурации, установить сетевые компоненты и порядок организации доступа к данным исследуемой сети.

Таким образом, к задачам идентификационного характера относится установление тождества исследуемого объекта его признакам, которые отобразились в материальной среде. К диагностическим задачам можно отнести решение вопроса об установлении различных свойств и характеристик исследуемых объектов.

Как справедливо отмечают Т.В. Аверьянова и В.Ф. Статкус, вопросы выносимые на экспертизу должны отвечать на ряд требовании. Такие требования, по мнению указанных авторов, можно разделить, на две группы:

1. Общие требования:

а) при постановке вопроса следователем необходимо исключить жаргонные и полупрофессиональные термины (такие как: «винчестер», «взлом» и т.д.) следует использовать только профессиональные термины. В случае отсутствия законодательного регулирования данного понятия, необходимо использовать понятийный аппарат употребляемые разработчиками программного средства в документациях, описаниях, справках к программно-техническим средствам;

б) вопрос должен быть выражен в четкой и однозначной формулировке;

в) формулировка вопроса не должна касаться этапов исследования информации (описание характеристик носителей информации и особенностей размещения информации на них, восстановление и исследование информации среди удаленных файлов, являются обязательным этапом исследования информации);

г) поставленные вопросы не должны содержать в себе справочный характер;

д) вопросы, поставленные перед экспертом не должны выходить за пределы его компетенции;

е) вопросы, поставленные перед экспертом, должны соответствовать методической и технической базе.

2. Частные требования:

а) вопросы должны содержать в себе требования, направленные на установление конкретных обстоятельств совершенного преступления;

б) вопросы, поставленные перед экспертом должны носить минимальные затраты (финансовые, технические, временные и пр.) при проведении назначенного исследования;

в) вопросы должны носить соответствующий характер уровню подготовки и техническому оснащению экспертного учреждения, которому назначается экспертиза;

г) вопросы не должны выходить за пределы предоставляемых вещественных доказательств.[1]

Выше мы указали, что экспертному исследованию могут быть подвергнуты разные средства компьютерной техники, программное обеспечение и собственно сама компьютерная информация. Поэтому логично вопрос об объекте и предмете СКЭ рассматривать в отношении отдельных её видов.

---

[1] Практическое руководство по производству судебных экспертиз для экспертов и специалистов: науч.-практич. пособие / под ред. Т.В. Аверьяновой, В.Ф. Статкуса. – М.: Издательство Юрайт, 2011. С.518-519.

Так, объектом аппаратно-компьютерной экспертизы (АКЭ) являются аппаратные объекты: персональные компьютеры, периферийные устройства, сетевые аппаратные средства, интегрированные системы (органайзеры, пейджеры, мобильные телефоны…), встроенные системы на основе микропроцессоров (иммобилайзеры, транспондеры…), комплектующие этих средств. Предметом этой экспертизы – закономерности эксплуатации аппаратных средств компьютерной системы как материальных носителей информации о факте или событии уголовного дела[1]

Объектом ПКЭ (программно-компьютерной экспертизы) будут являться программное обеспечение персонального компьютера (непосредственно операционная система установленная на компьютер) программы используемые в преступных целях, средства разработки и изменения официальных программ используемых в последующем для совершения преступления, текстовые и графические приложения установленные на компьютерно-технические средства и т.п. Предмет ПКЭ – способы разработки и применения программного обеспечения компьютера; установление функционального предназначения, характеристик и реализуемых требований, алгоритма и структурных особенностей, текущего состояния программного средства компьютерной системы[2]

Информационно-компьютерная экспертиза (ИКЭ). Объектом данного вида экспертизы являются документы, носящие в себе графическую и текстовую информацию, изготовленных при помощи компьютерных программ и средств; данные в формате мультимедиа; информация, носящая прикладной характер, без данных приложении. Предмет ИКЭ – поиск, обнаружение, системный анализ информации созданной человеком при помощи специальных программ для организации информационных процессов в компьютерной системе.

---

[1] Васильев А.А. Судебная аппаратно-компьютерная экспертиза. Правовые, организационные и методические аспекты: дис. ... канд. юрид. наук: 12.00.09 / А.А. Васильев. М., 2013

[2] Семикаленова А.И. Судебная программно-компьютерная экспертиза по уголовным делам: дис. … канд. юрид. наук: 12.00.09 / А.И. Семикаленова. М., 2015 г.

Компьютерно – сетевая экспертиза (КСЭ). Объектом данного вида экспертизы является компьютерно – технические средства, подключенные к сети Интернет, сервисы поставщиков услуг Интернет (провайдеры), используемые Интернет сайты (электронная почта, телеконференции и т.д.). Предмет КСЭ – установление факта подключения к телекоммуникационным сетям компьютерных технологии.[1]

Рост эффективности при расследовании преступлении правоохранительными органами во многом зависит от специализации профессионалов по не исследованным отраслям знании, а именно в сфере компьютерных технологии. В настоящее время экспертные подразделения специализирующихся на проведении компьютерных экспертиз испытывают нехватку специалистов в данной области, изучение языка программирования исходного кода, а также в сфере сетевого взаимодействия. Необходимо подчеркнуть тот факт, что в мире происходит образование новых профессии в сфере программирования, а в правоохранительной деятельности данный факт не состоялся, что влечет за собой отсутствие такого рода специалистов в правоохранительной сфере.[2]

Как показывает практика на сегодняшний день в МВД России и в Министерстве Юстиции России проводятся большинство перечисленных видов компьютерных экспертиз. Данные виды экспертиз проводились по разным категориям уголовных дел, где компьютерно-технические средства выступали как в качестве орудий, так и средств совершения преступления (в их число, безусловно, входили преступления в сфере компьютерной информации). В рамках изучения уголовных дел, был выявлен тот факт, что в каждом уголовном деле о мошенничестве в сфере компьютерной информации, было вынесено постановление о назначении компьютерной экспертизы. В некоторых

---

[1] Моисеева Т.Ф. Основы судебно-экспертной деятельности: конспект лекций. М.: РГУП, 2016. С. 138-141.

[2] Степаненко Д.А. «Адаптивная модификация» криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности // Российский следователь. – 2015. – №15. С. 20.

случаях, в рамках одного уголовного дела, имеет место назначение не одного, а нескольких экспертиз. Специалисты производящие экспертизы по делам о мошенничестве в сфере компьютерной информации не всегда являются сотрудниками государственных экспертных учреждений, они могут быть сотрудниками соответствующих организации, преподавателями учебных заведении, специализация которых связана с ЭВМ, данные лица участвуют в уголовном процессе в качестве эксперта для решения задач следствия и суда. Следует учитывать, тот факт, что их квалификация может быть известна не только лицам, ведущим расследование уголовного дела, но и преступникам, которые могут прибегнуть к их консультациям, взаимопомощи, при получении данного вида информации, такой факт автоматически является основанием для отвода эксперта (ст. 16 ФЗ «О государственной судебно-экспертной деятельности в РФ»[1], ст. 70 УПК РФ[2]).

Одним из основных форм использования специальных знании в расследовании преступлении является назначение и производство различных видов экспертиз по мошенничествам в сфере компьютерной информации, основной задачей которых является определение механизма содеянного противоправного деяния, последовательность определенных действии, обнаружение следов, оставленных в киберпространстве, установление и изобличение конкретного злоумышленника.

Ряд ученых, считает, что основным видом проводимых компьютерных экспертиз, является судебная информационно-компьютерная экспертиза (ИКЭ), так, как только она позволяет разрешить диагностические и идентификационные задачи, построить целостную картину преступления

---

[1] Федеральный закон "О государственной судебно-экспертной деятельности в Российской Федерации" N 73-ФЗ от 31.05.2001 г.// Собрание законодательства РФ от 4 июня 2001 г. №23 Ст. 2291.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ// Собрание законодательства Российской Федерации от 24 декабря 2001 г. №52 (часть I) ст. 4921.

связанной с компьютерной информацией.[1]

По нашему мнению, выбор одного вида экспертизы в качестве исключительной по мошенничеству в сфере компьютерной информации, было бы не правильным. Каждая судебная экспертиза, решает свои определенные задачи, входящий в предмет той или иной экспертизы. При этом назначение определенного вида экспертизы определяется наличием объектов, изъятых с места происшествия, носящие в себе сведения о информационных следах, а также конкретной следственной ситуацией.

В коллективной монографии «Судебная экспертиза: типичные ошибки» определены принципы, разработанные Международной организацией по компьютерным доказательствам, и которыми следует руководствоваться при поиске, обнаружении, фиксации, изъятии, исследовании и хранении цифровых доказательств:

1) при проведении работ с информационной (цифровой) доказательственной базой должны соблюдаться все процессуальные и общие судебные положения;
2) при изъятии доказательств с компьютерной техники, действия должны быть построены таким образом, чтоб они не изменяли свойство цифровой базы доказательств;
3) лицо получающее доступ к оригинальному (исходному) доказательству, должно иметь специальную соответствующую подготовку;
4) вся изъятая цифровая информация должна быть соответствующе запакована для ее дальнейшего хранения, и полностью в правильной форме задокументирована;
5) лицо производящее какие-либо действия с информационной доказательственной базой несет полную ответственность за ее сохранность, пока данная информация находится в его распоряжении;

[1] Хомколов В.П. Организационно-правовые аспекты расследования и предупреждения преступлений в сфере компьютерной информации: дис. … канд. юрид. наук: 12.00.09 / В.П. Хомколов; БГУЭП. Иркутск, 2014. С. 111.

6) любое учреждение, производящая изъятие, доступ, хранение, а также экспертизу должна строго соблюдать данные принципы.[1]

Как показывает практика, по уголовным делам о мошенничестве в сфере компьютерной информации, возможно назначение других видов экспертиз. К таким видам экспертиз относится исследование традиционных следов, обнаруженных и установленных в ходе расследования уголовного дела. Данный факт, связан с тем, что лицом, расследующим уголовное дело, может изыматься не только компьютерная техника, но и объекты традиционного характера (различные традиционные следы, документы, черновики, копии документов, материалы и вещества). Производство таких видов экспертиз, диктуется особенностью совершенного преступного деяния, и оставленными на месте происшествия следов преступником.

При рассмотрении отношении связи, «преступник – жертва», в их взаимосвязь вовлечено множество объектов и предметов, но итогом обязательно являются – материальные блага (денежные средства). Процесс перехода данных материальных благ к преступнику, который будет иметь возможность распорядиться ими в своих целях имеет свои особенности и специфику. Именно поэтому мошенничество в сфере компьютерной информации сложное явление для изучения, его отображения во внешней среде, но в то же время у данного преступления есть свои особенности, присущие только данному деянию. Именно данный характер, и наличие объектов, содержащих следы преступления – дают информацию о данном событии.

Как верно отметил Н.Н. Егоров, факты преступления устанавливаются в зависимости от объекта исследования как источника сведении. Иными словами, объект исследования, это носители информации, которые подвергаются исследованию. Объекты исследования на законодательном уровне определены как вещественные доказательства, документы, предметы, животные, трупы и их

[1] Судебная экспертиза: типичные ошибки / под ред. Е.Р. Россинской. М.: Проспект, 2013. С. 477-478.

части, живые лица, образцы для сравнительного исследования, а также материалы дела, по которому производится судебная экспертиза. Также дополняя список, можно отметить в качестве объектов экспертизы, могут быть жидкие вещества (чернила, жидкий клей и т.п.) и сыпучие вещества (разного рода порошковые краски, порошковый не разбавленный клей и т.п.)[1]

Доказательственная база рассматриваемой категории дел будет строиться таким образом, что фиксируется факт движения информации от одного объекта к другому при помощи компьютерно-технических средств, с последующим хищением материальных ценностей и обращение их в свою пользу преступником. Весь этот процесс, не может состояться без оформления различных бумажных документов (начиная от покупки компьютера, оформления договора предоставления услуг провайдером и заканчивая обналичиваем денежных средств, полученных преступным путем). Именно данные обстоятельства, указывающие на конкретное лицо, как причастного к совершенному преступлению, свидетельствуют о необходимости проведения традиционных видов экспертиз. К таким экспертизам, назначение которых необходимо, ученые относят: дактилоскопическую, трасологическую, почерковедческую, портретную, экспертизу технического исследования документов и т.п.[2]

Так, судом установлено, что преступления были совершены группой лиц по предварительному сговору, в которую входил З. Он не имел доступа к платежной системе «Б.». Однако именно благодаря доступу в эту систему и были совершены хищения денежных средств ООО «В.» и ООО «К.». При этом в компьютерной базе ООО «В.», созданного З., было найдено упоминание об организациях, на чьи расчетные счета переводились денежные средства потерпевших. Эти же сведения были обнаружены в компьютере Л. В письме от юридического лица о передаче домена ООО «В.» другому лицу согласно

---

[1] Егоров Н.Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспекты. М.: Юрлитинформ, 2017 г. С. 219.

[2] Криминалистика: учебник / Аверьянова Т. В. [и др.]; под ред. Р.С. Белкина. М., 2001. С. 415.

экспертному заключению, проставлена поддельная подпись У., выполненная неким иным лицом.[1]

В целях эффективного решения задач и получения результатов по раскрытию преступления, некоторые авторы, отмечают возможность назначения комплексной экспертизы, которая сочетает в себе как компьютерную экспертизу, так и другие виды экспертиз (дактилоскопическую, экспертизу веществ и материалов, технико-криминалистическую экспертизу документов и т.п.).[2] Данный вид изучения преступного явления, основывается на системном анализе и комплексном характере исследования, методами различных наук, а полученные результаты обобщаются и синтезируются в единое знание о нём.

По результатам комплексного исследования, следователь получает возможность, оперировать значительным объемом о связях лиц, участвовавших в совершении преступления, установить особенности совершения мошенничества в сфере компьютерной информации.

Так, например, проведенными по уголовному делу экспертизами был установлен факт переписки осужденных Б. и Б. путем использования программы «Skype» в которой ими обсуждалась деятельность по обналичиванию денежных средств в размере 2 312 000 рублей, похищенных с расчетного счета ООО «Т»[3]

Достаточно часто на практике, встречаются случаи участия руководителей предприятии и учреждении, а также сотрудников финансовых подразделении в хищении материальных ценностей. Выявить роль участия, а также факт участия, с учетом их руководящей роли, достаточно сложно, так как выше указанные лица имеют доступ к внутренним документам предприятия, организации что облегчает вносить изменения, и способствовать сокрытию

---

[1] Уголовное дело №35/184-12 // Архив Тверского районного суда г. Москвы.

[2] Шуваева М.С. Правовые, научные и организационные основы назначения и производства комплексной экспертизы: дис. … канд. юрид. наук: 12.00.09 / М.С. Шуваева. М., 2016; Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / под ред. Ю.В. Гаврилина. М.: ЮИ МВД РФ, 2013. С. 163.

[3] Уголовное дело №128/78-12 // Архив Городского суда г. Москвы.

следов мошенничества в сфере компьютерной информации. Поэтому при проведении экспертных исследовании, необходимо соблюдать правила непротиворечивости систем информации (учетной, внеучетной, правовой, аналитической и др.), что гарантирует правильность проверки оформления в соответствии требованиям документов конкретной финансово-хозяйственной деятельности. Это позволяет выявить несоответствия в хозяйственной деятельности предприятия, за коим руководители могли скрыть признаки экономических преступлении (подлоги документов, уничтожение, подмена и др).[1]

При обнаружении документов, в которых содержатся подложные или искаженные сведения, появляется необходимость назначения судебно-технической экспертизы документов и судебно-почерковедческой экспертизы.

В теории технико-криминалистические экспертизы и исследования документов делятся на следующие виды, в зависимости от характера решаемых задач и от объекта исследования:

а) экспертиза документов с измененным первоначальным содержанием (измененных путем дописки, дорисовки и допечатки, подчистки, травления и смывания, залитых и замазанных текстов); установление факта замены частей документов;

б) исследование невидимых и слабовидимых текстов (угасших); документов, подвергшихся воздействию высоких температур (сожженных); рельефных штрихов;

в) экспертиза по установлению технических приемов и средств воспроизведения подписи;

г) экспертиза бланков документов;

д) экспертиза оттисков удостоверительных печатных форм (печатей и штампов);

е) экспертиза текстов, выполненных на печатающих устройствах;

---

[1] Кеворкова Ж.А., Савин А.А. Судебно-бухгалтерская экспертиза: учеб. пособие. М.: Вузовский учебник, 2015. С. 34.

ж) экспертиза реквизитов документов с целью определения последовательности их выполнения;

з) экспертиза материалов документов (бумаги, клея, красящих веществ и т.п.)[1]

Такие исследования проводятся в случаях использования поддельных документов при совершении мошенничества в сфере компьютерной информации, когда преступники путем поддельного паспорта регистрируют, например, подключение Интернет-услуг через которые в последующем намереваются скрыть следы преступления. Такие приемы, часто используют злоумышленники при совершении преступления с входом в Интернет пространство через мобильные устройства и, как правило, такие преступления совершаются организованными преступными формированиями. Данные особенности необходимо учитывать при расследовании рассматриваемого вида мошенничества.

Следует отдельно отметить, что при выборе той или иной экспертизы по делам о мошенничестве в сфере компьютерной информации определенно зависит от конкретной следственной ситуации, а также результатов ОРД, и ранее проведенных следственных действии. Кроме этого, применение специальных знаний по делам рассматриваемой категории предусматривает их использование не только на первоначальном и последующем этапах, но и в ходе производства ОРМ. Такая специфика определяется механизмом преступной деятельности.

Оценка экспертного заключения является одним из видов доказательств, которые предусмотрены нормой права, а именно уголовно-процессуальным законодательством (ч. 2 ст. 74, ст. 80 УПК РФ). Согласно ч. 2 ст. 17 УПК РФ: ни одно доказательство не имеет заранее установленной силы (общее правило), данная формулировка предусматривает что, хоть и заключение эксперта несет в себе значимую информацию о событии преступного деяния для следователя

[1] Экспертизы на предварительном следствии: краткий справочник / под. Общ. ред. В.В. Мозякова. М.: ГУ ЭКЦ МВД России, 2013. с. 56.

(дознавателя), (так как основывается на бесспорных научных положениях науки), даже в этом случае оно не ставится в преимущество перед другими доказательствами. Несмотря на это, следователь (дознаватель) обязан оценить и проверить заключение эксперта, как и любое другое доказательство, по ст. 88 УПК РФ на относимость, допустимость, достоверность. Относимость предполагает, что выводы эксперта должны быть связаны с обстоятельствами, подлежащими доказыванию. Допустимость предусматривает, пригодность предоставленной информации в качестве доказательственной базы, включая правильность соблюдения назначения экспертизы в соответствии процессуальным порядкам; допустимость объектов экспертного исследования; соответствие лица производящего экспертизу определенным требованиям. Достоверность содержит в себе компетентность эксперта; научную обоснованность применяемых методов; логичность умозаключений; полное исследование; обоснованность выводов. Необходимость проверки предоставленных экспертом выводов, требует такой проверки, так как встречаются различного рода ошибки, допущенные как на подготовительном этапе исследования, так и в процессе производства самой экспертизы, а также возможны допущение ошибок при оформлении заключения экспертом. Особенно важную роль играет судебно-компьютерные экспертизы, так как они представляют новый класс судебных экспертиз, и говорить о полном правовом регулировании проведения такого вида экспертиз рано, как и о методическом обеспечении, а назначение таких видов экспертиз каждым годом увеличивается. Как отмечают в теории некоторые авторы, не каждая экспертиза может похвастаться высоким качеством ее проведения, и создаваемым на его основе заключением эксперта. Но исследования в данной области ведутся постоянно, обновляются научно-методические разработки, что повышает эффективность использования данного вида знания в правоохранительной

практике.[1]

В этой связи подтверждаются нами сказанное, о необходимости назначения для расследования уголовных дел данной категории наиболее опытным следователям. Кроме этого, для повышения эффективности деятельности следователя в расследовании преступления следует привлекать специалиста, профессиональные консультации которого значительно повышают эффективность производства следственных и процессуальных действии.

[1] Семикаленова А.И., Хатунцев Н.А. Ошибки, допускаемые при производстве судебных компьютерно-технических экспертиз / Судебная экспертиза: типичные ошибки / под ред. Е.Р. Россинской. М.: Проспект, 2013. С. 469-492;

ЗАКЛЮЧЕНИЕ

После проведенного исследования, можно сделать следующие выводы, имеющие практическое значение при расследовании мошенничества в сфере компьютерной информации:

1) Объективной особенностью изучения данного вида мошенничества является его специфический объект познания. С одной стороны – мошенничество, как определено законодателем хищение чужого имущества, с другой – виртуальная среда в которой совершается преступный умысел преступника, где он осуществляет вмешательство в компьютерную информацию, тем самым отражает следовую картину преступления. Именно в таком виде объект исследования, имеет определяющее значение в формировании криминалистически значимой информации о данном виде преступлений.

2) Криминалистическая характеристика мошенничества в сфере компьютерной информации, позволяет обобщить признаки и свойства преступления, предусмотренного ст. 159. 6 УК РФ. К таким элементам можно отнести: непосредственный предмет преступного посягательства; способ совершения преступления, орудия и средства преступления; следы и механизм следообразования; обстановка совершения преступления, его пространственно-временной континуум, которые в свою очередь, характеризуются корреляционной зависимостью между собой, и специфичностью проявлений во внешней среде (киберпространстве), что и отличает данный вид преступной деятельности от схожих видов преступлений, и позволяет служить основанием для выдвижения типичных версий о событии преступления и личности преступника, определения направления поиска и познания лица, ведущего расследование.

3) Специфической особенностью взаимодействия злоумышленника и жертвы, при совершении мошенничества в сфере компьютерной информации, осуществляемого посредством компьютерных технологий, подключенных и имеющих выход в сеть – Интернет. Учитывая такой характер, основными

элементами механизма преступления будут являться:

- деятельность субъекта преступления.
- действия и поступки пострадавшего от мошенничества в сфере компьютерной информации.
- действия и поступки лиц, косвенно связанных с данным видом мошенничества.
- элементы обстановки, используемые участниками преступного события, включая предмет преступного посягательства.

4) Возбуждению уголовного дела о фактах мошенничества в сфере компьютерной информации предшествует сбор информации путем оперативно-розыскной, следственной деятельности, и иных процессуальных действий, при соблюдении правил сохранения первоначальной формы доказательственной информации, и без ущерба свойствам изымаемой информации. Достижение данных задач, возможно путем использования технических средств с обязательным привлечением специалиста в данной области и своевременного активного взаимодействия с сотрудниками подразделении специализирующихся на расследовании и раскрытии данных видов преступлений.

5) Наиболее целесообразно, в ходе осуществления предварительной проверки по делам о мошенничестве в сфере компьютерной информации, следователю, лицу, производящему дознание, а также оперативным сотрудникам производство следующих действий:

- получение объяснений от лиц, заявивших о совершении в отношении их или предприятий мошенничества;
- осмотр и изъятие компьютерно-технических средств, которые предположительно были использованы в ходе совершения мошенничества;
- осмотр локальных и иных видов сетей, используемых на предприятиях и учреждениях;

- осмотр и изъятие документов, которые могут содержать следы преступления; осмотр и изъятие документов свидетельствующих об оказании услуг подключения к сети провайдером;
- назначение проверок и ревизий для проверки хозяйственной деятельности предприятия или учреждения, в целях установления факта хищения материальных ценностей;
- назначение и производство экспертиз, диктуемых складывающейся следственной ситуацией (компьютерной, дактилоскопической, судебно-бухгалтерской, экспертизы документов и т.п.);
- дача поручений о производстве оперативно-розыскных мероприятий, направленных на установление лиц, причастных к совершению мошенничества, а также свидетелей.

6) Выбор тактики производства следственных и процессуальных действий зависит от самого механизма преступного события, применяемыми злоумышленником компьютерно-технических средств, программным обеспечением установленных на компьютер злоумышленника и потерпевшего, наличием знании о навыках и умениях лица, совершившего преступление данного вида, а также предположительных знаниях поведения подозреваемых лиц в ходе проведения следственных действий.

7) При расследовании мошенничества в сфере компьютерной информации наиболее целесообразно производство следующих следственных и иных процессуальных действий:

- допрос свидетелей, потерпевших, подозреваемых, обвиняемых;
- осмотра места происшествия, предметов и документов;
- обыска и выемки;
- получения образцов для сравнительного исследования;
- а также других следственные действия, выбор которых обусловлен складывающейся следственной ситуацией.

8) Учитывая характер использования специальных знании при

расследовании мошенничества в сфере компьютерной информации, наиболее успешными их использованием является привлечение специалиста, который оказывает консультационную помощь при производстве следственных и иных процессуальных действий. Для формирования доказательственной базы, также используется следователем назначение и производство экспертиз. По делам рассматриваемой категории производится такие виды экспертиз:

- компьютерные экспертизы (аппаратно-компьютерная; программно-компьютерная; информационно-компьютерная; компьютерно-сетевая);
- экономические экспертизы (бухгалтерская);
- криминалистические экспертизы (техническая экспертиза документов, и в ряде случаев – трасологическая экспертиза).

Исходя из содержания, выпускная квалификационная работа способствует решению ряда задач методики расследования мошенничества в сфере компьютерной информации. Перспективы развития и применения, достижении в области кибернетики, в одном ряде с разработкой необходимых практических рекомендации расследования мошенничества рассматриваемой категории обеспечивает успешную деятельность по расследованию преступления следователю.

Таким образом, данные исследования позволяют, исходя из задач, стоящих перед правоохранительными органами, актуализировать частную методику расследования мошенничеств в сфере компьютерной информации, выработать криминалистические рекомендации и наметить пути совершенствования криминалистических средств и методов раскрытия и расследования указанного преступления.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

Законы, нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // Собрание законодательства РФ", 04.08.2014, N 31, ст. 4398;
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 23.04.2018) // Собрание законодательства РФ, 24.12.2001, N 52 (ч. I), ст. 4921;
3. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 23.04.2018, с изм. от 25.04.2018) // Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954;
4. О полиции: [федер. закон от 07.02.2011 №3-ФЗ: принят Гос. Думой 28 дек. 2014 г.: по состоянию на 13 июля 2015 г.] // «Собрание законодательства РФ». – 2011. – №7. – ст. 900.
5. Об информации, информационных технологиях и о защите нформации [федер. закон от 27.07.2006 №149-ФЗ: принят Гос. Думой 8 июля 2006 г.: по состоянию на 19 дек. 2016 г.] // «Собрание законодательства РФ». – 31.07.2006. – №31 (1 ч.). – ст. 3448.
6. «Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» (утв. Генпрокуратурой России). Текст документа приведен в соответствии с публикацией на сайте http://genproc.gov.ru по состоянию на 15.04.2014.

Монографии, учебники, учебные пособия

1. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореферат дис. ... канд. юрид. наук: 12.00.09 / В.Ю. Агибалов. Воронеж, 2010; Мещеряков В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков // Библиотека криминалиста. – 2013. – № 5. С 640.
2. Айвазова О.В. Криминалистическая характеристика преступлений как систематизированное отражение механизма преступной деятельности: результаты научной полемики // Вестник Томского государственного университета. – 2014. – №389. С 782.
3. Атаманов, Р.С. Основы методики расследования мошенничества в сети интернет: автореф. дис. … канд. юрид. наук: 12.0012 / Р.С. Атаманов. М., 2012. С. 12. С 326.
4. Белкин Р.С. Проблемы, тенденции, перспективы. От теории к практике. М., 1988 г. С 874.
5. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. – 2012. – №1. С 428.
6. Видонов Л.Г. Криминалистическая характеристика убийств и системы типовых версий о лицах, совершивших убийства без очевидцев. Горький, 2013г. С 280.
7. Воробец И.Н. Глобальная сеть Интернет, как пространство для совершения преступлений // Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России: доклады междунар. науч.-практ. конф. / под ред. А.М. Кустова, Т.Ю. Прокофьевой. М.: МЭЙЛЕР, 2012 г. С 175.
8. Вражнов А.С. Криминалистический риск при расследовании неправомерного доступа к компьютерной информации: автореферат дис. ... кандидата юридических наук: 12.00.12 / А.С. Вражнов. М., 2015 г. С 29.
9. Гавло В.К. Теоретические проблемы и практика

применения методики расследования отдельных видов преступлений. Томск, 2015 г. С 574.

10. Егоров Н.Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспекты. М.: Юрлитинформ, 2017 г. С 210.
11. Ершов В.А., Костылева Г.В., Милованова М.М. Методика расследования преступлений против жизни и здоровья граждан, совершаемых членами неформальных групп (движений): науч.-практ. пособие. М.: Юрлитинформ, 2017 г. С 632.
12. Згадзай О.Э., Хафизова Л.С. Финансовая преступность и мошенничество в сети Интернет. Казань. 2006 г. С 250.
13. Зигура Н.А., Кудрявцев А.В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. М., 2015.
14. Зубань О.В. Проблема спама и ее решения // Материалы конференции. М., 2013 г. С 110.
15. Кеворкова Ж.А., Савин А.А. Судебно-бухгалтерская экспертиза: учеб. пособие. М.: Вузовский учебник, 2015 г. С 372.
16. Ким Д.В. Проблемы теории и практики разрешения криминалистических ситуаций в процессе раскрытия, предварительного расследования и судебного рассмотрения уголовных дел: дис. … д-ра юрид. наук: 12.00.09 / Д.В. Ким. Барнаул, 2009 г. С 140
17. Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. … д-ра. юрид. наук: 12.00.2013 г. С 70.
18. Колоколов Н.А. Преступления против собственности: комментируем новеллы УК РФ // Мировой судья. – 2013. – №1. С 280.
19. Комарова А.А. Интернет-мошенничество: проблемы детерминации и предупреждения: монография. М.: Юрлитинформ, 2014. С 310.
20. Косынкин А.А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на

стадии предварительного расследования // Российский следователь. – 2012 г. С 365.

21. Кустов А.М. Теоретические основы криминалистического учения о механизме преступления. М., 2015 г. С 280.
22. Кустов А.М. Криминалистика и механизм преступления: цикл лекций. М.: МПСИ; Воронеж: МОДЕК, 2012 г. С 461.
23. Лавров В.П. Криминалистика. М.: Норма, 2014. С. 330.
24. Махтеев М.Ш. Методика расследования компьютерных преступлений: учеб. пособие. М.: РосНОУ, 2017 г. С 257.
25. Методика расследования налоговых преступлений: учеб. пособие / под общ. ред. А.А. Кузнецова. М.: ЦОКР МВД России, 2017 г. С 273.
26. Мещеряков В.А. «Виртуальные следы» под «скальпелем Оккама» / Информационная безопасность. Саратов: ГОУВПО «Саратовский юридический институт МВД России. 2016. №1(4). С 270.
27. Моисеева Т.Ф. Основы судебно-экспертной деятельности: конспект лекций. М.: РГУП, 2016 г. С 179.
28. Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / под ред. Ю.В. Гаврилина. М.: ЮИ МВД РФ, 2013 г. С 290.
29. Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С 235.
30. Протасевич А.А., Зверянская Л.П. Проблемы собирания и оценки компьютерной информации как доказательства // Современная криминалистика: проблемы, тенденции, имена (к 90-летию профессора Р.С. Белкина): сб. материалов 53-х криминалистических чтений: в 3 ч. М.: Академия управления МВД России, 2012. Ч. 3. С 492.
31. Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. – 2016. – №11. С 70.

32. Пучкова И.М. Психологические аспекты профессиональной подготовки пользователей ЭВМ: автореф. …канд. психол. наук: 19.00.03 / И.М. Пучкова. М., 2016г. С 59.
33. Россинский С.Б. Результаты «невербальных» следственных и судебных действий как вид доказательств по уголовному делу. М.: Юрлитинформ, 2015 г. С 164.
34. Самойлов А.В. Современное состояние учения о криминалистической характеристике преступлений // Российский следователь. – 2012. – № 22. С 74.
35. Семенов Г.В. Криминалистическая классификация способов совершения мошенничества в системе сотовой связи // ИНФОРМОСТ–Средства связи. М., 2011. №3. С 190.
36. Семикаленова А.И., Хатунцев Н.А. Ошибки, допускаемые при производстве судебных компьютерно-технических экспертиз / Судебная экспертиза: типичные ошибки / под ред. Е.Р. Россинской. М.: Проспект, 2013г. С 458.
37. Семикаленова А.И. Судебная программно-компьютерная экспертиза по уголовным делам: дис. … канд. юрид. наук: 12.00.09 / А.И. Семикаленова. М., 2015. С 180.
38. Скобелин С.Ю. Использование специальных знаний при работе с электронными следами // Российский следователь. – 2014. – №20. С 350
39. Смушкин А. Виртуальные следы в криминалистике. 2014 г. С 281.
40. Степаненко Д.А. К вопросу о поисково-познавательном «инструментарии» следователя // Российское правосудие. – 2012. – №7. С 257.
41. Хомколов В.П. Организационно-правовые аспекты расследования и предупреждения преступлений в сфере компьютерной информации: дис. … канд. юрид. наук: 12.00.09 / В.П. Хомколов; БГУЭП. Иркутск, 2014 г. С 172.
42. Чекунов И.Г. Квалификация мошенничеств, связанных с блокированием

программного обеспечения компьютеров пользователей сети Интернет // Российский следователь. – 2012. – №5. С 72.

43. Челышева О.В. Механизм преступления и криминалистическая характеристика // Вестник криминалистики. Вып. 2. М., 2010 г. С 54.
44. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. …канд. юрид. наук: 12.00.12 / Е.С. Шевченко. М., 2012. С 75.
45. Шепель В.А. Современные способы мошенничества в сети Интернет // Актуальные проблемы борьбы с преступностью на современном этапе: тез. докл. и сообщ. всерос. науч.-практ. конф. Омск: Омская акад. МВД РФ, 2013 г. С 167.
46. Шурухнов Н.Г. Использование при допросе ранее данных объяснений // Тактические приемы допроса и пределы их использования. М., 2013 г. С 249.
47. Экспертизы на предварительном следствии: краткий справочник / под. Общ. ред. В.В. Мозякова. М.: ГУ ЭКЦ МВД России, 2013 г. С 176.

Эмпирические материалы (материалы судебной, следственной практики)

48. Уголовное дело №00234-12 // Архив судебного участка №2 Авиастроительного района г. Казани.
49. Уголовное дело №35/184-12 // Архив Тверского районного суда г. Москвы.
50. Уголовное дело №128/78-12 // Архив Городского суда г. Москвы.

Электронные ресурсы

51. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Россия (дата обращения: 17.12.2017).

52. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Россия (дата обращения: 15.01.2018).
53. [Электронный ресурс]. URL: http://portaltele.com.ua/news/officially/2013-02-14-13- 34-52.html (дата обращения: 14.11.2017).
54. [Электронный ресурс]. URL: https://мвд.рф/mvd/structure1/Centri/JEkspertno_ kriminalisticheskij_centr(дата обращения: 17.12.2017).