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

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность
(специализация «Оперативно-розыскная деятельность»,
узкая специализация «Деятельность сотрудника подразделения
по контролю за оборотом наркотиков»),
форма обучения очная, набор 2019 года

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:

ОСОБЕННОСТИ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Выполнил:
Слушатель группы П 1902
младший лейтенант полиции
Кулаков Антон Васильевич

Руководитель:
заместитель начальника
кафедры криминалистики
кандидат юридических наук
подполковник полиции
Поляков Николай Владиславович

Дата защиты:
«19» 06 2024 г.
Оценка: хорошо
Председатель ГЭК
полковник полиции _____ А. П. Голубев
(специальное звание) (подпись) (инициалы, фамилия)

Красноярск 2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Человечество живет в век цифровизации и развития компьютерных технологий, когда у каждого дома и на работе есть компьютерные устройства. Практически безграничные возможности сети Интернет в области передачи и обработки информации, обеспечивают коммуникацию доступной в разных формах, торговлю, совершение финансовых операций и многое другое, делают Интернет благоприятной средой для развития общественных отношений, с одной стороны, с другой же стороны, служит плацдармом для совершения преступлений.

Когда интернет-пространство впервые стало использоваться преступниками для совершения общественно опасных деяний, такие преступления рассматривались лишь в рамках преступлений в сфере компьютерной информации. В сегодняшних реалиях Интернет используется преступниками различных категорий, выступая в качестве как способа, так и средства совершения преступлений, таким образом выходя за ранее обозначенные рамки.

По данным статистики органов внутренних дел за 2019 год, количество зарегистрированных преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, составляет 294409, за 2020 год было зарегистрировано 510596 преступлений данной категории, в 2021 году – 517722 преступления, в 2022 – 522065 преступлений, а в 2023 году число зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, равно 676951[1].

Проведя анализ вышеуказанных данных, видим, что на всем протяжении, рассматриваемого периода, усматривается стабильный рост числа зарегистрированных преступлений, совершенных с использованием

[1] Данные официального сайта МВД России. URL: https://мвд.рф (дата обращения: 20.03.2024).

информационно-телекоммуникационных технологий или в сфере компьютерной информации, что также показывает актуальность выбранной темы исследования.

Актуальность выбранной темы исследования также обусловлена имеющимися недостатками в деятельности органов внутренних дел, занимающихся выявлением, раскрытием и расследованием преступлений в сфере информационно-телекоммуникационных технологий, что выражается в недостаточно оперативном реагировании сотрудниками полиции на указанные преступления, и в том числе, в неполном и некачественном проведении первоначальных следственных действий, что в свою очередь, приводит к отсутствию или неполноте собранной информации.

Объект исследования включает в себя с одной стороны, преступную деятельность по совершению преступлений в сфере информационно-телекоммуникационных технологий, а с другой стороны деятельность компетентных лиц по расследованию указанных преступлений.

Предметом исследования выступают закономерности деятельности преступников причастных к преступлениям в сфере информационно-телекоммуникационных технологий, а также закономерности деятельности правоохранительных органов по расследованию данных преступлений.

Цель выпускной квалификационной работы заключается в том, чтобы на основе анализа теоретических источников и судебно-следственной практики исследовать методику расследования преступлений в сфере информационно-телекоммуникационных технологий и определить проблемные аспекты, возникающие в ходе расследования уголовных дел по выбранной теме.

Достижение цели предопределило постановку и решение следующих **задач**:

- Проанализировать теоретические источники о расследовании преступлений в сфере информационно-телекоммуникационных технологий;

- Рассмотреть судебно-следственную практику о расследовании преступлений в сфере информационно-телекоммуникационных технологий;

- Изучить элементы криминалистической характеристики преступлений в сфере информационно-телекоммуникационных технологий

- Раскрыть тактические особенности производства следственных действий, проводимых при расследовании преступлений в сфере информационно-телекоммуникационных технологий;

- Исследовать особенности использования специальных знаний при расследовании преступлений в сфере информационно-телекоммуникационных технологий.

Методы и методология исследования. Методологическую основу исследования составляют общенаучные методы познания, в частности анализ, синтез, классификация, логико-аналитический метод опроса и анализа документов, систематизации и обобщения. В качестве частно-научных методов применялись следующие: сравнение, системно-структурный и эмпирический методы.

Теоретическая основа исследования. В работе была использована специальная и научная литература, монографии, а также материалы судебной практики. В своём исследовании автор основывался на трудах следующих известных учёных-криминалистов: Р.С. Белкина, А.Г. Волеводза, В.А. Мещерякова, Е.Р. Россинской, Сидоровой А.Е., Д.А. Соколова, И.Г. Чекунова и др.

Нормативно-правовая основа исследования. Конституция Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с

использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»».

Структура работы. Работа состоит из введения, двух глав, включающих в себя пять параграфов, заключения и списка используемых источников.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

1.1 Способы совершения преступлений в сфере информационно-телекоммуникационных технологий

Р.С. Белкин считает, что данные о способе совершения преступления является центральной частью криминалистической характеристики в силу того, что именно они выражают функциональную сторону деятельности преступника[2].

Нельзя не согласиться с данным мнением и в связи с этим, считаем, что при формировании методики расследования преступлений в сфере информационно-телекоммуникационных технологий важно подробно рассмотреть данный элемент криминалистической характеристики.

А.А. Бессонов в своих трудах отмечает, что способ совершения преступления – есть система объединенных общим преступным умыслом действий преступника, включающих в себя не только выполнение общественно опасных действий, но и подготовку к выполнению, и дальнейшее сокрытие факта выполнения общественно опасных действий, детерминированных условиями его обстановки, объектом посягательства и психологическими свойствами личности, представляющих совокупность приемов, орудий, следов и находящих свое отражение в объективной реальности в виде следов, обуславливающая методику его расследования и установление ретроспективной модели совершенного преступления[3].

---

[2] Белкин Р.С. Криминалистика. - М.: НОРМА, 2006.-693 с.

[3] Бессонов, А.А. Способ преступления как элемент его криминалистической характеристики // Пробелы в российском законодательстве. – 2014. – №4. – С. 171-173.

Многие «традиционные» преступления, такие как мошенничество, кражи, шпионаж и даже терроризм, теперь находят свое отражение в киберпространстве.

Мошенничество, безусловно, является наиболее распространенным преступлением в информационно-телекоммуникационной сети Интернет. С помощью различных схем и методов, преступники могут обмануть и нанести ущерб, как отдельным пользователям, так и организациям. Например, фишинговые атаки, вредоносные программы, кража личных данных и кредитной информации, фейковые онлайн-магазины и многое другое – все это является способами интернет-мошенничества.

Такое разнообразие способов мошенничества делает киберпространство особенно опасным для пользователей. Важно быть бдительными и принимать меры предосторожности при работе в сети, например, проверять подлинность веб-сайтов, не раскрывать личную информацию без необходимости, устанавливать антивирусное программное обеспечение и так далее.

Понимание способов, используемых мошенниками, а также обучение кибербезопасности становятся все более важными в нашей современной цифровой эпохе. Только путем повышения осведомленности и принятия соответствующих мер мы можем защитить себя и свои данные от киберпреступников.

Изучив научные труды и судебную практику по анализируемой категории уголовных дел, можем выделить следующие способы совершения кибермошенничества, существующие на сегодняшний день:

1) «Фишинг». Способ совершения мошенничества в информационно-телекоммуникационной среде Интернет, который заключается в обмане пользователя для получения личных данных: номер телефона или банковской карты, логина или пароля от аккаунтов различных приложений, социальных сетей и т.п.

Реализация данных преступлений проста. Правонарушители отправляют электронные письма потерпевшим, представляясь при этом именем сервиса или организации, услугами которых пользуется жертва. Адрес отправителя письма похож на настоящий. Мошенники маскируют фишинговые письма под официальные, рассчитывая на невнимательность пользователей при их изучении.

Мошенники стремятся завоевать доверие пользователей, чтобы затем убедить их перейти по ссылке в электронном письме на поддельный веб-сайт и предоставить там личные данные. Как правило, фишинговые сайты являются точной копией настоящих. Беря во внимание вышесказанное, видим, когда пользователей просят ввести конфиденциальные данные на таких сайтах, они не могут распознать обман. В случае, когда потерпевший вводит конфиденциальные данные, информация оказывается у преступников.

Для наглядности приведем пример из судебной практики. Чертановским районным судом г. Москвы П, П1 и С признаны виновными в совершении преступлений, предусмотренных ч. 2 ст. 272, ч. 1 ст. 273 и ч. 4 ст. 159 УК РФ. Братья П. изучили основные принципы работы дистанционного банковского обслуживания, изучили возможное вредоносное программное обеспечение, а также его назначение, правила и порядок установки вредоносного программного обеспечения, порядок и способы его модификации в целях сокрытия указанных программ от антивирусных средств, механизм регистрации собственного веб-ресурса, порядок его администрирования и разработали план по хищению денежных средств. В реализации задуманного им помогали С., а также неустановленные лица, которым отвели определенные роли в разработанном плане хищения. С. благодаря использованию троянского вируса, изменил параметры банковского сайта, что привело к перенаправлению клиентов на фальшивый веб-сайт, на котором были размещены контактные номера

службы поддержки, используемые для сбора уникальных номеров и паролей от клиентов[4].

2) Так же «фишинг» может быть представлен в своем упрощенном виде и выражается лишь в создании фальшивых интернет-сайтов каких-либо организаций, будь то: благотворительные организации, фирмы и государственные структуры. Жертва, попадая на данный сайт, и не подозревает, что, приобретая какой-либо продукт и услугу взамен ничего не получит и лишь лишится своих денежных средств.

В качестве примера можно привести случай, произошедший в г.Красноярске. Молодой человек познакомился с девушкой на интернет-площадке для знакомств. Далее девушка предложила сходить на свидание в театр, отправила ссылку на фальшивый сайт театра и попросила заранее купить билеты. Молодой человек не стал проверять сайт на подлинность, купил два билета на представление[5].

3) «Скимминг». Способ совершения мошенничества, заключающееся в получении данных банковской карты жертвы, при помощи использования специальных считывающих технических устройств. Скимминговые устройства выглядят как накладки и внешне очень похожи на считывающие устройства банкоматов. Часто так же используют накладную клавиатуру или скрытую камеру.

Приведем пример из судебной практики. Пролетарским районным судом г. Тверь М. признан виновным в совершении преступления, предусмотренного ч.3 ст.30, ч.3 ст.272 УК РФ. Движимый корыстными побуждениями М., находясь в неустановленном месте, вступил с

---

[4] Приговор Чертановского районного суда г. Москвы от 7 сентября 2012 г. по уголовному делу № 1–486/12. – Текст: электронный // СудАкт: Судебные и нормативные правовые акты РФ. – URL: https://sudact.ru/regular/doc/j4eDxuKkqebt/?regular-txt=Попелыши®ular-case_doc=®ular-lawchunkinfo=272+УК+РФ+®ular-date_from=®ular-date_to=®ular-workflow_stage=®ular-area=®ular-court=®ular-judge=&_=1657025602537. (дата обращения: 20.03.2024).

[5] В Красноярске мошенники обманывают горожан с помощью билетов в театр [Электронный ресурс] // NGS24.ru [сайт]. URL: https://ngs24.ru/text/incidents/2022/07/26/71517146/ (дата обращения: 20.03.2024).

неустановленным лицом в сговор, направленный на неправомерный доступ к охраняемой законом компьютерной информации, содержащейся на магнитных полосах пластиковых платежных банковских карт неопределенного круга граждан путем ее копирования, с целью дальнейшей записи откопированной информации на магнитные полосы дубликатов платежных карт, и последующего использования поддельных карт в платежной системе РФ путем обналичивания содержащихся на лицевых счетах скомпрометированных банковских карт денежных средств. С целью успешной реализации своего совместного прямого преступного умысла М. и неустановленное лицо разработали план совершения совместных преступных действий, согласно которому М. и неустановленное лицо намеревались: приискать банкомат для установки на него нештатного оборудования; с целью копирования охраняемой законом компьютерной информации временно установить на приисканный банкомат заранее приготовленное, добытое при неустановленных обстоятельствах неустановленным лицом нештатное «скимминговое» оборудование, изготовленное кустарным способом с использованием элементов промышленного изготовления, состоящее в комплекте из накладной панели, закамуфлированной под инструктивный элемент картоприёмника банкомата и видеорегистратора, выполненного в виде пластиковой планки, закамуфлированной под конструктивный элемент банкомата, предназначенное для негласного получения и регистрации данных с магнитной полосы банковских карт и ПИН-кодов держателей карт; после снятия указанного нештатного оборудования с банкомата произвести запись откопированных магнитных полос скомпрометированных пластиковых платежных банковских карт, информации на магнитные полосы дубликатов пластиковых платежных карт, после чего, в целях получения для себя выгод имущественного характера, с использованием изготовленных дубликатов пластиковых платежных карт и незаконно полученной информации о ПИН-кодах держателей скомпрометированных банковских карт, произвести обналичивание

содержащихся на их лицевых счетах денежных средств, размещенных в целях хранения законными владельцами в кредитных и банковских организациях. М. и неустановленное лицо прибыли на место совершения преступления, где приискали для осуществления своих намерений банкомат. Далее М. и неустановленное лицо вернулись к банкомату. В указанном месте, в указанное время, М. согласно отведенной ему роли подошел к вышеуказанному банкомату, на который установил вышеуказанное «скимминговое» оборудование. В это время неустановленное лицо согласно отведенной ему роли находилось в автомобиле в непосредственной близости от места совершения преступления и наблюдало за окружающей обстановкой, с целью предупреждения М. о возникших непредвиденных обстоятельствах, которые могут помешать реализации их совместного преступного умысла. Однако, довести свой преступный умысел до конца М. и неустановленное лицо не смогли по независящим от них обстоятельствам, так как М. был задержан сотрудниками правоохранительных органов сразу после установки на банкомат вышеуказанного внештатного оборудования, а неустановленное лицо успело скрыться с места преступления. В случае доведения М. и неустановленным лицом преступного умысла до конца, был бы совершен неправомерный доступ к охраняемой законом компьютерной информации, посредством ее копирования[6].

4) «Магические кошельки», «прибыльные игры» и проведение ложных акций и розыгрышей призов. При реализации данного способа совершения кибермошенничества преступники уверяют, что обнаружили «магический кошелек», который работает по следующему принципу: при внесении на него денежных средств, получаешь обратно приумноженное их количество. Цель действий преступников – внушить доверие путем возвращения первых взносов с процентами, вводя при этом потерпевшего в

[6] Приговор Пролетарского районного суда г. Твери от 2 декабря 2014 г. по уголовному делу № 1–281/2014. – Текст: электронный // СудАкт: Судебные и нормативные правовые акты РФ. – URL: https://sudact.ru/regular/doc/ShCnL5gPwRmP/. (дата обращения: 20.03.2024).

азарт от полученного заработка, намекая на более крупную сумму ставки и, следовательно, выигрыша и выманить более крупную сумму. В свою очередь, при проведении ложных акций и розыгрышей призов мошенники действуют схожим образом. Злоумышленники сообщают будущему потерпевшему о том, что последний выиграл приз в акции и для того, чтобы получить свой выигрыш необходимо оплатить доставку. После оплаты через определенное время сообщают, что возникли трудности с оформлением доставки и необходимо доплатить еще определенное количество денежных средств. В конечном итоге мошенники сообщают, что осуществить доставку не представляется возможным и для того, чтобы вернуть внесенные денежные средства необходимо дополнительно внести денежные средства. В конечном же итоге, конечно же, жертва преступления ничего не получает и понимает, что имела дело с мошенниками.

В качестве примера вышеуказанного, приведем случай из судебной практики. Соликамским городским судом Пермского края в Т. признана виновной в совершении преступления, предусмотренного ч. 1 ст. 159 УК РФ. 11 декабря 2020 года по23 января 2021 года, Т., используя информационно-телекоммуникационную сеть «Интернет», со своей страницы в социальной сети Х, в группе А, разместила объявление о розыгрыше духов. 23 января 2021 года у Т., из корыстных побуждений возник преступный умысел, направленный на хищение путем обмана денежных средств потерпевший №1, реализуя который Т. 23 января 2021 года, направила сообщение потерпевшей №1, о том, что последняя выиграла духи за вступление в группу А, при этом Т. в действительности не имела в наличии духов, и не намеревалась осуществлять их доставку, вместе с тем, сообщив последней о том, что для получения духов потерпевшей №1 необходимо оплатить доставку товара. Потерпевшая №1, поверив, что выиграла духи и, что у Т. имеются в наличии выигранные ею духи, сообщила о готовности оплатить доставку товара. После чего Т. указала потерпевшей №1, что для доставки требуется предоставить свои личные данные, номер телефона, адрес

проживания и индекс почты, а также указала номер карты, на которую необходимо оплатить доставку духов. Потерпевшая №1, будучи введенной в заблуждение и поверив, что действительно Т. отправит ей вышеуказанные духи, не подозревая о преступных намерениях последней 23 января 2021 года с банковского счета № перевела, путем использования мобильного приложения, денежные средства в сумме 450 рублей на вышеуказанный Т. счет карты. Далее Т. 23 января 2021 года через непродолжительное время после вышеуказанных преступных действий сообщила потерпевшей №1, что ей необходимо перевести еще денежные средства для оформления почтового отправления. Потерпевшая №1 23 января 2021 года перевела денежные средства в сумме 150 рублей с комиссией в сумме 30 рублей Т. Далее 25 января 2021 года Т. направила сообщение потерпевшей №1, о том, что последней для получения духов необходимо оформить «Ваучер» почтового отправления, для чего перевести денежные средства в сумме 950 рублей. Потерпевшая №1 25 января 2021 года перевела денежные средства в сумме 950 рублей с комиссией в сумме 30 Т. 25 января 2021 года Потерпевшая №1, усомнившись в том, что ей будет направлен подарок, в ходе переписки с Т. высказала желание о возврате своих денежных средств, переведенных ранее за оформление почтового ваучера. Т. 25 января 2021 года в ходе переписки указала, что для возврата денежных средств необходимо, чтобы на балансе карты Потерпевшей №1 находилось 4 000 рублей. Потерпевшая №1, будучи обманутой в том, что денежные средства будут ей возвращены, выполнила условие Т., а именно 25 января 2021 года пополнила баланс своей банковской карты № банковский счет №, на сумму 4 000 рублей. После чего 25 января 2021 года Потерпевшая №1, будучи обманутой Т., выполняя условие последней, осуществила перевод денежных средств в сумме 4 000 рублей со своего банковского счета №, на баланс учетной записи QIWI-кошелька №, открытого на имя Свидетель №4, после чего 25 января 2021 года Т., перевела указанную сумму на банковскую карту эмитированную на свое имя, тем самым похитив

денежные средства потерпевшей №1 в сумме 4 000 рублей. В результате преступных действий Т. потерпевшей №1 причинен материальный ущерб на общую сумму 5 640 рублей, которыми Т. распорядилась по своему усмотрению[7].

Подобным образом обстоят дела и с играми. Они представляют собой игры на подобии фермы, которые приносят «настоящие» денежные средства. Также мошенники указывают, что за плату можно ускорить развитие своей «фермы». При вылечивании первой суммы обычно проблем не возникает, и пользователи, войдя в азарт, ускоряют развитие «фермы» за реальные денежные средства.

Стоит обратить внимание на то, что и в «магических кошельках», и в «прибыльных играх» мошенники предлагают льготные или бонусные условия при использовании их реферальной системы, таким образом и происходит популяризация данного способа совершения кибермошенничества.

Преступники постоянно придумывают новые способы совершения кибермошенничества. Это объясняется просто: когда правоохранительные органы обнаруживают новый способ совершения данного вида преступлений, в дальнейшем исследуют его и информируют об этом население, проводя различные профилактические мероприятия. В связи с ранее сказанным, раскрытый способ совершения интернет-мошенничества теряет свою «актуальность». Таким образом, в полном объеме еще не изучены следующие способы:

1. Шпионское программное обеспечение. Цель данной угрозы – сбор информации о пользователях, которая используется в дальнейшем в целях совершения мошеннических действий. Шпионское программное обеспечение представляет собой программное обеспечение, предназначенное для

[7] Приговор Соликамского городского суда Пермского края от 9 декабря 2021 г. по уголовному делу № 1-463/2021. – Текст: электронный // Актофакт: Архив судебных дел и решений. – URL: https://actofact.ru/case-59RS0035-1-463-2021-2021-11-16-2-0/. (дата обращения: 01.04.2024).

несанкционированного сбора и передачи данных пользователя иному субъекту. В числе собранных данных могут оказаться также и пороли, логины и даже банковские реквизиты. Как правило, шпионское программное обеспечение устанавливается незаметно при совершении таких операций, как: загрузка файлов, установка какой-либо программы, щелчок курсором компьютерной мыши по всплывающему окну. Файлы cookie — это инновационные инструменты, используемые для сбора данных о действиях пользователей в Интернете. При посещении веб-сайтов пользователь соглашается на использование файлов cookie, что позволяет сайтам создавать персонализированный опыт для каждого посетителя. Однако существует риск, что злоумышленники могут использовать файлы cookie для внедрения вредоносного кода на компьютер пользователя без его ведома. В современном мире большинство веб-ресурсов требуют разрешить использование файлов cookie, что делает их более уязвимыми для атак со стороны киберпреступников. Подмена cookie файлов предоставляет преступникам возможность нелегально получать, к примеру, партнерские начисления или проценты как посредникам, если пользователь что-либо приобретет в интернет-магазине.

2. Ботнет. Использование бота или ботнета считается одним из основных методов распространения спама. Ботнет – есть сеть ботов, которые находятся под дистанционным контролем правонарушителей.

М.Ю. Косенко и А.В. Мельников в своей работе отмечают, что бот представляет собой программное обеспечение робота, экземпляр вредоносного программного обеспечения, работающий на зараженном компьютере автономно, автоматически и скрытно от пользователя[8]. Вредоносное программное обеспечение бота заражает хост, как правило, это происходит посредством отправления электронных писем или ссылок на веб-

[8] Косенко М.Ю., Мельников А.В. Вопросы обеспечения защиты информационных систем от ботнет атак // Вопросы кибербезопасности. – 2016. – №4(17). – С. 20 – 28.

страницы посредством загрузки и установки средств дистанционного управления.

Зараженный компьютер, превращенный в зомби, является лишь одним звеном в цепи благодаря связям с серверами, под контролем бот-мастера. Не стоит забывать, что эти серверы играют ключевую роль в управлении всей сетью взломанных устройств, то есть ботнетом. Передача вредоносного программного обеспечения с зараженных компьютеров на другие устройства в сети – это лишь начало цепочки действий, которые могут привести к серьезным негативным последствиям. Важно помнить, что такая цепочка рискует разглашением различных приватных данных, что делает ситуацию еще более опасной.

Существует множество способов, которыми зараженные устройства могут передавать вирусы и другие вредоносные программы на устройства в сети. Возможность автоматического распространения инфекции через слабо защищенные узлы может привести к катастрофическим последствиям. Необходимо понимать, что каждый зараженный компьютер становится звеном в цепи, усиливающим масштаб угрозы для всей сети.

3. Вредоносные программы. При реализации данного способа используются вирусы, которые активируются на компьютере пользователя и в дальнейшем размножаются и распространяются. Как правило, вирусы программируют на: заполнение свободной памяти компьютера, остановку работы windows, обеспечение доступа к конфиденциальным данным пользователя, использование вычислительных ресурсов компьютера в целях добычи криптовалюты.

Чаще всего вирусы распространяются посредством электронной почты, интернет-сайтов, загружаемых файлов, а также USB устройств.

Вирус – майнер представляет собой вредоносную компьютерную программу, использующую вычислительные ресурсы компьютер пользователя с целью добычи криптовалюты. Данные вирусы добывают цифровую валюту прямо на компьютерах пользователей, а после добычи

отправляют монеты на кошельки мошенников. Чаще всего данный вид вирусов устанавливается злоумышленниками в компьютерных сервисах и компьютерными мастерами на дому.

Кроме вирусов так же существуют сетевые черви и трояны. В отличие от вирусов, черви не требуют внедрения в программы для своего распространения. Это одно из ключевых различий между ними. Сетевые черви могут самостоятельно отправлять свои копии на другие компьютеры в сети, что делает их чрезвычайно оперативными в распространении.

Процесс работы сетевого червя начинается с его способности работать независимо, без необходимости активации пользователем. Червь автоматически выполняет рассылку своих копий, поражая большое количество хостов в короткие сроки. Эта способность к самостоятельной и быстрой репликации делает сетевые черви особенно опасными.

Троян представляет собой вредоносное программное обеспечение, маскирующие свое истинное назначение. Он не имеет возможности самостоятельно размножаться. От успешности маскировки трояна под программу, которую согласился запустить пользователь, зависит успешное выполнение своих функций вредоносным программным обеспечением.

Так же стоит отметить, что мошенники получают доступ в сеть при помощи эксплуатации уязвимостей программного обеспечения, атакуя техническое устройство или даже простое угадывание чужого имени пользователя и пароля. Нередко происходят и те случаи, когда бывший сотрудник, имевший в связи с должностными обязанностями пароль и логин фирмы, будучи уволенным, пользуется тем, что работодатель не обновил средства аутентификации, и причиняет ущерб.

Для примера, обратимся к судебной практике. Центральным районным судом г. Челябинска в постановлении о прекращении уголовного дела от 14.09.2009 г. по делу №1 – 356/2010 установлено, что гражданин Х., являющийся заместителем начальника отдела технического обслуживания ООО «А», получил доступ к паролю и логину пользователя почтового

сервера ООО «А», в связи со служебной необходимостью. В дальнейшем данный сотрудник был уволен в связи со сложившимися неприязненными отношениями с работодателем, Х. совершил противоправный доступ к охраняемой законом компьютерной информации, подключившись к серверу ООО «А», удалил компьютерную информацию с сервера, что послужило причиной уничтожения, блокирования и модификации информации.

4. Злоупотреблений доверием пользователей. Реализуя данный способ кибермошенничества, преступники используют выдуманный предлог, чем побуждают будущих потерпевших разгласить нужную для мошенников информацию или выполнить конкретные действия. Если преступнику удается втереться в доверие к потерпевшему, данный метод становится максимально эффективным. Отметим, что шансы на успех прямо пропорциональны массивам информации о жертве, которыми располагает мошенник.

Стоит отметить, что в доктрине отсутствует разделение способов совершения интернет-мошенничества на отдельные группы по схожим признакам, что, в свою очередь, приводит к смешению понятий. В целях систематизации информации, предлагаем следующую классификацию указанных выше способов мошенничества, совершенного при помощи информационно-телекоммуникационной сети Интернет:

1) Перекочевавшие в киберсферу «традиционные» способы совершения мошенничества;

2) Способы, реализация которых основана на внедрении и использовании электронной коммерции;

3) Ложная интернет-реклама;

4) Сигнатурные способы;

5) Способы, построенные на организации онлайн азарта;

6) Онлайн-аукционные способы мошенничества;

На основе вышеперечисленного можем прийти к выводу о том, что можно избежать угрозы кибермошенничества путем применения защитных мер. Для обеспечения безопасности конфиденциальных данных можно

применять помимо простых, сложные реализации фаерволлов и систем обнаружения вторжений. Для входа в компьютер или приложение пользователю необходимы лишь логин и пароль. Рекомендуется изменять имена пользователей по умолчанию, так как они широко известны. Если мошенник знает хотя бы один из этих элементов, ему останется только узнать второй для доступа к системе. Так же не меньшую важность имеет выбор пароля. Подавляющее большинство пользователей выбирают пароль, который легко запоминается, так как строится на основе известных данных, а значит, такой пароль легко угадывается, примеры данных, на основе которых пользователи составляют пароли: дата рождения себя или близкого родственника, имя питомца, номер транспортного средства и многое другое. Исходя из вышесказанного, отметим, что не стоит умалять важность выбора максимально надежного пароля.

По всему миру у пользователей сети Интернет остро встает вопрос кибербезопасности. Чтобы обезопасить свое имущество от деятельности кибермошенников, необходимо укреплять не только личную, но также и имущественную безопасность следующими способами:

1. Своевременное обновление, а также исправление программного обеспечения. Уязвимость в программном обеспечении является главной причиной получения злоумышленниками доступа к хостам и сетям. Необходимо эксплуатировать актуальные версии программного обеспечения, устанавливая текущие и обновления. Исправление – есть небольшой фрагмент кода, назначением которого является устранение определенной проблемы. В отличие от исправления, обновление может не только содержать исправления проблем, но и расширить программный пакет дополнительным функционалом. Поставщики операционных систем и приложений постоянно выпускают новые обновления и исправления, устраняющие известные уязвимости программного обеспечения.

2. Антивирусная защита. Антивирусное ПО выполняет функции предотвращения и реагирования на угрозы. Оно способно предотвратить

заражение компьютера, а также обнаруживать и удалять вредоносные программы, такие как вирусы, интернет-черви и трояны. Для обеспечения максимальной безопасности, рекомендуется установить антивирусное ПО на все компьютеры, подключенные к сети.

3. Средства блокирования спама. Антиспам-системы защищают хосты, идентифицируя и принимая меры против нежелательной почты. Фильтры спама могут быть установлены как на отдельные устройства пользователей, так и на почтовые серверы. Кроме того, многие интернет-провайдеры предлагают услуги фильтрации спама.

4. Брандмауэры. Брандмауэры устанавливаются между различными сетями и играют ключевую роль в контроле сетевого трафика и блокировке несанкционированного доступа. Это делает их одним из самых надежных инструментов за соблюдением безопасности для защиты сетевых пользователей от внешних нападений.

Взглянув на вышеизложенное, можем сделать вывод, что компьютерные сети играют важную роль в повседневной жизни. Кибербезопасность зависит от надежной работы компьютеров и сетей в таких задачах, как электронная почта, учет, организационное управление и работа с файлами. Несанкционированное вторжение в сеть может иметь разрушительные последствия, включая финансовые потери и утрату важной информации. Перечень интернет-мошенничеств, который был рассмотрен, не исчерпывает все возможные виды преступлений в сети. С развитием информационно-телекоммуникационных технологий продолжают прогрессировать и преступления в этой сфере, что подчеркивает важность изучения данной темы.

Стоит отметить, что научно-технический прогресс не стоит на месте, а информационно-телекоммуникационные и компьютерные технологии все больше внедряются в различные сферы человеческой жизнедеятельности. В связи с чем способы совершения данных преступлений нуждаются в постоянном изучении.

1.2 Личность типичного преступника, совершающего преступления в сфере информационно – телекоммуникационных технологий

Личность преступника входит в предмет изучения нескольких юридических наук. Для криминалистики же изучение личности преступника имеет особый интерес, который носит отличный характер, чем, например, в психологии, уголовном праве и криминологии. Это следует из основной задачи криминалистического установления личности, а именно – использование информации для разработки тактики следствия[9].

Знание особенностей личности преступника облегчает расследование преступления. Обусловленность заинтересованности криминалистики в личности преступника состоит в том, что свойства личности преступника дают мотивацию действий лица, определяют цель преступления, способы совершения преступления, сокрытие следов, особенности поведения при подготовке и совершении преступления, а также особенности посткриминального поведения.[10]

Стоит отметить, что типовой набор личностных характеристик подозреваемого во многом формирует характер и содержание складывающейся следственной ситуации.

[9] Повреснюк Г.И. Криминалистические методы и средства установления личности в процессе расследования преступлений. По материалам стран СНГ. М., 2005. С. 28.

[10] Сидорова Е.А. Роль следователя в установлении механизма преступления // Следователь сегодня: материалы науч.-практ. конф. Саратов, 2000. С. 42.

Рассмотрим три ключевых, по нашему мнению, признака структуры личности: социально-демографические, нравственно-психологические, уголовно-правовые.

Статистические данные указывают на то, что наибольшая часть киберпреступлений совершается лицами в возрастной категории от 18 до 29 лет, в свою очередь, наименьшее количество преступлений, совершенных с использованием информационно телекоммуникационной сети Интернет приходится на несовершеннолетних. В соответствии с официальной статистикой, в Российской Федерации доля лиц, которые совершили преступные деяния в возрасте от 18 до 29 лет составляет 42%, также данные свидетельствуют о том, что каждый 5 человек, совершивший рассматриваемую категорию преступлений относится к возрастной группе от 30 до 34 лет, что составляет 20,5%, лица в возрастной группе от 35 до 39 лет – 16,6%, а лица 40 лет и старше – 18,9%. Несовершеннолетние преступники составляют незначительную долю – 2% от общего числа киберпреступников[11].

Произведя анализ данных статистики, приведенных выше, приходим к такому выводу – наибольшая криминальная активность населения в киберпространстве приходится на лиц в возрастной категории от18 до 29 лет, а также от 30 до 34 лет. Такая градация по возрастным категориям объясняется тем, что граждане данных категорий входят в социально-демографическую группу – молодежь, которая проводит в социальных сетях достаточное количество времени, предпочитая общение в киберпространстве.

[11] Редькина, Е. А. Анализ личности преступника, совершающего преступления экстремистской направленности в сети "Интернет" / Е. А. Редькина // Трибуна ученого. – 2022. – № 5. – С. 560-565. – EDN TMOMIO.

Обратив внимание на половые признаки, замечаем, что доля лиц мужского пола значительно превышает долю лиц женского пола, и составляет 65%[12].

Криминалистами установлен факт того, что наиболее криминально активной частью населения являются лица мужского пола. Отметим, что преступления в сфере информационно-телекоммуникационных технологий не являются исключением. Доминирование мужчин объясняется их социальной ролью, статусом в социуме. Немаловажное значение играют и биологические критерии, особенности психологии мужчин.

Также, на ряду с возрастными критериями и половыми признаками, к социально-демографическим признакам относится и уровень образования, который является определяющим фактором в оценке социальной ценности личности. Круг общения индивида, его интересы и жизненные цели во многом зависят от уровня и качества образования.

Рассматривая преступников, совершающих преступления в сфере информационно-телекоммуникационных технологий, видим, что среди них доминирующее положение занимают лица с полным общем уровнем образования – 53%. Далее следует категория лиц, имеющих среднее профессиональное образование – 27%, а на третьем месте по степени криминальной активности находится группа лиц, имеющих неоконченное высшее образование – 19%.

Киберпреступники имеют оконченное среднее специальное образование, некоторые из них имеют профильное образование в сфере информационных технологий и коммуникаций.

Также стоит отметить, что доля трудоспособных, но не трудоустроенных правонарушителей составляет 55%, в то время как 35% заняты неквалифицированным видом деятельности, и лишь 10% -

[12] Дерюшев А.А., Гаврилова О.В. Проблемы, связанные с осуществлением оперативно-розыскных мероприятий в социальной сети Даркнет. В сборнике материалов Межведомственной научно-практической конференции: Деятельность оперативных подразделений: теория и практика. Ленинградская область, 2022. С. 43-46.

трудоустроены на постоянной основе. Трудоустроенные киберпреступники имеют постоянную работу, и кроме того, перспективы карьерного роста, а доходы данных лиц сопоставимы с доходами лиц среднего класса. Результат сравнительного анализа преступлений свидетельствует о том, что лица, которые совершают преступления в сфере информационно-телекоммуникационных технологиях, являются нетипичными представителями общеуголовного преступного мира. Также стоит отметить, что рассматриваемая категория преступников становится на преступный путь осознанно.

Рассматривая вопрос психического развития и здоровья киберпреступников, отмечаем, что свыше 95% указанных лиц не имеют психических отклонений. Из данного факта следует то, что преступления в сфере информационно-телекоммуникационных технологиях совершаются умышленно и тщательно спланированно.[13]

К нравственно-психологическим признакам личности также относят семейное положение преступника. По мнению психологов семья обладает определенным сдерживающим фактором. В ходе многочисленных исследований учеными было установлено, что 82% лиц, которые привлечены к уголовной ответственности не состояли в брачных отношениях, что в свою очередь и обуславливает криминальную активность лиц молодого возраста.

Затрагивая уголовно-правовые характеристики личности, обращаем внимание на то, что из рассматриваемой группы преступников лишь 59% лиц являются несудимыми, в то время как остальные либо были судимы, либо с недавно снятой судимостью. Из данного факта следует вывод о рецидивном характере киберпреступности.

Стоит отметить, что в характеристике структуры личности преступника, совершающего преступления в сфере информационно-

[13] Левгеева Т.Б. Криминалистический анализ личности преступника, совершившего преступление с использованием интернет-технологий // Сборник материалов XXX Международной научной конференции «Исследования молодых ученых». Казань: Молодой ученый, 2022. С. 33-36.

телекоммуникационных технологиях, большое значение имеет преступная мотивация, побудившая совершение общественно опасных деяний. В мир интернет-преступности часто попадают из простого любопытства, чтобы получить навыки и опыт, необходимые для проникновения в сложные виртуальные миры и реализации амбициозных проектов, приносящих большую прибыль. При этом мотивы озорства и хулиганства часто сопровождаются и переплетаются с такими вульгарными мотивами, как месть, злость, жадность, мелочность и алчность. Большинство киберпреступников руководствуются корыстными интересами. Проанализировав проведенные учеными исследования в данной области, видим, что самым малораспространённым мотивом в сфере кибер-преступности являются мотивы мести – 4%, озорство, а также хулиганские побуждения – 5%, исследовательский интерес – 7%, политические мотивы – 17%, и чаще всего в интернет-криминальном пространстве встречаются лица, преследующие исключительно корыстные цели – 67%[14]. Интернет-преступники, реализуя корыстные мотивы в 18,6% случаев успешно распространяли вредоносные программы, посредством которых у других пользователей изымали материальные средства. Совершали преступления в целях безвозмездного получения программного обеспечения (7,1%) либо последующей продажи похищенного программного обеспечения или иной информации (5,7%). В 8,6% случаев преступники преследовали цель получения бесплатного доступа к сети «Интернет», а в 7,1% – к иным техническим каналам связи (например, бесплатного пользования средствами мобильной связи). В 5,7% случаев целью совершения компьютерного преступления выступало манипулирование денежными средствами в электронных системах безналичных расчетов[15].

[14] Мерзлов Ю.А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Вестник Краснодарского университета МВД России. – 2015. – № 4 (30). – С. 116 – 118.

[15] Романова Л.И. Личность интернет-преступника // Азиатско-Тихоокеанский регион: экономика, политика и право. 2018. № 3. С. 159-169.

Также, считаем необходимым, помимо криминалистической характеристики личности преступника рассмотреть особенности криминалистической характеристики посткриминальной деятельности указанных лиц.

При расследовании преступлений в сфере информационно-телекоммуникационных технологиях компетентные органы крайне редко сталкиваются с таким уголовно процессуальным институтом, как явка с повинной. Такое посткриминальное поведение киберпреступников нетипично, так как данные лица убеждены в своей безнаказанности в силу того, что киберпреступления имеют высокую степень латентности.

Рассматривая постпреступное поведение лиц, совершающих киберпреступления, связанные с незаконным оборотом наркотических средств и психотропных веществ, отличительным является то, что зачастую исполнители распоряжаются доходами, полученными преступным путем, в целях приобретения наркотических средств и психотропных веществ в силу того, что зачастую сбытчик является также и потребителем. Если же рассматривать такого участника данных преступлений как организатора, то заметим, что денежные средства, полученные преступным путем данные лица зачастую инвестируют в развитие собственного наркобизнеса.

Так же приметным является то, что при раскрытии преступлений данной категории компетентные органы чаще всего сталкиваются с фактами активного способствования раскрытию и расследованию преступления.

Далее рассмотрим постпреступное поведение лиц, совершающих киберпреступления в сфере экономики. В ходе опроса действующих сотрудников органов внутренних дел, расследующих преступления в сфере информационно-телекоммуникационных технологий установлено, что хакеры 21 века в отличие от своих «коллег» 90-х годов 20 века доходы, полученные преступным путем, вкладывают в движимое и недвижимое имущество. Современные правонарушители инвестируют денежные средства в развитие своего преступного бизнеса. Еще одной немаловажной статьей

расходов с прибыли современных интернет-правонарушители является их личная безопасность и юридическая защита.

Так же при расследовании данной категории преступлений сотрудники органов внутренних дел, как правило, сталкиваются с попытками преступников уклониться от уголовной ответственности, так как данные лица имеют твердое убеждение в трудности доказывания киберпреступлений в сфере экономики, в связи с тем, что у следствия, как правило, доказательной базы довольно мало.

Рассматривая посткриминальное поведение лиц, совершающих преступления против основ конституционного строя и безопасности государства, стоит отметить, что данные преступления совершаются людьми, владеющими особыми навыками, прошедшими подготовку и соответствующее обучение. Интернет-преступники, совершающие рассматриваемую категорию преступлений, противодействуют следствию и пытаются уклониться от уголовной ответственности.

Проанализировав вышесказанное, можно сделать вывод, что типичный преступник, совершающий преступления в сфере информационно-телекоммуникационных технологиях, мужчина в возрасте от 19 до 34 лет, имеющий полное общее образование, трудоспособен, но не трудоустроен, состоящий в брачных отношениях, имеет корыстную мотивацию в совершении правонарушениях.

Типичное посткриминальное поведение киберпреступников выражается в желании преступников уклониться от уголовной ответственности и противодействие расследованию.

1.3 Следовая картина и типичная обстановка на месте совершения преступлений в сфере информационно – телекоммуникационных технологий

«Ничто не берется из ниоткуда и не исчезает в никуда» – данное положение было сформулировано Альбертом Эйнштейном и представляет собой закон сохранения энергии. На наш взгляд данный фундаментальный закон физики имеет отношение и к криминалистике, так как ещё Р.С. Белкин в своих трудах писал: «Каждый преступный акт вызывает изменения в окружающей среде»[16]. Данное высказывание также справедливо и для преступлений в сфере информационно – телекоммуникационных технологий.

Традиционно следы преступления принято делить на идеальные и материальные[17]. Идеальные следы преступления – есть отображение событий в сознании человека. Знания об их свойствах заимствуются из социологии, психологии и других наук. Идеальные следы материализуются через показания потерпевших, свидетелей, и прочих участников уголовного судопроизводства.

В свою очередь, материальные следы преступления представляют собой традиционный объект криминалистического исследования, составляют содержание учения о следах (трасологии), а также включают в себя следы-отображения, следы-предметы и следы-вещества.

По мнению В.А. Мещерякова, стоит дополнить предложенную классификацию, выделяя виртуальные следы, оставленные в ходе совершения компьютерных преступлений[18].

А.Г. Волеводз считает, что «виртуальные следы» представляют собой данные о происхождении информации: таблицы размещения файлов (FAT, NTFS или другие), системные реестры операционных систем, отдельные кластеры магнитного носителя информации, файлы и каталоги хранения

---

[16] Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Российская Е.Р. Криминалистика. Учебник для вузов. Под ред. Заслуженного деятеля науки Российской Федерации, профессора Р. С. Белкина. - М.:Издательство НОРМА - 990 с.

[17] Филиппов А.Г. Криминалистика: учебник. 2-е изд., перераб. И доп. М.: Спартак,2000. С. 73.

[18] Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронежск. гос. ун-т, 2001. С. 74-76.

сообщений электронной почты, файлы конфигурации программ удаленного доступа и иное[19].

В свою очередь В.Е. Козлов утверждает, что «виртуальный след» — это система команд электронно-вычислительной машины, в которой виртуальный объект будет являться следообразующим[20].

Д.А. Соколов в своих научных трудах предлагает разделить цифровые следы на две категории: пассивные и активные. К пассивным следам автор относит информацию об IP-адресе, используемом для доступа к онлайн-ресурсам (например, загрузка или просмотр фотографий на фотохостинге). К активным же - номер телефона или адрес электронной почты, предоставленные для доступа к определенным ресурсам (например, при торговле криптовалютой)[21].

О.Ю. Введенская в своей работе, посвященной данной теме, приводит результат анкетирования сотрудников следственных и оперативных подразделений органов внутренних дел РФ, и приходит к выводу, что современная преступная интернет-деятельность оставляет за собой материальные следы, – так считают 24% опрошенных, идеальные следы в виде показаний потерпевших, свидетелей и подозреваемых (обвиняемых) – 22%, виртуальные следы в виде кэш-файлов, IP-адресов, журналов историй, log-файлов и т.п. – 27% и 27% опрошенных отмечают, что одним из важнейших элементов следственной картины рассматриваемой категории преступлений является информация, оставленная преступниками в сети

[19] Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4.

[20] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия – Телеком, 2002. С. 144.

[21] Соколов, Д.А. Средства анонимизации, цифровые следы. Программный комплекс «Иолай» / Д.А. Соколов. // Оперативно-розыскное противодействие наркопреступности: материалы всероссийского научно-практического семинара / отв. ред. Н.Н. Цуканов [и др.]. – Красноярск: Сибирский юридический институт МВД России (СибЮИ), 2021. – С.51-55.

Интернет, либо как следствие их контакта с жертвой (переписка, фотографии, всевозможные записи и т.п.)[22].

Проанализировав вышесказанное, видим, что следы, образуемые при совершении киберпреступлений, включают как традиционные следы, которые в свою очередь делятся на материальные и идеальные, так и новые, менее изученные криминалистикой следы – виртуальные и информационные. Обращению с виртуальными и информационными следами следует уделять особое внимание из-за их уникальных свойств, которые могут затруднить их обнаружение, фиксацию и изъятие

А.Л. Осипенко подчеркивает, что обнаружение следов киберпреступлений особенно сложно из-за уникальных характеристик сети Интернет. Автор просит уделить особое внимание на тот факт, что следы преступных действий будут распределены по множеству объектов (компьютерная система жертвы, преступника, провайдера, промежуточные сетевые узлы и т.п.)[23].

При обнаружении факта совершения преступления в сфере информационно-телекоммуникационных технологий складывается следующая типичная следственная ситуация: не известно лицо совершившее преступление и не известно из какого места был совершен преступный акт.

И так, будем последовательны и разберемся с местом совершения преступления. Преступления в сфере информационно-телекоммуникационных технологий совершаются дистанционно, а иногда и вовсе имеют трансграничный характер. В соответствии с этим встает закономерный вопрос: что считать местом совершения рассматриваемого вида преступлений?

---

[22] Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. №4 (34). URL: https://cyberleninka.ru/article/n/osobennosti-sledoobrazovaniya-pri-sovershenii-prestupleniy-posredstvom-seti-internet (дата обращения: 01.04.2024).

[23] Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская акад. МВД России, 2009.

Местом совершения преступления в сфере информационно-телекоммуникационных технологий является место совершения лицом действий, входящих в объективную сторону состава преступления[24].

Возвращаясь к вопросу идентификации лица, совершившего преступный акт, стоит отметить, что трудности данного процесса вызваны использованием преступниками средств анонимизации. К современным средствам анонимизации можно отнести следующие:

1. «Приватные» интернет-браузеры (например, TOR, Epic).

«Приватные» браузеры разработаны для минимизации цифрового следа, позволяющего идентифицировать пользователей.

Некоторые из них включают встроенные инструменты маршрутизации. TOR Browser широко используется в преступном мире из-за своей высокой степени анонимности.

2. Сервисы маршрутизации трафика (VPN, Proxy).

И VPN, и Proxy могут перенаправлять трафик, заменяя реальный IP-адрес на IP-адрес сервера, часто расположенного за пределами России.

Ключевое отличие заключается в том, что VPN создает зашифрованный туннель для трафика, что обеспечивает более высокий уровень защиты от посторонних лиц

3. Удаленные серверы и иные виртуальные инфраструктуры (VPS/VDS). Используя эти сервисы, злоумышленники могут хранить компрометирующие данные на удаленном сервере, а не на своем собственном устройстве. Это позволяет им получать постоянный доступ к данным с любого устройства с подключением к Интернету, не оставляя следов на своем собственном устройстве.

4. Интернет-мессенджеры (Telegram, VIPole и др.).

[24] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» // СПС «КонсультантПлюс.

Огромное количество людей ежедневно ведут общение посредствам сети Интернет во всем мире. Однако простые обыватели не задумываются о том, что происходит с сообщением, когда его отправляют, в отличие от правонарушителей, которые при выборе средств общения всегда ориентируются на следующие критерии:

– End-to-end шифрование (E2EE) – тип шифрования «сквозное»;

– степень централизации;

– возможность анонимного использования и регистрации (для регистрации аккаунта не требуются установочные данные, такие как абонентский номер телефона или адрес электронной почты клиента) – например, у мессенджера Pidgin.

5. Интернет-сервисы шифрованной передачи данных (Temp.pm, protonmail.com и др.).

Эти сервисы повышения конфиденциальности дополняют основные инструменты безопасности. Например, "Temp.pm" предлагает самоуничтожающиеся зашифрованные сообщения, которые исчезают после прочтения или по истечении определенного времени. "Protonmail.com" обеспечивает безопасную переписку, защищая содержимое электронных писем сквозным шифрованием.

6. Различные финансовые инструменты (электронные платежные системы, криптовалюта). Финансовые инструменты условно можно поделить на такие категории, как цифровые валюты (далее по тексту – криптовалюты), электронные платежные средства и фиат.

Рассмотренные инструменты анонимизации часто объединяются для повышения секретности, но их использование само по себе оставляет различные цифровые следы.

Таким образом, проанализировав все вышесказанное, можно прийти к выводу, что появление такого явления как киберприступность повлекло за собой дополнение традиционной классификации следов преступлений, к которой добавились цифровые следы. Следственная ситуация же

складывается таким образом: следы преступных действий распределены по множеству объектов, которые в свою очередь зачастую находятся на удаленном расстоянии, отсутствие информации о личности преступника и месте его расположения, в силу использования злоумышленниками средств анонимизации.

ГЛАВА 2. ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

2.1 Тактика производства следственных действий при расследовании преступлений в сфере информационно-телекоммуникационных технологий

Следственные действия являются неотъемлемой частью расследования преступлений. От результатов следственных действий зависит ход расследования и его итог. Для успешного и качественного производства расследования преступлений должностные лица правоохранительных органов используют различные тактики производства следственных действий в зависимости от сложившейся следственной ситуации.

На первоначальном этапе расследования преступлений в сфере информационно – телекоммуникационных технологий ключевое значение имеет производство осмотра места происшествия. Стоит отметить, что важную роль играет неотложность и внезапность производство данного следственного действия, так как информацию, находящуюся в компьютере или ином устройстве, с помощью которого было совершено преступление, можно с легкостью уничтожить.[25]

Перед производством осмотра места происшествия при расследовании преступлений в сфере информационно-телекоммуникационных технологиях следователю необходимо:

1)Установление цели проводимого мероприятия. Основными целями данного следственного действия являются: 1) установление обстоятельств, произошедшего события путем исследования обнаруженных признаков

[25] Балашов Д.Н. Криминалистика: учебник. 2015 (электронный ресурс). URL: https://studref.com/590744/pravo/kriminalistika (дата обращения 24.12.2024).

преступления; 2) выявления, фиксация, изъятие и оценка следов преступления и различных вещественных доказательств; 3) получение информации, необходимой для построения и проверки следственных версий и осуществления розыскной работы по уголовному делу.[26]

2)Решение вопроса о составе участников производства следственного действия.

Ввиду того, что киберпреступления имеют свою специфику, для обнаружения следов преступлений в процессе производства данного следственного действия необходимо наличие специальных знаний в области компьютерных технологий.

Сотрудники, расследующие преступления данной категории, и работники судебной системы зачастую не имеют специальных познаний в сфере информационно-телекоммуникационных технологий, что в свою очередь влечет ошибки в расследовании. Данный тезис можно подтвердить, обратившись к результатам опроса правоохранительных, правоприменительных органов и специалистов сферы IT, проведенного А.А. Протасевичем и Л.П. Зверянской: только 40 % следователей владеют компьютером на уровне обычного пользователя, 40 % не разбираются и не понимают процесс работы компьютера. Так же интересен факт того, что 95% из числа опрошенных программистов считают, что на сегодняшний день без участия профессионала найти нужную, «скрытую» информацию в компьютере без риска её уничтожения довольно сложно.[27]

Привлечение к участию в осмотре места происшествия специалистов и экспертов в области информационно-телекоммуникационных технологий способствует успешному проведению данного следственного действия, затрудняя сообщение ложных сведений, сокрытие важной для расследования

[26] Расследование неправомерного доступа к компьютерной информации: учеб. пособие / под ред. Н.Г. Шурухнов. – 2-е изд. – М.: Моск. ун-т МВД России, 2004. – 352 с.

[27] Протасевич Александр Алексеевич, Зверянская Лариса Павловна Особенности осмотра места происшествия по делам о киберпреступлениях // Baikal Research Journal. 2013. №2. URL: https://cyberleninka.ru/article/n/osobennosti-osmotra-mesta-proisshestviya-po-delam-o-kiberprestupleniyah (дата обращения: 27.01.2024).

информации, к тому же предотвращая должностных лиц от совершения ненужных действия, способствующих уничтожению важных доказательств.

Кроме того, для обеспечения прозрачности и предотвращения необоснованных обвинений в манипуляциях с электронными данными, в качестве понятых при проведении данного следственного действия следует привлекать лиц, обладающих техническими знаниями в области компьютерных технологий. Это позволит гарантировать достоверность и сохранность собранных доказательств.

При проведении данного следственного действия следователь может выбрать один из тактических приемов, в зависимости от расположения следов преступления на месте происшествия: 1) концентрический способ (осмотр ведется по спирали от периферии к центру места происшествия); 2) фронтальный способ (осмотр ведется в виде линейного осмотра площадей от одной их границы к другой); 3) эксцентрический способ (осмотр ведется по спирали от центра к периферии места происшествия).

Центральной точкой осмотра места происшествия, в зависимости от вида этого места, будет признаваться: либо электронный терминал, посредством которого было осуществлено преступление; либо рабочее место, на котором было создано средства совершения преступления.[28]

В протоколе делается запись о расположении компьютера, а также отображается на схеме места происшествия. Так же, указывается «иерархия» соединений, и должны быть установлены способы соединения, такие как, локальные сети, и способы связи компьютеров, такие как, Интернет, а также приборы, посредством которых это происходит. Стоит отметить, что необходимо проверить нахождение компьютера «в сети» или самостоятельная работа, может быть исследован определенный домен. Основная задача следователя – выявить терминал, с которого происходит управление остальными. В дальнейшем необходимо осуществлять

[28] Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь. – 2004. - №7. – С. 4.

последующий осмотр конкретных персональных компьютеров с компьютера-сервера.

Осмотр персональных компьютеров предполагает не только фиксацию выведенной на дисплей информации, но и проверку работы различных компьютерных программ. Следователю необходимо остановить работу компьютерной программы и зафиксировать результат прекращения её работы. Производится осмотр, с указанием в протоколе, о внешних устройствах, присоединенных к компьютеру, например, принтер, веб-камера и иные. Выявляется модель компьютера и его тип, а также внешние устройства ввода и вывода. Подлежит проверке использование запоминающих устройств.[29]

Стоит отметить, что информация, содержащаяся в компьютере, а именно файлы, необходимые для работы операционной системы и файлы с записями о событиях, расположенные в хронологическом порядке, должна обязательно копироваться на внешний жесткий диск. Также обязательной является проверка электронной почты, а также иных программ и мессенджеров, посредством которых происходит онлайн или офлайн общение.

Производится проверка, на присутствие следов пальцев рук, микрочастиц и иных трасологических следов на компьютере, в местах наибольшей вероятности их нахождения, таких как: кнопка включения/выключения компьютера, тачпад или компьютерная мышь и клавиатура. Результаты проверки фиксируются в протоколе следственного действия.

После того, как компьютер со всеми комплектующими устройствами полностью был изучен, например, когда был установлен пароль BIOS при входе в систему, происходит его изъятие. Так же изъятие компьютера происходит в случае, если следователь не имеет возможности скопировать

[29] Савельева М.В., Смушкий А.Б. Криминалистика: учебник / под ред. М.В. Савельева, А.Б. Смушкин. М.,: Издательство Издательский дом «Дашков и К», 2009. С. 226.

информацию на винчестер. При упаковке осматриваемой компьютерной техники фиксируется схема соединений, опечатываются разъемы и кнопки. Компьютер, системный блок, флеш-накопители, диски и иные устройства укладываются раздельно, так как высока вероятность повредить и нарушить их нормальное функционирование. При осмотре электронных документов, устанавливаются их местоположение, время их создания или модификации, а также формат, например, pdf, html, объем файлов. В открытом документе в обязательном порядке изучается содержащаяся информация.

Особое внимание стоит обратить на тот факт, что ошибкой является использование при опечатывании жидкого клея или других веществ, которые могут повредить компьютер. Также необходимо:

1. Выключить компьютер.

2. Отсоединить его от источника питания.

3. Отключить все кабели и разъемы, подлежащие опечатыванию.

4. На бумажную ленту ставятся подписи следователя, специалиста, понятых, и иных участвующих лиц, а также указывается номер. Далее, эта бумажная полоса должна быть приклеена на каждый разъем компьютера. Липкой лентой необходимо нанести таким образом, чтобы снятие такой полосы привело к нарушению ее целостности.

5. Подобным образом необходимо опечатать разъем соединительного провода, указывая на полосе бумаги тот же номер, что и на самом описываемом компьютере.

6. В случае, если полоса бумаги окажется слишком длинной, то возможно ее крепление к боковым поверхностям блоков компьютера или к поверхности стенки, но не задевая другие детали.[30]

В ходе расследования преступлений в сфере информационно-телекоммуникационных технологий особое значение приобретает подготовка к допросам и всестороннее изучение личности допрашиваемого лица.

[30] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: ООО «Издательство «Юрлитинформ», 2001. С. 159-160.

Следователю следует собрать как можно больше информации о допрашиваемом лице в максимально короткие сроки. Для этого необходимо обеспечить получение данных по месту жительства, учебы, работы и досуга лица.[31]

При первоначальных допросах свидетелей и потерпевших необходимо выяснить: назначение и функции компьютерной системы; кто имел доступ к ней и в помещения, где располагалась компьютерная техника, не появлялись ли там посторонние лица, сколько их было, не интересовались ли они сведениями, которые не должны знать; какие средства зашиты использовались; каким образом осуществляется подключение к сети Интернет; какие действия предпринимались для ослабления вредного воздействия или по ликвидации преступных по-следствий; какой вред (имущественный, неимущественный) причинен преступлением и имеются ли способы его уменьшить.[32]

В ходе допросов по делам о рассматриваемых преступлениях, могут быть использованы все известные криминалистике тактические рекомендации.

Допрос свидетелей и потерпевших необходимо начинать с их свободного рассказа обо всем, что им известно по делу. Выслушав свободный рассказ, следователь начинает задавать вопросы.

Основными тактическими задачами допроса потерпевших и свидетелей при расследовании уголовных дел рассматриваемой категории являются:

- выявление элементов состава преступления в наблюдавшихся ими действиях;

[31] Поливанюк В. Особенности проведения допросов при расследовании преступлений, совершенных в сфере использования компьютерной информации. URL: http://www.crime-research.ru (дата обращения: 07.02.2024).

[32] Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учеб. для вузов / под ред. Р.С. Белкина. М.: НОРМА, 2000. С.968.

- Установление обстоятельств, места и времени совершения преступления, способа и мотивов его совершения, а также сопутствующих обстоятельств;

- определение предмета преступного посягательства и размера причиненного ущерба;

- установление других свидетелей и лиц, причастных к совершению преступления.

При подготовке, планировании и проведении допросов подозреваемых и обвиняемых по уголовным делам о компьютерных преступлениях необходимо учитывать специфику составов этих преступлений, особенно субъективную сторону и криминалистическую характеристику личности предполагаемого преступника.

Важным этапом является подготовка к допросу. На данном этапе следователь должен попытаться определить психологический тип подозреваемого или обвиняемого и разработать тактику допроса на основе этого определения.

Целесообразно проводить допрос в помещении, исключающем присутствие посторонних лиц. Перечень конкретных вопросов, подлежащих выяснению, следует формулировать с участием специалиста. Также необходимо подготовить имеющиеся доказательства для их предъявления. Может быть использован и компьютер, подключенный к сети Интернет.

Тактика допроса зависит от сложившейся ситуации: конфликтной, либо бесконфликтной.

В бесконфликтной следователь должен быть готов помочь восполнить подозреваемому информационные пробелы. В конфликтной же - должен быть заранее готовым парировать допрашиваемому, например, предъявив доказательства или известные следствию факты.

В ходе рабочего этапа допроса подозреваемого применяются общие правила допроса:

- выяснение и изучение личности допрашиваемого;

- установление психологического контакта с ним;

- определение отношения подозреваемого к предмету допроса, а также к проходящим по делу лицам;

- готовность скорректировать тактику допроса, так как ситуация может измениться с бесконфликтной на конфликтную и наоборот.

На стадии свободного рассказа используются тактические приемы, направленные на напоминание и формирование мыслительной задачи допрашиваемого. Особое внимание уделяется алгоритмам действий, лежащим в основе сетевых технологий.

Вопросно-ответная стадия включает в себя дополняющие, уточняющие и детализирующие вопросы.

В бесконфликтной ситуации могут быть использованы следующие тактические приемы:

- предложение изложить факты в строгой последовательности;

- предъявление объектов, которые могут способствовать напоминанию;

- предложение обозначить логическую связь между описываемыми обстоятельствами.

В конфликтной ситуации могут быть признаны эффективными:

- разъяснение подозреваемому значимости для него правдивых показаний;

- предупреждение о неотвратимости наказания;

- предъявление доказательств;

- создание у допрашиваемого преувеличенного представления об осведомленности следователя;

- отвлечение внимания;

- демонстрация современных возможностей правоохранительных органов.

В случае совершения преступления группой лиц необходимо также выяснить:

- наличие сговора в груше и кем приходятся друг другу ее члены;

- роль каждого с подробным описанием действий, направленных на совершение преступления;

- какова доля каждого из соучастников, которую он должен был получить в результате совершения преступления (преступлений).

Правдивые показания подозреваемые дают в тех случаях, когда уверены, что следствием установлен круг фактических данных.

По прибытии к месту проведения обыска необходимо быстро и неожиданно войти в обыскиваемое помещение. Зачатую решающим фактором является внезапность обыска. Если получены сведения о том, что компьютеры организованы в локальную сеть, то следует заранее установить местонахождение всех средств компьютерной техники, подключенных к этой сети, и организовать групповой обыск одновременно во всех помещениях, где установлены компьютеры. Перед началом обыска принимаются меры, по предотвращению возможного повреждение или уничтожение информации. Для этого следует обеспечить контроль за бесперебойным электроснабжением, удалить всех посторонних лиц с территории, на которой производится обыск, принять меры по исключению возможности оставшихся лиц прикасаться к средствам компьютерной техники и к источникам электропитания.

Для успешного производства обыска по месту жительства, работы подозреваемого, стоит перекрыть доступ пользователя к персональным компьютерам. В случае, если установлено функционирование программ по ликвидации данных, которые содержатся на компьютере, необходимо незамедлительно выключить компьютер, исключив доступ электропитания.

Экспертизы, назначаемые по уголовным делам о киберпреступлениях, зависят от вида конкретного преступления и определяются в зависимости от следов, подлежащих исследованию.

Очевидно, что наиболее специфичной для рассматриваемой категории уголовных дел является компьютерная экспертиза.

В то же время анализ следственной практики свидетельствует о том, что чаще всего из множества традиционных криминалистических экспертиз проводятся трасологические (67%), почерковедческие, автороведческие (25%), технико-криминалистические экспертизы документов (39%), а из нетрадиционных - психофизиологические экспертизы с использованием полиграфа, медико-психологические и/или психолого-психиатрические экспертизы в отношении лиц, страдающих интернет-зависимостью, комплексные психолого-искусствоведческие (по уголовным делам о незаконном изготовлении, распространении и обороте порнографических материалов или предметов), психологолингвистические (по делам о интернет-преступлениях экстремисткой направленности) и др.[33]

Проанализировав все вышесказанное, приходим к выводу, что фундаментальными следственными действиями при расследовании преступлений в сфере информационно-телекоммуникационных технологий являются: осмотр места происшествия и технических устройств допрос, обыски, конечно, производство экспертиз.

Общие следственные действия по поиску и изъятию средств компьютерной техники и электронных носителей информации в ходе расследования уголовных дел о интернет-преступлениях являются важнейшей и первоочередной задачей следователя. Это связано непосредственно с тем, что информация в электронном виде подвержена быстрой ликвидации или изменению, вследствие чего доказать сам факт события преступления или умысла преступления не будет представляться возможным. Также невозможно будет доказать в некоторых случаях причастность отдельных лиц к совершенному преступлению.

Следственные действия, связанные с производством допроса потерпевших и свидетелей, а также подозреваемого или обвиняемого, являются важнейшей и первоочередной задачей следователя в ходе всего

[33] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. канд. юрид. наук. М., 2016. С. 24-25.

расследования. Это связанно с тем, что при допросах свидетелей и потерпевших следователь получает важную для расследования информацию о событии преступления. Именно хорошо спланированный и проведенный допрос способствует скорейшему расследованию уголовного дела.

2.2 Особенности использования специальных знаний при расследовании преступлений в сфере информационно-телекоммуникационных технологий

Успешное расследование преступлений в сфере информационно-телекоммуникационных технологий зависит от наличия у следователя специальных знаний. В свое время Максим Горький говорил, что нет силы более могучей, чем знание, человек, вооруженный знанием, – непобедим. Однако как было уже сказано ранее, зачастую лицо, расследующее преступления рассматриваемой нами категории, специальными познаниями в сфере информационно-телекоммуникационных технологий не обладает.

Стоит отметить, что специальные знания при расследовании киберпреступлений чаще всего применяются в следующих формах:

1) привлечение специалистов к проведению следственных действий;
2) назначение и производство судебных экспертиз.

Привлечение к участию в следственных действиях специалистов является важной формой применения специальных познаний.

Стоит отметить, что в правоприменительной практике, зачастую возникает проблема, связанная с определением уровня знаний и компетентности специалиста. В криминалистической науке не раз отмечалось, что следователь, имея необходимость произвести осмотр компьютерного оборудования, должен осуществить подбор

соответствующего специалиста и удостовериться в его компетенции. Однако в отечественном законодательстве не установлен процессуальный порядок удостоверения следователя в компетентности специалиста, в том числе обладающего знаниями в области информационно-телекоммуникационных технологий.

Для эффективного решения вопросов в данном направлении необходимо привлекать экспертов, обладающих специальными знаниями в области IT-технологий и специализированного оборудования для обнаружения и сбора цифровых доказательств. Для получения такой информации, в том числе на самом месте происшествия, разработаны специальные программы, позволяющие изучать и документировать цифровые следы.

В настоящее время UFED, XRY и «Мобильный криминалист» являются широко признанными программными комплексами, используемыми в этой области. Основная задача вышеупомянутых систем заключается в их способности эффективно извлекать, восстанавливать и декодировать цифровую информацию с различных устройств, таких как мобильные телефоны, смартфоны, GPS- навигаторы, карты памяти и другие. Цифровые следы (сообщения голосовой почты, фотографии и их геолокация, а также тексты SMS-сообщений) могут быть обнаружены и сохранены. Однако наиболее примечательная особенность заключается в их способности расшифровывать информацию из широко используемых мессенджеров, таких как «WhatsApp», «Viber», «Telegramm», а также извлекать важные данные из облачных хранилищ[34].

На наш взгляд, чтобы работать с цифровыми следами в области компьютерной информации, специалистам необходимо обладать всесторонними научными познаниями и опытом работы в области IT-технологий. Иначе говоря, знать базовые принципы работы компьютеров и

[34] Крякина Т.А. Цифровые следы в криминалистике: понятие и значение в расследовании преступлений // Тенденции развития науки и образования. 2020.

смартфонов, функционирования сетей электронно-вычислительной техники и средств телекоммуникаций, обеспечить безопасность информации, владеть основами электроники и электротехники, микроэлектроники, алгоритмизации и программирования, создания и использования баз и банков данных, технологии функционирования периферийных устройств, проектирования схем, а также владеть методами и инструментами, используемыми при судебной экспертизе компьютерных систем и мобильных устройств.

И. Г. Чекунов утверждает, что специалист, обладающий знаниями в области компьютерной информации, должен отвечать следующим требованиям:

1. иметь опыт управления компьютерами с различными операционными системами (Windows, Linux, MacOS, iOS, Android и т. д.);
2. обладать знаниями в области сетевых технологий (локальные и глобальные сети, сетевое оборудование, сетевые протоколы);
3. обладать навыками реверс-инжиниринга и исследования вредоносного кода;
4. владеть методами компьютерной криминалистики;
5. иметь информированность о правоприменительной практике и криминальных тенденциях в сфере компьютерной информации[35].

Так же следственные действия могут проводиться с устройствами, находящимися как в рабочем, так и в выключенном состоянии, например при задержании подозреваемого лица можно проводить осмотр с работающий техникой, а с выключенной – уже непосредственно в момент фиксации доказательственной информации.

Экспертные знания часто являются востребованными при осмотре

[35] Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учебное пособие / И. Г. Чекунова и др. М.: Московский университет МВД России имени В.Я. Кикотя, 2018. С. 87–88.

места происшествия и иных видов осмотра[36]. Таким образом, деятельность специалиста во время осмотра состоит из следующих мероприятий:

1. выявление наличия соответствующего программного обеспечения (при нахождении компьютера в включенном состоянии);

2. тщательное изучение и описание изображения на мониторе;

3. фото- или видеофиксация изображения и действий специалиста во время осмотра;

4. завершение работы компьютерной программы, оформление хода и результатов осмотра путем протоколирования;

5. установление наличия внешних и периферийных устройств компьютера;

6. отключение сетевого кабеля при включённом сетевом питании по завершении процессуальных действий;[37]

7. копирование необходимых для расследования данных со всех файлов на виртуальных и физических носителях;

8. тщательная упаковка каждого устройства, проводов и кабелей для обеспечения сохранности.

Важно иметь в виду, что в ходе обысков и осмотров можно обнаружить скрытые отпечатки пальцев на клавиатуре, сетевых кабелях, выключателях и других предметах.

При осмотре места преступления, связанного с компьютерными преступлениями, могут быть обнаружены и задокументированы значимые документы, которые впоследствии станут вещественными доказательствами:

Документы, содержащие следы преступления, такие как рукописные тексты, записи, пароли, телефонные счета, банковские реквизиты, которые могут указывать на связь с другими лицами, а также информацию о

[36] Коломинов В.В. Осмотр места происшествия по делам в сфере компьютерной информации / В.В. Коломинов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3. – С. 145-149.

[37] Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И.Г. Чекунов // Право и кибербезопасность. – 2012. – № 1. – С. 9-22.

действиях, совершенных на компьютере или в сети.

Документы со следами печати, которые следует искать в периферийных устройствах (принтерах, сканерах, факсах), а также в бумажных носителях информации, оставшихся в этих устройствах.

Личные документы подозреваемого.

Правила использования компьютера, нормативные акты, инструкции, регламентирующие работу с компьютером и сетью, и могут доказать умысел преступника.

Документы с описанием оборудования или устройств, которые могут подтвердить нелегальное приобретение.[38].

Поиск массивов данных и компонентов программного обеспечения часто требует специальных знаний, поскольку это сложная процедура. В оперативной памяти компьютера может храниться информация о запущенных программах, которая также может быть найдена в оперативной памяти периферийных устройств и различных накопителей. Наиболее эффективным способом фиксации данных, отображающихся на экране монитора, является их распечатка на бумажном носителе.

При неработающем компьютере информация может храниться в почтовых ящиках, на электронных носителях и устройствах, а также в компьютерных сетях. Тщательный анализ этих источников должен проводиться в лабораторных условиях или на рабочем месте следователя со специалистом. Предпочтительно изучать копии, полученные с электронных устройств с использованием копирования данных, а не оригиналы. Для повышения точности следует учитывать скрытые файлы, которые могут содержать ценную информацию, защищенную паролями или кодами. В таких случаях материалы необходимо направлять на декодирование и расшифровку специалистам[39].

---

[38] Еникеев М.И. Следственные действия: психология, тактика, технология: учеб. пособие / М.И. Еникеев, В.А. Образцов, В.Е. Эминов. – М.: Проспект, 2011. – 216 с.

[39] Лантух Э.В., Ишигеев В.С., Грибунов О.П. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации // Всероссийский

По результатам осмотра и фиксации в соответствующих процессуальных документах следователь назначает необходимую экспертизу, определяя виды исследований, выбирая экспертное учреждение и специалиста. При этом выделяются объекты для экспертного исследования и формулируются вопросы, требующие ответов от эксперта.[40].

Объектами компьютерной экспертизы могут быть электронные носители или бумажные документы с текстовой информацией. Следует учитывать, что носителем информации может выступать не только персональный компьютер, но и локальная сеть, а также само место происшествия.

Помимо компьютерной экспертизы следует учитывать традиционные виды экспертиз, которые также могут быть необходимы при расследовании компьютерных преступлений:

1) Дактилоскопическая экспертиза: выявление и исследование следов рук на компьютере, периферийных устройствах и других поверхностях.

2) Техническая экспертиза документов: установление подлинности оттисков печатей, штампов, денежных знаков, ценных бумаг; выявление подделок, подчисток и допечаток.

3) Почерковедческая экспертиза: исследование подписей в документах и ценных бумагах.

Ключевой экспертизой при расследовании компьютерных преступлений является компьютерная экспертиза, которая включает следующие виды исследований:

1) Судебная аппаратно-компьютерная экспертиза: исследование технических средств компьютерной системы, закономерностей ее

криминологический журнал. 2020. №6. URL: https://cyberleninka.ru/article/n/ispolzovanie-spetsialnyh-znaniy-pri-rassledovanii-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 20.03.2024).

[40] Криминалистика: учебник / ред. Е.П. Ищенко. – М.: Проспект, 2020. – 560 с.

эксплуатации и аппаратных средств.

2) Судебная программно-компьютерная экспертиза: исследование программного обеспечения компьютерной системы, его характеристик, алгоритмов и структурных особенностей.

3) Судебная информационно-компьютерная экспертиза (данных): поиск, обнаружение, анализ и оценка информации, созданной пользователем или сгенерированной программами в компьютерной системе.

4) Судебная компьютерно-сетевая экспертиза: исследование функциональных возможностей компьютерных средств, реализующих сетевые информационные технологии.

Данные виды экспертиз получили обоснование и детальное изучение в работах Е.Р. Россинской.[41].

Экспертиза в области высоких технологий и участие специалистов на всех этапах расследования преступлений, связанных с компьютерными технологиями, играют важную роль в поддержке правоохранительных органов. Эти инструменты не только помогают раскрывать и расследовать такие преступления, но и эффективно противодействуют преступной деятельности, в которой информационные технологии являются неотъемлемой составляющей.

[41] Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных пре- ступлений в условиях цифровизации / Е.Р. Россинская // Вестник университета им. О.Е. Кутафина. – 2019. – № 5 (57). – С. 31–44.

ЗАКЛЮЧЕНИЕ

Рост количества преступлений в сфере информационно-телекоммуникационных технологиях в мире и в Российской Федерации с каждым годом увеличивается, при этом уровень раскрываемости преступлений данной категории довольно низок. Это связано с одной стороны с непрекращающимся научно-техническим прогрессом, с созданием новейших способов совершения преступлений в области высоких технологий, с другой стороны с нехваткой квалифицированных кадров правоохранительных органов, а именно их знаний и умений в области информационно-телекоммуникационных технологий.

Исследовав актуальные проблемы данной темы, проанализировав теоретические источники и судебно-следственную практику по преступлениям в сфере информационно-телекоммуникационных технологий, полагаем цель выпускной квалификационной работы достигнута.

Так, в работе выявлено, что компьютерные сети играют важную роль в повседневной жизни. Кибербезопасность зависит от надежной работы компьютеров и сетей в таких задачах, как электронная почта, учет, организационное управление и работа с файлами. Несанкционированное вторжение в сеть может иметь разрушительные последствия, включая финансовые потери и утрату важной информации. Перечень интернет-мошенничеств, который был рассмотрен, не исчерпывает все возможные виды преступлений в сети. С развитием информационно-телекоммуникационных технологий продолжают прогрессировать и преступления в сфере информационно-телекоммуникационных технологий.

Типичный преступник, совершающий преступления в сфере информационно-телекоммуникационных технологиях, мужчина в возрасте от 19 до 34 лет, имеющий полное общее образование, трудоспособен, но не

трудоустроен, состоящий в брачных отношениях, имеет корыстную мотивацию в совершении правонарушениях.

Типичное посткриминальное поведение киберпреступников выражается в желании преступников уклониться от уголовной ответственности и противодействие расследованию.

Появление такого явления как киберприступность повлекло за собой дополнение традиционной классификации следов преступлений, к которой добавились цифровые следы. Следственная ситуация же складывается таким образом: следы преступных действий распределены по множеству объектов, которые в свою очередь зачастую находятся на удаленном расстоянии, отсутствие информации о личности преступника и месте его расположения, в силу использования злоумышленниками средств анонимизации.

Фундаментальными следственными действиями при расследовании преступлений в сфере информационно-телекоммуникационных технологий являются: осмотр места происшествия и технических устройств допрос, обыски, конечно, производство экспертиз.

Общие следственные действия по поиску и изъятию средств компьютерной техники и электронных носителей информации в ходе расследования уголовных дел о интернет-преступлениях являются важнейшей и первоочередной задачей следователя. Это связано непосредственно с тем, что информация в электронном виде подвержена быстрой ликвидации или изменению, вследствие чего доказать сам факт события преступления или умысла преступления не будет представляться возможным. Также невозможно будет доказать в некоторых случаях причастность отдельных лиц к совершенному преступлению.

Следственные действия, связанные с производством допроса потерпевших и свидетелей, а также подозреваемого или обвиняемого, являются важнейшей и первоочередной задачей следователя в ходе всего расследования. Это связанно с тем, что при допросах свидетелей и потерпевших следователь получает важную для расследования информацию

о событии преступления. Именно хорошо спланированный и проведенный допрос способствует скорейшему расследованию уголовного дела.

Не только проведение экспертизы специалистами, имеющими специальные знания в сфере высоких технологий, по уголовным делам, связанным с преступлениями в сфере компьютерных технологий, является серьезной поддержкой, оказываемой правоохранительным органам в борьбе как с данными преступлениями, так и с целым спектром преступлений, в которых информационные технологии выступают частью базы преступной деятельности, но и участие специалиста на всех этапах расследования данных преступлений, а также при проведении всех следственных действий становится залогом успешного раскрытия, расследования и предупреждения данного вида преступлений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты и иные официальные документы

1. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» // СПС «КонсультантПлюс.

2. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 28.04.2023).

Монографии, учебники, учебные пособия

3. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. Учебник для вузов. Под ред. Заслуженного деятеля науки Российской Федерации, профессора Р. С. Белкина. - М.:Издательство НОРМА - 990 с.

4. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учеб. для вузов / под ред. Р.С. Белкина. М.: НОРМА, 2000. С.968.

5. Балашов Д.Н. Криминалистика: учебник. 2015 (электронный ресурс). URL: https://studref.com/590744/pravo/kriminalistika (дата обращения 24.12.2024).

6. Белкин Р.С. Криминалистика. - М.: НОРМА, 2006.-693 с.

7. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: ООО «Издательство «Юрлитинформ», 2001. С. 159-160.

8. Еникеев М.И. Следственные действия: психология, тактика, технология: учеб. пособие / М.И. Еникеев, В.А. Образцов, В.Е. Эминов. — Москва: Проспект, 2011. — 216 с.

9. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия – Телеком, 2002. С. 144.

10. Криминалистика: учебник / ред. Е.П. Ищенко. — Москва: Проспект, 2020. — 560 с.

11. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учебное пособие / И. Г. Чекунова и др. М.: Московский университет МВД России имени В.Я. Кикотя, 2018. С. 87–88.

12. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская акад. МВД России, 2009.

13. Поврезнюк Г.И. Криминалистические методы и средства установления личности в процессе расследования преступлений. По материалам стран СНГ. М., 2005. С. 28.

14. Расследование неправомерного доступа к компьютерной информации: учеб. пособие / под ред. Н.Г. Шурухнов. – 2-е изд. – М.: Моск. ун-т МВД России, 2004. – 352 с.

15. Савельева М.В., Смушкий А.Б. Криминалистика: учебник / под ред. М.В. Савельева, А.Б. Смушкин. М.,: Издательство Издательский дом «Дашков и К», 2009. С. 226.

16. Филиппов А.Г. Криминалистика: учебник. 2-е изд., перераб. И доп. М.: Спартак,2000. С. 73.

17. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. канд. юрид. наук. М., 2016. С. 24-25.

Научные публикации и иные статьи в периодических изданиях

18. Бессонов, А.А. Способ преступления как элемент его криминалистической характеристики/ А.А. Бессонов// Пробелы в российском законодательстве. – 2014. – №4. – С. 171-173.

19. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. №4 (34). URL: https://cyberleninka.ru/article/n/osobennosti-sledoobrazovaniya-pri-sovershenii-prestupleniy-posredstvom-seti-internet (дата обращения: 01.04.2024).

20. Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь. – 2004. - №7. – С. 4.

21. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4.

22. Дерюшев А.А., Гаврилова О.В. Проблемы, связанные с осуществлением оперативно-розыскных мероприятий в социальной сети Даркнет. В сборнике материалов Межведомственной научно-практической конференции: Деятельность оперативных подразделений: теория и практика. Ленинградская область, 2022. С. 43-46.

23. Коломинов В.В. Осмотр места происшествия по делам в сфере компьютерной информации / В.В. Коломинов // Сибирские уголовно-процессуальные и криминалистические чтения. — 2017. — № 3. — С. 145–149.

24. Косенко М.Ю., Мельников А.В. Вопросы обеспечения защиты информационных систем от ботнет атак/ М.Ю. Косенко, А.В. Мельников// Вопросы кибербезопасности. – 2016. – №4(17). – С. 20 – 28.

25. Крякина Т.А. Цифровые следы в криминалистике: понятие и значение в расследовании преступлений // Тенденции развития науки и образования. 2020.

26. Лантух Э.В., Ишигеев В.С., Грибунов О.П. Использование специальных знаний при расследовании преступлений в сфере компьютерной

информации // Всероссийский криминологический журнал. 2020. №6. URL: https://cyberleninka.ru/article/n/ispolzovanie-spetsialnyh-znaniy-pri-rassledovanii-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 20.03.2024).

27. Левгеева Т.Б. Криминалистический анализ личности преступника, совершившего преступление с использованием интернет-технологий // Сборник материалов XXX Международной научной конференции «Исследования молодых ученых». Казань: Молодой ученый, 2022. С. 33-36.

28. Мерзлов Ю.А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Вестник Краснодарского университета МВД России. – 2015. – № 4 (30). – С. 116 – 118.

29. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронежск. гос. ун-т, 2001. С. 74-76.

30. Поливанюк В. Особенности проведения допросов при расследовании преступлений, совершенных в сфере использования компьютерной информации. URL: http://www.crime-research.ru (дата обращения: 07.02.2024).

31. Протасевич Александр Алексеевич, Зверянская Лариса Павловна Особенности осмотра места происшествия по делам о киберпреступлениях // Baikal Research Journal. 2013. №2. URL: https://cyberleninka.ru/article/n/osobennosti-osmotra-mesta-proisshestviya-po-delam-o-kiberprestupleniyah (дата обращения: 20.03.2024).

32. Редькина, Е. А. Анализ личности преступника, совершающего преступления экстремистской направленности в сети "Интернет" / Е. А. Редькина // Трибуна ученого. – 2022. – № 5. – С. 560-565. – EDN TMOMIO.

33. Романова Л.И. Личность интернет-преступника // Азиатско-Тихоокеанский регион: экономика, политика и право. 2018. № 3. С. 159-169.

34. Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях

цифровизации / Е.Р. Россинская // Вестник университета им. О.Е. Кутафина. – 2019. – № 5 (57). – С. 31–44.

35. Сидорова Е.А. Роль следователя в установлении механизма преступления // Следователь сегодня: материалы науч.-практ. конф. Саратов, 2000. С. 42.

36. Соколов, Д.А. Средства анонимизации, цифровые следы. Программный комплекс «Иолай» / Д.А. Соколов. // Оперативно-розыскное противодействие наркопреступности: материалы всероссийского научно-практического семинара / отв. ред. Н.Н. Цуканов [и др.]. – Красноярск: Сибирский юридический институт МВД России (СибЮИ), 2021. – С.51-55.

37. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И.Г. Чекунов // Право и кибербезопасность. – 2012. – № 1. – С. 9–22.

Интернет-ресурсы

38. В Красноярске мошенники обманывают горожан с помощью билетов в театр [Электронный ресурс] // NGS24.ru [сайт]. URL: https://ngs24.ru/text/incidents/2022/07/26/71517146/ (дата обращения: 01.04.2024).

39. Справочная правовая система «Гарант» [Электронный ресурс] // URL: https://www.garant.ru/.

40. Справочная правовая система «Консультант плюс» [Электронный ресурс] // URL: https://www.consultant.ru/.

41. Справочная правовая система «СудАкт» [Электронный ресурс] // URL: https://www. sudact.ru/.

Эмпирические материалы

42. Приговор Пролетарского районного суда г. Твери от 2 декабря 2014 г. по уголовному делу № 1–281/2014. — Текст: электронный // СудАкт: Судебные и нормативные правовые акты РФ. — URL: https://sudact.ru/regular/doc/ShCnL5gPwRmP/. (дата обращения: 01.04.2024).

43. Приговор Соликамского городского суда Пермского края от 9 декабря 2021 г. по уголовному делу № 1-463/2021. — Текст: электронный // Актофакт: Архив судебных дел и решений. — URL: https://actofact.ru/case-59RS0035-1-463-2021-2021-11-16-2-0/. (дата обращения: 01.04.2024).

44. Приговор Чертановского районного суда г. Москвы от 7 сентября 2012 г. по уголовному делу № 1–486/12. — Текст: электронный // СудАкт: Судебные и нормативные правовые акты РФ. — URL: https://sudact.ru/regular/doc/j4eDxuKkqebt/?regular-txt=Попелыши®ular-case_doc=®ular-lawchunkinfo=272+УК+РФ+®ular-date_from=®ular-date_to=®ular-workflow_stage=®ular-area=®ular-court=®ular-judge=&_=1657025602537. (дата обращения: 01.04.2024).