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

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность
специализация № 1 «Оперативно-розыскная деятельность»
узкая специализация «Деятельность подразделений по контролю за оборотом наркотических средств и психотропных веществ органов внутренних дел»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:
Методика расследования преступлений в сфере компьютерной информации

Выполнил:
слушатель группы П 1602
младший лейтенант полиции
Чусов Игорь Андреевич

Решение о допуске к защите:
допущен
Начальник кафедры криминалистики
полковник полиции
_____ Е.Б. Мельников
«23» мая 2021 г.

Руководитель
старший преподаватель
кафедры криминалистики
майор полиции
Поляков Николай Владиславович

Дата защиты:
«21» июня 2021 г.

Консультант
Профессор
кафедры криминалистики
к.ю.н., доцент
Земцова Светлана Игоревна

Оценка: хорошо
Председатель ГЭК

полковник полиции _____ В.В. Скиба
(специальное звание) (подпись) (инициалы, фамилия)

Красноярск 2021

Оглавление

Введение 3

Глава 1. Криминалистическая характеристика преступлений в сфере компьютерной информации 7

1.1. Элементы криминалистической характеристики преступлений в сфере компьютерной информации 7

1.2. Личность типичного субъекта преступления 15

1.3. Типичная обстановка, способы, орудия и следовая картина при расследовании преступлений в сфере компьютерной информации 22

Глава 2. Особенности первоначального этапа расследования преступлений в сфере компьютерной информации 35

2.1. Особенности возбуждения уголовного дела 35

2.2. Типичные следственные ситуации 40

2.3. Тактические особенности производства следственных действий на первоначальном этапе расследования 46

Глава 3. Особенности последующего и заключительного этапов расследования преступлений в сфере компьютерной информации 55

3.1. Особенности производства следственных действий на последующем и заключительном этапах расследования 55

3.2. Возможности судебных экспертиз при расследовании преступлений в сфере компьютерной информации 60

Заключение 64

Библиографический список 67

Введение

Мы живем в век развития технологий и компьютеризации, наука не стоит на месте, а значит появляется новое техническое оснащение, которое становится доступнее для обычного человека. В наше время, почти у каждого дома, на работе, даже при себе имеется компьютер. К данной категории можно отнести и сотовые устройства, которые, практически, заменили компьютер в повседневной жизни, следовательно, все чаще выявляются новые виды преступлений, которые в последнее время совершенствуются.

Компьютерные устройства доступны не только законопослушным гражданам, но и лицам, которые могут использовать указанные средства в преступной деятельности. В Уголовном кодексе РФ преступлениям в сфере компьютерной информации отведена гл. 28, такие преступления принято называть киберпреступления. На наш взгляд, помимо положений, в обозначенной главе, к киберпреступлениям необходимо отнести преступления против собственности, так называемые кибермошенничества, предусмотренные ст. 159.3 («Мошенничество с использованием электронных средств платежа») и ст. 159.6 УК РФ («Мошенничество в сфере компьютерной информации»)[1].

Анализ уголовной статистики свидетельствует о значительной доле зарегистрированных преступлений, предусмотренных ст. 159.6 УК РФ в общей массе преступлений, совершаемых с использованием компьютерной информации.

Общее число зарегистрированных в стране преступлений в 2020 г. увеличилось на 1%, тяжких и особо тяжких – на 14%. Основное влияние на рост тяжких преступлений по итогам 2020 г. оказало увеличение

[1] Проблемы кибербезопасности в России и пути их решения (электронный ресурс). URL: https://www.garant.ru/article/520694/ (дата обращения: 01.04.2021).

количества криминальных деяний данной категории, совершенных с использованием информационно-телекоммуникационных технологий.

В отчетном периоде число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети Интернет – на 91,3%, при помощи средств мобильной связи – на 88,3%.

По данным ведомственной статистики в России в период с января по декабрь 2020 года, количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации составило 510396, при этом направленных в суд с обвинительным заключением – 82977 преступлений. Проблемой остается большое количество не раскрытых преступлений в данной сфере, в 2020 г. их было 379830, что показывает актуальность выбранной нами темы исследования[1].

В целях своевременного документирования данной преступной деятельности и получения необходимой доказательственной базы в отношении лиц, их совершивших в 2001 г. в структуре МВД России создано специализированное подразделение – Управление «К» БСТМ МВД России.

Актуальность выбранной темы исследования также обуславливается имеющимися недостатками в деятельности органов внутренних дел по расследованию и раскрытию преступлений в сфере компьютерной информации, выражающимися в недостаточно оперативном реагировании сотрудников полиции на указанные преступления, а также в неполном и некачественном проведении первоначальных следственных действий, что приводит к отсутствию или неполноте собранной информации.

Исходя из вышеизложенного, объектом исследования выступают с одной стороны, преступная деятельность по совершению

[1] Данные официального сайта МВД России. URL: http://мвд.рф (дата обращения: 01.04.2021).

киберпреступлений, а с другой стороны деятельность по расследованию и раскрытию таких преступлений.

Предметом исследования выступают закономерности деятельности преступников и причастных к преступлениям в сфере компьютерной информации лиц, а также закономерности деятельности правоохранительных органов по раскрытию и 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 компьютерной информации и определить проблемные аспекты, возникающие в ходе расследования уголовных дел по выбранной теме.

Исходя из поставленной цели, автором работы выделены следующие задачи:

1. Проанализировать теоретические источники о расследовании преступлений в сфере компьютерной информации;

2. Рассмотреть судебно-следственную практику о расследовании преступлений в сфере компьютерной информации;

3. Изучить элементы криминалистической характеристики преступлений в сфере компьютерной информации;

4. Определить особенности возбуждения уголовного дела по факту совершения преступления в сфере компьютерной информации;

5. Раскрыть типичные следственные ситуации и тактические особенности производства следственных действий, возникающих при расследовании преступлений в сфере компьютерной информации.

Для достижения поставленных задач были использованы следующие методы:

1. Общенаучные и частнонаучные методы познания – анализ, синтез, классификация;

2. Практические методы научного исследования – сравнение, эмпирический метод.

Теоретической основой исследования являются труды ученых-криминалистов: В.К. Гавло, И.Е. Мазурова, Н.В. Олиндер, А.Г. Филиппова, Н.Р. Шевко, А.В. Шмонина, Н.П. Яблокова и др.

Нормативно-правовой базой выпускной квалификационной работы послужили Конституция РФ, Уголовно-процессуальный кодекс РФ, Уголовный кодекс РФ, Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации».

Эмпирическую базу научного исследования составили: аналитические материалы МВД России, практика судебных органов общей юрисдикции, правоприменительная практика органов внутренних дел.

Теоретическое значение исследования состоит в научном и практическом анализе, обобщении, систематизации и расширении общетеоретических знаний и представлений о методике расследования киберпреступлений.

В результате проведенного исследования автором сформулированы выводы и предложены рекомендации по обнаружению, фиксации и изъятию следов преступления, а также по производству следственных действий: осмотра места происшествия, обыска компьютерного оборудования и информации, относящихся к расследуемому событию, а также допрос потерпевшего, свидетелей и подозреваемых, назначению компьютерно-технических и иных судебных экспертиз.

Структурно выпускная квалификационная работа состоит из введения, трех глав, состоящих из восьми параграфов, а также заключения и библиографического списка.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1. Элементы криминалистической характеристики преступлений в сфере компьютерной информации

Законодатель объединил компьютерные преступления в главу 28 Уголовного кодекса РФ, именуемую «Преступления в сфере компьютерной информации». Настоящая глава состоит всего из четырех статей: неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274); неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1).

В аспекте компьютерных преступлений, затрагивается лишь та информация, которая была размещена на магнитном носителе, в электронно-вычислительных машинах либо в их сети, системе[1].

Однако уголовный закон включает более 10 составов, которые в качестве квалифицирующего признака содержат позицию об их совершении с использованием информационно-телекоммуникационных технологий (далее – ИКТ). К ним в частности относят: ст. 110 УК РФ (Доведение до самоубийства); ст. 171.2 УК РФ (Незаконные организация и проведение азартных игр); ст. 185. 3 УК РФ (Манипулирование рынком); ст. 242 УК РФ (Незаконные изготовление и оборот порнографических

[1] Шаталов А.С. Пархоменко А.Н. Криминалистическая характеристика компьютерных преступлений (электронный ресурс). URL: http://www.crime-research.ru/library/Shatal.htm (дата обращения: 01.04.2021).

материалов или предметов); ст. 280 УК РФ (Публичные призывы к осуществлению экстремистской деятельности) и др.

Кроме указанных выше составов преступлений, к преступлениям, совершаемым с использованием ИКТ, следует также отнести составы, которые указаны в гл. 21 УК РФ «Преступления против собственности», в частности: ст. 158 УК РФ (Кража); ст. 159 УК РФ (Мошенничество); ст. 159.3 УК РФ (Мошенничество с использованием электронных средств платежа); ст. 159.6 УК РФ (Мошенничество в сфере компьютерной информации).

Объект компьютерных преступлений – информация, а действия преступника рассматриваются как покушение на информационные отношения общества.

Объективную сторону компьютерных преступлений и, в частности, преступлений, совершаемых в телекоммуникационных сетях, образует как действие, так и бездействие, связанное с нарушением прав и законных интересов по пользованию информацией, находящейся в телекоммуникационной сети. По конструкции объективной стороны киберпреступления имеют материальный состав преступления. Существенный вред может быть причинен правам и законным интересам личности, обществу или государству такими действиями либо бездействием, вместе с тем, состав преступления, предусмотренного ч.1 ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ), формальный, что является исключением из выше обозначенного. Уголовным законом преступные последствия определяются применительно к конкретным видам киберпреступлений. Причинно-следственная связь всегда устанавливается между деянием и наступившим последствием.

Субъективная сторона киберпреступлений, а также преступлений, совершаемых в телекоммуникационных сетях, характеризуется умышленной виной.

Субъект киберпреступления общий – физическое вменяемое лицо, достигшее 16 лет. Помимо этого, в преступлениях, предусмотренных ч. 3 ст. 272, ч. 2 ст. 273, ч. 4 ст. 274.1 УК РФ и др. предусмотрен специальный субъект, а именно лицо, совершившее изучаемое деяние с использованием своего служебного положения.

Всего же разделяют 9 основных видов киберпреступлений:

1. Операции с поддельными картами.

2. Снятие денежных средств с помощью средств электронного банкинга.

3. Операции с украденными / утерянными картами.

4. Многократная оплата услуг и товаров.

5. Мошенничество с интернет заказами и магазинами.

6. Многократное снятие со счета.

7. Мошенничество с использованием подложных слипов.

8. Мошенническое использование банкоматов при выдаче наличных денег.

9. Подключение электронного записывающего устройства к POSтерминалу / банкомату (skimming).

10. Другие виды мошенничества[1].

Дискуссионным в науке остается вопрос о понятии и содержании криминалистической характеристики преступлений. Так, в своих научных трудах Н.П. Яблоков указывает, что криминалистическая характеристика преступлений есть не что иное, как система, при которой описываются криминалистически значимые признаки преступления, которые окажут

[1] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Методические рекомендации по предупреждению, пресечению, раскрытию и расследованию преступлений, совершенных с использованием высоких технологий и коммуникаций: учебное пособие / Н.Р. Шевко, Е.Э. Турутина, В.В. Панченко, А.М. Каримов. Казань: КЮИ МВД России, 2016. С. 16-17.

помощь в раскрытии, расследовании совершенного преступлений, а также его предупреждении[1].

В понимании В.С. Бурдановой, криминалистическая характеристика преступления – это комплекс данных или сведений, которые были выявлены путем анализа и особых исследований[2].

Таким образом, проанализировав вышесказанное, под криминалистической характеристикой преступления понимают систему типичных признаков, зависящих от вида преступления, а знание этих признаков прямо способствует решению задач, стоящих перед следователем.

Элементы криминалистической характеристики киберпреступлений стандартны, к ним относятся: предмет преступного посягательства, способ, орудия, следы преступления, личность преступника, личность потерпевшего, типичная обстановка совершения преступления.

Однако для преступлений, совершаемых в телекоммуникационных сетях, характерны некоторые особенности: множество предметов и средств преступления; объект преступного посягательства неоднороден; телекоммуникационная информация проявляется в качестве объекта и средства преступного посягательства; ИТКС выступает или в качества предмета, или средства совершения преступления[3].

Предметом кибермошенничества признается чужое имущество или право на него, а предмет киберпреступлений, указанных в гл.28 УК РФ, является компьютерная информация, средства защиты такой информации; программное обеспечение; компьютерные технологии.

---

[1] Яблоков Н.П. Криминалистическая характеристика преступлений и типичные следственные ситуации как важные факторы разработки методики расследования преступлений / Вопросы борьбы с преступностью. – 1979. – № 30. – С. 121.

[2] Бурданова В.С. Криминалистическая характеристика преступлений, связанных с незаконным оборотом наркотиков // Прокурорско-следственный работник. –1998. – №3. – С. 7.

[3] Алексеров В.И., Колокольчикова О.Н. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации: учебно-практическое пособие / В.И. Алексеров, О.Н. Колокольчикова. М.: ВИПК МВД России, 2016. С. 48.

В примечании 1, ст. 272 УК РФ изложено понятие компьютерной информации, под которой законодатель понимает сведения, вне зависимости от средств хранения, обработки и передачи таких данных, которые сформированы в электрические сигналы[1]. Идентичное понятие закреплено Федеральным законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»[2].

Ратифицированное РФ в 01.10.2018 г. соглашение «О сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации» закрепляет понятие компьютерной информации, определяющееся «как информация на машинном носителе в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети»[3]. На основании вышеизложенного можно сделать вывод, что понятие «компьютерная информация нуждается в усовершенствовании и модернизации, поскольку, термина «электронно-вычислительная машина» неактуален, является пережитком прошлого в веке непрерывного зарождения ранее неизвестных носителей компьютерной информации (чипы, смартфоны, устройства, содержащие микропроцессоры).

Кроме того, предметом компьютерных преступлений является и оборудование, обеспечивающее информационно-телекоммуникационные процессы. Истории известны факты использования Интернета для разжигания «цветных революций» в ряде стран мира. Так, американскими и израильскими спецслужбами в 2010 г. был создан сетевой компьютерный

[1] Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ // СПС «КонсультантПлюс».
[2] Об информации, информационных технологиях и защите информации: федеральный закон от 27.07.2006 г. №149-ФЗ // СПС «КонсультантПлюс».
[3] О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: федеральный закон от 01.10.2008 г.№ 164-ФЗ // СПС «КонсультантПлюс.

червь для кибератак, послуживших стартом к дезорганизации работы оборудования по обогащению урана в Иране[1].

Стоит отметить, что выявлены определенные факторы, которые способствуют совершению киберпреступлений, к ним относятся: слабый уровень программного обеспечения; высокая вероятность незаконного доступа или преобразования компьютерной информации, а также недостаточный контроль за доступом к информации; безграмотность и пренебрежительное отношение к мерам предосторожности при использовании электронных средств платежа и Интернета и др.[2]

Преступления, затрагивающие компьютерную информацию и телекоммуникации можно разделить на 2 категории:

1. Преступления, связанные с вмешательством в работу ЭВМ;

2. Преступления, совершаемые с использованием ЭВМ.

Основные виды преступлений, связанных с противоправным вмешательством в работу компьютеров:

— Незаконный доступ к компьютерной информации;

— Создание и распространение вредоносных компьютерных программ (вирусов), а также их ввод в программное обеспечение;

— Преступная небрежность в несоблюдении правил эксплуатации компьютерной техники и систем;

— Хищение, уничтожение, подделка компьютерной информации.

Основные виды преступлений, совершаемых с использованием ЭВМ (преступления, в которых компьютер является средством достижения цели):

---

[1] Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминалистическая классификация и квалификация киберпреступлений // Право и кибербезопасность. – 2012. – № 1. – С. 11.

[2] Центр исследования проблем компьютерной преступности. Криминалистическая характеристика компьютерных преступлений (электронный ресурс). URL: http://www.crime-research.ru/library/Shatal.htm (дата обращения 01.04.2021).

— Выработка различных математических моделей, при которых входными данными служат условия реализации преступления, а выходными будут служить предложения по выбору наилучшего варианта действий субъекта преступления.

— Преступления с общим названием – «воздушный змей» (вид преступлений с использованием компьютера, когда деньги переводятся из одного банка в другой постепенно повышающимися необеспеченными суммами, затем крупная сумма быстро снимается и владелец счета исчезает).

Также важно отметить личность потерпевшего, так как она играет немаловажную роль при расследовании компьютерных преступлений. Зачастую, потерпевшими суд признает именно юридических лиц, в связи с тем, что они являются активными пользователями компьютерных систем и программ.

Второй группой потерпевших являются лица, пользующиеся услугами юридических лиц, на которых были совершены кибератаки. Так, например, в феврале 2020 г. Урицким районным судом п. Нарышкино рассмотрено уголовное дело №1-1-4/2020 в отношении М., который скачал программу, предназначенную для сканирования открытых портов Интернет оборудования провайдера Филиала в Брянской и Орловской областях ПАО «…», и получения списка интернет-оборудования, подключенного к ИТКС «Интернет». После чего, М., используя указанную программу, для получения доступа к ИКТС «Интернет» на более высокой скорости передачи данных, посредством персонального компьютера и интернет-оборудования компании получил доступ к интернет-оборудованию пользователя У. Затем М. скопировал логин и пароль для доступа в ИТКС Интернет, относящиеся к билинговой системе старт-IP, и являющиеся коммерческой тайной. После чего, неправомерно ввел полученные учетные данные в виде логина и пароля на своем интернет-оборудовании, тем

самым осуществил неправомерный доступ к компьютерной информации, что привело к блокированию доступа к ИКТС «Интернет» указанного пользователя и модификации, выразившейся в изменении данных об интернет-оборудовании, времени его использования и месте его нахождения у оператора связи, причинив своими действиями вред деловой репутации этого филиала[1].

Третьей группой потерпевших обычно признают лиц, которые пострадали от действий «компьютерных пиратов», которые осуществляют кражу лицензионной компьютерной продукции, нейтрализуя ее защиту и распространяя ее в сети Интернет бесплатно либо за определенную плату.

Так, например, в сентябре 2017 г. Красноярским краевым судом рассмотрено уголовное дело № 22-5203/2017 в отношении Т., который разместил объявление об оказании им услуг, а именно установление программного обеспечения за денежное вознаграждение в сумме 1000 рублей и договорившись с лицом, действовавшим в рамках оперативно-розыскного мероприятия «Проверочная закупка», Т. установил указанное программное обеспечение. Для установки контрафактного программного продукта, правообладателем которого является корпорация «Майкрософт», Т. скопировал из сети Интернет на имеющийся у него компакт-диск установочные пакеты операционной системы, и на USB flash-накопитель программу-активатор, созданная для несанкционированной правообладателем регистрации и активации вышеуказанного программного продукта. Использование указанной программы-активатора приводит к невозможности реализации программных средств защиты программного обеспечения, с целью ликвидации установленных производителем

[1] Приговор Урицкого районного суда п. Нарышкино от 11 февраля 2020 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

технических ограничений, связанных с защитой авторского права от незаконного использования программного обеспечения[1].

Таким образом, законодателем закреплены преступления в сфере телекоммуникаций и компьютерной информации в гл. 28 УК РФ, а также в иных главах УК РФ. Под криминалистической характеристикой преступлений понимают систему типичных признаков, зависящих от вида преступления, а элементами криминалистической характеристики киберпреступлений являются предмет, способ, орудия и следы преступления, а также личность преступника, потерпевшего и типичная обстановка совершения преступного деяния. Предметом кибермошенничества признано чужое имущество, а иных киберпреступлений – компьютерная информация, средства защиты такой информации; программное обеспечение; компьютерные технологии. Потерпевшими от данного вида преступлений могут быть физические и юридические лица, что подтверждается анализом судебной практики. Далее некоторые элементы криминалистической характеристики будут раскрыты более подробно.

1.2. Личность типичного субъекта преступления

Следы личности преступника содержат в себе любые преступления. Это и социально-психологические качества личности, и специальные знания, возраст и т.д. В достаточно тесной взаимосвязи с личностью

[1] Апелляционное постановление Красноярского краевого суда от 26 сентября 2017 года (электронный ресурс). Режим доступа URL: https://sudact.ru (дата обращения: 01.04.2021).

человека, совершившего преступления находится характер и вид совершенного им преступления.

Зачастую лиц, совершающих киберпреступления объединяют в следующие группы:

1) Лица, у которых трудовой договор с организацией-жертвой не заключен, однако имеют другого рода отношения с нею;

2) Работники организации, занимающие ответственные должности;

3) Работники организации, злоупотребляющие своим служебным положением.

К лицам, совершающим киберпреступления относят:

1) Граждан, которые пользуются компьютером и имеют специальную подготовку и доступ к компьютерной сети;

2) Программисты, IT-специалисты, лица, производящие ремонт и обслуживание компьютеров и их сетей;

3) Мотрудники юридических лиц и учреждений, использующие в своей работе компьютер[1].

Можно выделить характерные черты личности типичного киберпреступника, так данные лиц о поле указывают, что мужчинами совершаются киберпреступления от 86 до 92% случаев, а вот доля женщин варьируется от 4,8 до 12,2%. Интересным представляется, что в последнее время наблюдается динамика доли женщин в совершении данных преступлений, по причине использования компьютерной техники в работе (секретари, делопроизводители, бухгалтер, кассир и др.) Зачастую можно столкнуться с случаями пособничества женщин при совершении рассматриваемых преступлений.

Рассматривая научные труды, касающиеся возраста киберпреступников, наблюдается отсутствие единой точки зрения в их

[1] Центр исследования проблем компьютерной преступности. (электронный ресурс). URL: http://www.crime-research.ru/library/Shatal.htm (дата обращения:01.04.2021).

классификации. В целом, большую часть киберпреступников составляют лица мужского пола от 16 до 48 лет.

А.С. Лакомов классифицирует субъектов компьютерных преступлений по следующим группам:

1) 18-24 лет (39,6%);

2) 25-29 лет (30,6%);

3) от 50 лет и старше (3% преступников).

Полагаем, что столь низкий процент преступников, совершивших киберпреступления в возрасте старше 50 лет обусловлен отсутствием умений в пользовании компьютером и информационными технологиями[1].

Однако, ряд авторов полагают, что верхнего возрастного предела у компьютерных преступников не существует и предлагают классифицировать их на две возрастные группы:

1) с 14-20 лет;

2) с 21 и старше[2].

Подобной позиции придерживается С.В. Баринов, утверждая, что возраст и пол не являются значительными препятствиями в освоении технологий, используемых при совершении преступных деяний рассматриваемой группы и приводит в своих трудах в пример уголовное дело, возбужденное в отношении 63-летней гражданки С., жительницы г.Улан-Удэ[3].

---

[1] Лакомов А.С. Киберпреступность: современные тенденции // Академическая мысль. – 2019. – №2 (7). – С. 55.

[2] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий: учебно-практическое пособие / А.В. Шмонин, Е.А. Ефремова, В.В. Баранов, А.В. Казюлин. М.:АУ МВД России, 2016. С. 34.

[3] Баринов С.В. Криминалистическая характеристика личности преступника, совершающего преступные нарушения неприкосновенности частной жизни в киберпространстве (электронный ресурс). URL: https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-lichnosti-prestupnika-soveshayuschego-prestupnye-narusheniya-neprikosnovennosti-chastnoy (дата обращения: 01.04.2021).

Следует отметить, киберпреступники в основной своей массе обладают достаточно высоким уровнем образования. Примерно треть осужденных за преступления в сфере компьютерной информации имеют диплом о высшем образовании или же не окончили Вуз, но обучались в нем, и более 37% преступников получили средне специальное образование[1]. Столь высокий образовательный уровень субъектов исследуемых преступлений обусловлен потребностью в знаниях и умениях в сфере высоких технологий и программирования, а иногда и базовыми знаниями использования техники.

Профессионалы в области компьютерных преступлений являются наиболее опасной группой преступников, поскольку около 80% всех киберпреступлений совершены непосредственно ими. Зачастую такие преступления являются хищениями денежных средств в особо крупном размере. Такие профессионалы обладают высшим экономическим, техническим или юридическим образованием. Наиболее характерные черты такой группы субъектов преступления: владение программированием, сокрытие следов преступления, отличные знания и умение использования современной техники и др.[2].

Род занятий киберпреступников: учащиеся, работающие, временно безработные. Ю.А. Мерзлов в своем исследовании указывает, что 52% киберпреступников обладали особой подготовкой в сфере автоматизированной обработки компьютерной информации. 97% преступников – это работники государственных и иных организаций, пользующиеся в своей работе информационными технологиями и компьютером[3].

---

[1] Лакомов А.С. Указ. соч. С. 55.
[2] Мерзлов Ю.А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. – 2015. – № 4 (7). – С. 60.
[3] Там же. С. 58.

Субъекты изучаемых нами преступлений являются представителями всех социальных слоев населения. Превалирующее большинство преступников это рабочие (23,4%) и служащие (более 14%). Киберпреступники достаточно часто совершают много эпизодов преступлений и, в основном, не привлекаются к уголовной ответственности. Однако отмечается, что более 4% преступников имеют неснятую или непогашенную судимость, а около 3% – рецидивисты[1].

В редких случаях на практике можно столкнуться с групповыми преступлениями в сфере высоких технологий. Зачастую, исполнителем признается квалифицированный специалист в сфере IT-технологий, а соучастниками являются как профессиональные хакеры, так и террористы, педофилы, и мошенники[2].

Характеризуя киберпреступников, исследователями наблюдается ряд свойств и особенностей поведения таких как: склонности к точным наукам; повышенный интерес к абстрактным видам искусства, фантастике и нетрадиционным религиозным учениям; хорошее знание английского языка; им характерен свободолюбивый и эгоцентричный характер; их сопровождает семейная неустроенность и холостяцкий образ жизни; заинтересованности в поддержании порядка в доме и его обустройстве такие лица не имеют; центральное место жилья – комната, в которой находится компьютер[3].

Наиболее характерными мотивами лиц, совершающих компьютерные преступления, можно считать: корыстные, хулиганские, политические, игровые, исследовательский интерес, потребность в самоутверждении,

[1] Лакомов А.С. Указ. соч. С. 56.
[2] Головинов О. Н, Погорелов А. В. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. – 2016. – № 6 (1). – С. 81.
[3] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Указ. соч. С. 32.

месть, мотивы, связанные с психическими отклонениями[1]. Мотивы преступлений несовершеннолетних зачастую являются исследовательский интерес, самоутверждение и жажда славы, они редко участвуют в групповом преступлении. С развитием социальных сетей информация о частной жизни граждан, размещаемая там, все чаще становится объектом преступных посягательств и в этой связи, распространенным мотивом является ревность со стороны близких и знакомых пострадавших[2].

Молодое поколение, зачастую совершает преступления в области подделки лицензионных соглашений и мелкие мошенничества, а взрослые лица вторгаются и незаконно используют личные данные и совершают преступления, при которых причиняется более тяжкий ущерб потерпевшим.

Специалисты подразделяют лиц, совершающих такие преступления на несколько категорий:

1. Хакеры. Попытки защитить гражданами и организациями компьютерную систему негативно воспринимается ими на свой счет, и удовлетворяя свои амбиции, они взламывают систему и иногда продают полученные данные.

2. Хактивисты. Побуждающим мотивом к совершению киберпреступлений такими лицами является социальный протест и хакерство.

3. Корыстные киберпреступники. Преследуют имущественные выгоды при совершении преступлений.

4. Так называемые «шпионы». Они занимаются вскрытием данных компьютеров для того, чтобы в дальнейшем полученные незаконным путем

---

[1] Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Среднерусский вестник общественных наук. – 2014. – № 1 (31). – С. 119.

[2] Поляков В.В., Попов Л.А. Особенности личности компьютерных преступников // Известия Алтайского государственного университета. – 2018. – №6 (104). – С. 258.

сведения можно было использовать в военных, экономических и политических целях.

5. Террористы. Лица, использующие сведения, полученные в результате взлома компьютерных систем, для дестабилизации и запугивания общества.

6. Вандалы. Преследуют при совершении киберпреступлений цель разрушения компьютерных систем.

7. Лица, обладающие различными психическими отклонениями и заболеваниями, в том числе, компьютерными фобиями и информационными болезнями[1].

Также целесообразно рассмотреть профили преступников, в области высокий технологий:

1. Кодеры. Высококвалифицированные программисты, специализирующиеся на вирусных программах, программах, рассылающих спам и др.

2. Дропы. Важное звено в цепочке лиц, совершающих киберпреступления. Эти лица трансформируют добытую незаконным путем информацию о логинах и PIN-кодах в денежные средства. Их деятельность для них достаточно рисковая, поскольку эти лица обналичивают денежные средства и после отдают их заказчику.

3. Подростковая киберпреступность, характеризующаяся тем, что несовершеннолетние интересуются созданием фишинговых страниц и кардингом, черпая информацию на просторах Интернета, в котором проводят все свое свободное время.

4. Провайдеры, предоставляющие услуги мошенникам. Так, в сети Интернет существуют, так называемые, «абузоустойчивые хостинги», при

[1] Яблоков Н.П. Криминалистика: учебник / отв. ред. Н.П. Яблоков. М.: ЛексЭст, 2006. С. 354.

которых имеется возможность размещения незаконных сайтов и защита собственников таких сайтов от контроля правоохранительных органов[1].

Рассмотрение особенностей личности киберпреступников и систематизация полученных знаний – важная криминалистическая задача, которую требуется осуществлять на регулярной основе в связи с высокой динамикой преступности в этой сфере, что будет способствовать раскрытию и расследованию таких преступлений, и окажет помощь в их криминалистическом предупреждении.

На основании вышеизложенного, можно сделать вывод, что типичным преступником, совершающим киберпреступления, в основном является лицо мужского пола в возрасте от 18 до 40 лет, житель города, имеющий средне специальное, незаконченное или оконченное высшее образование, учащийся, работающий или временно безработный, ранее не судимый, владеющий навыками работы с персональным компьютером, являющийся активным пользователем сети Интернет, не женатый, замкнутый и эгоцентричный человек.

1.3. Типичная обстановка, способы, орудия и следовая картина при расследовании преступлений в сфере компьютерной информации

Важнейшую роль при совершении любого преступления играет обстановка совершения преступления. В науке криминалистике последнюю рассматривают в широком и узком смыслах.

[1] Миронов С.Н. и др. Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации, предусмотренных статьей 159.6 Уголовного кодекса Российской Федерации: методические рекомендации / С.Н. Миронов и др. Казань: КЮИ МВД России, 2017.С. 15.

Так, в широком смысле обстановка совершения преступления – комплекс социальных, политических, экономических, правовых и иных условий, образующихся на конкретном этапе развития общества и воздействующих на динамику преступности. А в узком смысле – совокупность факторов, которые влияют на взаимосвязь объектов, различных процессов между собой и описывают условия времени, места, производственные процессы, отличительные черты поведения участников происшествия и иные обстоятельства объективной реальности, которые возникли в момент преступления и оказывающие воздействие на механизм совершения преступления[1].

Как часть криминалистической характеристики, обстановка совершения преступления имеет важное значение для киберпреступлений. Грамотная оценка обстановки способствует:

— определить отличительные черты личности киберпреступника, а также способе совершения преступления;

— обнаружить следовую информацию;

— предпринять меры по розыску и задержанию киберпреступников;

— выявить обстоятельства, оказавшие воздействие на ход и итог преступления;

— установить обстоятельства, которые благоприятствовали совершению преступления[2].

Обстановку совершения преступлений в сфере высоких технологий характеризует несоответствие места совершения преступления и места наступления общественно опасных последствий. Место данного преступления состоит из двух элементов: местонахождение в действительности, т.е. фактический или юридический адрес нахождения

[1] Волохова О.В., Егоров Н.Н., Жижина М.В. и др. Криминалистика: учебное пособие / под ред. Е.П. Ищенко. М.: Проспект, 2011. С. 170.
[2] Там же. С. 170.

лица, и местонахождение, идентифицируемое в глобальной или локальной сети с IP-адресом[1]. Также местом совершения данного вида преступлений, на наш взгляд, могут являться различный интернет-кафе либо места, где имеется точка доступа выхода в Интернет, что в наше время дает преступникам больше возможностей совершать данные преступления, скрываясь при этом. К тому же появляется больше устройств, дающих доступ к сети Интернет и по своему функционалу не уступающие обычному стационарному компьютеру.

Изучаемые нами преступления совершаются в виртуальном кибернетическом пространстве, главной особенностью, которой является, что единовременно в преступлении возможно использование нескольких компьютеров, которые могут быть расположены не только в разных помещениях, но и городах, и странах[2].

Таким образом, обстановка совершения компьютерных преступлений требует углубленного изучения и исследования, поскольку этот вид преступления еще мало изучен, а обстановка преступления является важным элементом криминалистической характеристики, отражающего деятельность участников события и механизм преступного деяния.

Достаточно большим объемом криминалистически значимой информации можно охарактеризовать способ совершения преступления. Дифференциация способов компьютерных преступлений условна, поскольку они могут быть взаимосвязаны друг с другом. Проанализировав научные труда по данной теме, можно выделить ряд способов совершения данных преступлений.

---

[1] Олиндер Н.В. Время и место совершения преступления как элемент криминалистической характеристики преступлений, совершенных с использованием электронных платежных средств и систем // Вестник Самарского государственного университета. – 2014. – №11-1. – С. 91.

[2] Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. – 2013. – №2. – С.114.

Кардинг – жаргонное наименование преступлений с использованием платежных карт. Характеризуется противоправным использованием самих карт или информации о них, которая не была дана владельцем карты[1]. Действия преступников могут осуществляться с помощью оплаты за товары в Интернет-магазинах либо путем перевода денег на другие счета, а также путем использования POS-терминалов при оплате за товары или оказанные услуги, либо имитируя оплату[2]. Так же известны случаи использования платежных карт для оплаты в традиционных торгово-сервисных предприятиях либо снятие денежных средств в банкомате по подложным картам. Следует отметить, что до массового перевода карт на чиповые технологии, копировались данные магнитной полосы карты и производилась кража PIN-кода, цель которой – последующее изготовление подделки. Занимаясь кардингом, есть возможность собрать информацию о действующей карте лица, или сформировать эти данные. Не секрет, что любой человек может легко отыскать сайты, продающие сведения о банковских платежных картах.

Фишинг – это способ совершения киберпреступления, целью которого признается доступ к конфиденциальной и охраняемой законом информации владельца банковской карты, к сведениям, составляющим банковскую тайну[3]. Необходимые данные передает сам владелец карты. Для этого используются компьютерные программы, которые предназначены для противоправного уничтожения, изменения, копирования компьютерной информации либо нейтрализации средств защиты компьютерной системы. В отличие от кардинга, банковская карта участия не принимает, ее данные попадают к преступникам посредством

---

[1] Кредитки в руках кибермошенников. (электронный ресурс). URL: https://www.sravni.ru/text/2010/9/9/kreditki-v-rukah-kibermoshennikov/ (дата обращения: 01.04.2021).

[2] Приговор Кировского районного суда г. Саратова от 9 августа 2016 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

[3] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 9.

Интернета. При этом создаются фишинговые (поддельные) страницы, имитирующие официальные сайты банков, платежных сервисов или магазинов, меняются в названии несколько букв или знаков.

Так, например, в ноябре 2018 года Верховным судом Республики Марий Эл рассмотрено уголовное дело № 22-783/ 2018 в отношении Б. и Л., которые отправляли абонентам смс-сообщения от банка со ссылкой на вирус. Когда абонент заходил по ссылке, программа начинала зависать, а Л. получал доступ к мобильному банку абонента и осуществлял перевод денежных средств на банковские карты. После этого Д. сообщал Ю., на какие банковские карты перечислены денежные средства, а последний обналичивал их в банкоматах. Примечательно, что суд первой инстанции верно классифицировал их одиннадцать эпизодов преступления по ч. 2 ст. 273 УК РФ и неверно как кражу по ст. 158 УК РФ, а апелляционным постановлением суд переквалифицировал действия Б. и Л. на ч. 2 ст. 159.6 УК РФ[1].

Изучая такое преступление как кибермошенничество, предусмотренное ст. 159.6 УК РФ, необходимо указать, что лицо приобретает право на имущество, при совершении данного преступления, несколькими способами: посредством ввода, уничтожения, блокирования и изменения компьютерной информации, а также путем иного вмешательства в работу средств хранения, обработки и передачи информации.

Относительно новым способом собирания преступниками конфиденциальной информации признается вишинг – это «голосовой» фишинг, осуществляемый путем мобильной телефонной связи[2]. Так, в письме или смс-сообщении обозначается ситуация, к примеру, противоправное снятие денежных средств с карты, для разрешения которой необходимо связаться с сотрудником банка по телефону. Ответить

[1] Апелляционное постановление Верховного Суда Республики Марий Эл от 26 ноября 2018 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).
[2] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 9.

на звонок может как автоответчик, так и человек. Цель - заставить назвать идентификационные данные. Возможна и другая схема вишинга, когда на телефон жертвы звонят с «проверкой службы безопасности», указывая, что при отказе ее прохождения, карту заблокируют или произойдут иные неблагоприятные для владельца карты последствия. В ходе такой проверки нужно сказать данные, которые придут в СМС. Находясь под влиянием субъекта преступления, владельцы карт дают всю информацию, даже ту, которую нельзя сообщать даже сотрудникам банка[1].

Так, например, в августе 2013 г. Курагинским судом рассмотрено уголовное дело № 1-564/2013, в отношении И., согласно которому на номер телефона потерпевшей пришло смс - сообщение о том, что ее банковская карта заблокирована, и всю информацию она может получить по указанному в смс номеру телефона. Позвонив на указанный номер, ей ответила И., представившись работником банка и пояснила, что произошел сбой в системе, и банковская карта заблокирована, в связи с этим, нужно предоставить сведения для разблокирования карты (паспортные данные и номера банковской карты), а позже с ее карты уже была снята денежная сумма в размере 15029 руб. И., выполняя отведенную ей роль в хищениях имущества владельцев банковских карт в 16 эпизодах, передавала информацию неустановленному участнику преступлений, который в свою очередь, платил ей за это от 1 000 до 2 000 рублей за день работы, и используя Интернет, осуществлял незаконное подключение банковских карт потерпевших к абонентским номерам оператора сотовой связи и через платежную систему совершал переводы денежных средств. Таким образом, суд посчитал, что достаточных доказательств виновности

[1] Что такое фишинг в сети, какую цель он преследует, и как защититься? (электронный ресурс).URL: https://stolohov.com/poleznye-stati/chto-takoe-fishing-v-seti.html#i-15 (дата обращения: 01.04.2021).

подсудимой в совершении преступлений, предусмотренных ч. 3 ст. 272 УК РФ не имеется, и признал ее виновной по ч. 2 ст. 159 УК РФ[1].

М.В. Лелетова рассматривает 2 способа мошенничества. Первое направлено на завладение денежными средствами (сбережениями) граждан, в том числе их средств, находящихся на счетах кредитных учреждений (банков). Второе направлено на хищение денег, которые находятся на счете мобильного телефона клиента в учреждениях сотовой связи. При совершении данных преступных посягательств средство сотовой связи используется как устройство, посредством которого осуществляется удаленных контакт с потерпевшим[2].

Яркими примерами первого способа является схема, при которой лицо, как правило, уже отбывает наказание в исправительном учреждении ФСИН России, звоня на телефоны, в основном женщинам преклонного возраста, представляется сотрудником правоохранительных органов, охранником и т.д., сообщает о совершении членом их семьи правонарушения и предлагает заплатить деньги для решения вопроса об освобождении его от ответственности или возмещения ущерба[3]. Некоторые авторы именуют этот способ, как «просьба о помощи»[4].

Другим примером будут являться мошеннические действия, направленные на завладение денежными средствами потерпевшего, так, под видом выигрыша лотереи, потерпевшему отправляется смс-сообщение на мобильный телефон, жертве сообщается о том, что лицо выиграло приз

---

[1] Приговор Курагинского городского суда от 22 августа 2013 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

[2] Лелетова М.В. Особенности расследования преступлений, совершаемых с использованием средств сотовой связи // отчет о НИР (заключительный) / сост. М.В. Лелетова. Нижний Новгород: НА МВД России, 2015. С. 14.

[3] Приговор Калининского районного суда г. Челябинска от 23 декабря 2014 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

[4] Яджин Н.В., Егоров В.А. Особенности расследования корыстных преступлений, совершаемых с использованием средств сотовой связи // отчет о НИР (заключительный) / сост. Н.В. Яджин, В.А. Егоров. Тюмень: ТИПК МВД России, 2016. С. 11-12.

(например, автомобиль, телевидеоаппаратуры или техники), одновременно предлагая заплатить налог за выигранный приз, указывая номер счета в банке[1].

Так, в ноябре 2019 г. Воркутинским городским судом рассмотрено уголовное дело № 1-278/2019, в отношении Л., который путем набора цифр случайных абонентских номеров отправлял СМС сообщения, о том, что владелец абонентского номера стал победителем розыгрыша и обладателем денежного сертификата в размере 129 000 рублей, все подробности предлагалось узнать по абонентскому номеру, указанному в сообщении. После того как потерпевший перезванивал, Л. представлялся сотрудником компании «Мобайл Телеком» и предлагал для получения им денежного приза оплатить налоговый сбор или же пополнить потерпевшим счет своего абонентского номера на определенную сумму[2].

Примерами второго способа мошенничества являются:

1. Снятие денег со счета клиента по его команде, например, предлагается подключить услугу за определенную плату или вовсе бесплатно либо оформить подписку бесплатно, но впоследствии данная услуга все-равно оказывается платной. При этом списание денежных средств производится периодически, в незначительной сумме, вместе с тем регулярно.

2. Генерирование пин-кодов для карт экспресс-оплаты. Абонентам предлагают чудо-программу, генерирующую коды карточек экспресс-оплаты за мобильную связь. Нередко программу присылают, и она оказывается ничем иным, как генератором случайных чисел. В данной ситуации потерпевший не обращается в ОВД, поскольку сам пытался совершить обманные действия, направленные на пополнение баланса своего сотового средства связи.

---

[1] Лелетова М.В. Указ. соч. С. 15.

[2] Приговор Воркутинского городского суда от 21 ноября 2019 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

3. Мобильные приложения – опустошители баланса. Абонент скачивает на wap-сайте небольшое приложение, например, порно-слайдшоу, которое в процессе своей работы само незаметно для абонента посылает SMS-ки на платные номера. Изготовитель приложения же получает свое партнерское вознаграждение у контент-провайдера, владельца короткого номера. Зачастую контентпровайдер может и не знать о том, что его партнеры занимаются мошенничеством[1]. Встречаются и другие виды обманов в сети Интернет[2].

Хищение может совершаться как со счетов граждан, привязанных к банковским картам, так и не привязанных к ним. Хищению, как правило, предшествуют действия, связанные с неправомерным получением сведений о счетах, данных клиента, размере средств, находящихся на счете, сроке действия, номере и CVV2 или CVC2-коде банковской карты (в отношении карт)[3]. Эти сведения могут быть получены так же путем неправомерного доступа к базе данных банка сотрудником банка и использования соответствующих сведений для совершения преступления[4].

Широко известна стала информация о кибермошенничестве и способах его совершения, в связи с чем был придуман новый вид мошенничества – фарминг. Это процесс скрытого перенаправления на фейковые IP-адреса в сети Интернет жертв этого преступления. При фарминге, используется компьютер собственника банковской карты, на который размещается вирусная программа «троян», при этом сам собственник не замечает этих действий. Этот способ компьютерных преступления возможно осуществить на DNS-сервере интернет провайдера

---

[1] Мобильный контент. Новый вирус для мобильных телефонов (электронный ресурс).URL: http://www.procontent.ru/news/4864.html (дата обращения: 01.04.2021).
[2] Лелетова М.В. Указ. соч. С. 16-17.
[3] Петраков С.В, Миронов И.А., Карнаухов О.Г., Попов А.А. Раскрытие и расследование мошенничеств, связанных с неправомерным доступом к компьютерной информации и списанием денежных средств с расчетных счетов граждан // ответ о НИР (заключительный) / сост. С.В, Петраков и др. СПб: СПбУ МВД России, 2016. С. 8.
[4] Приговор Кировского районного суда г. Омска от 26 декабря 2019 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

собственника карты. Кибермошенники погружают потенциальных жертв в чувство полной уверенности пользования услугами конкретного банка. Владелец платежной карты, вводя банковские реквизиты, автоматически перенаправляется на официальный сайт банка[1].

По уголовному делу от 7 сентября 2012 года № 1-486/2012, рассмотренного Чертановским районным судом г. Москвы, П. и П. приобрели комплекс вредоносного программного обеспечения типа «Троян». Для обеспечения массового посещения пользователями приобретенного Интернет-ресурса и заражения их компьютеров они воспользовались услугами неустановленных лиц, которые за вознаграждение организовали скрытное перенаправление пользователей на зараженный П. сервер. В ходе исполнения вредоносного кода компьютерной программы, происходило изменение или подмена служебного файла операционной системы персонального компьютера пользователя сети Интернет (клиента Банка). В результате любое обращения клиентов Банка к веб-сайту банка перенаправлялось на ip-адреса серверов, принадлежащих субъектам преступления, с расположенной там поддельной веб-страницей. В базу данных указанной веб-страницы без согласия обладателей информации, копировались аутентификационные данные, а именно УНК, пароли и переменные коды клиентов Банка, являющихся обладателями сведений, совокупность которых определена, как аналог их собственноручной подписи и признается в качестве однозначного и бесспорного подтверждения платежа[2].

Следующим способом являются Бот-сети – сети в зараженных компьютерах. Такой бот-компьютер задействуется мошенниками для отправки спама и совершения кибератак. Вирусная программа для

[1] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 10.

[2] Приговор Чертановского районного суда г. Москвы от 7 сентября 2012 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

заражения компьютера устанавливается незаметно для его пользователя на каждый компьютер бот-сети[1]. Например, правоохранительными органами в 2012 г. были задержаны члены организованной группы, которые создали группу бот-сетей, основу которых составляла программа «троян», именуемая «Оригами». Практически все боты находились на территории России[2].

Скимминг – это один из разновидностей мошенничества с платежными картами, предполагающий использование разнообразных приборов типа скиммер. Скиммеры ни что иное, как устройство, устанавливаемое на банкомат для незаконного копирования информации с банковской карты. К скиммерам относятся накладные клавиатуры, закрепляемые на клавиатуре банкомата и практически невидимые обычному пользователю видеокамеры[3].

Так, например, в марте 2015 г. рассмотрено уголовное дело №1-54/2015 Заельцовским районным судом г. Новосибирска, в отношении Х. и Л., которые на картоприемник банкомата установили техническое устройство «скиммер», при прохождении через которое с магнитных полос на встроенный носитель информации считывается информация об индивидуальных цифровых свойствах банковских карт, а также на корпус банкомата установили техническое устройство «планка» со скрытой видеокамерой и носителей информации для видеофиксации последовательности набора на клавиатуре банкомата цифровых символов пин-кодов с сохранением видеоданных. Х. и Л. признали виновными в совершении преступлений, предусмотренных ч.3 ст. 183, ч.3 ст. 272, п. «а» ч. 2 ст. 158, ч.3 ст. 30 п. «в» ч.3 ст. 158 УК РФ[4].

---

[1] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 10.
[2] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Указ. соч. С. 68.
[3] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 10.
[4] Приговор Заельцовского районного суда города Новосибирска от 24 марта 2015 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

Современные технологии, стали подспорьем для усовершенствования вышеизложенных устройств, в связи с чем появился новый способ совершения преступления – шимминг. В данном случае, используются более тонкие и гибкие компьютерные платы, которые вставлены субъектами преступления в отверстие для приема пластиковых карт банкомата, при этом происходит считывание данных этих карт. Толщина платы и волоса человека одинакова (0,1 мм). Отличием шимминга от скимминга является большая визуальная незаметность первого[1]. В наши дни единственной эффективной защитой от шимминга является использование чиповых пластиковых карт[2].

Таким образом, были раскрыты лишь некоторые способы совершения киберпреступлений, которых в науке криминалистики исследовано достаточно много. Полагаем, что с непрерывным научно-техническим прогрессом, вскоре мы будет сталкиваться со все новыми изощренными способами совершения данных преступлений.

Орудием является любой предмет, используемый лицом для совершения преступления. Основными орудиями при совершении изучаемых преступлений являются: компьютерная техника, средства сотовой связи, специальное оборудование, например, скиммер.

Определенные особенности имеет следовая картина компьютерных преступлений, которые выражаются в неосновном значении материальных следов (следов рук, ног). Главные следы киберпреступлений – это различного рода информация на магнитных носителях, например, специальные компьютерные программы, алгоритмы, пароли и коды и др. Достаточно трудным, а иногда и вовсе нереальным представляется идентификация пользователя компьютера по следам, которые остались на

[1] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 11.
[2] Способы совершения компьютерных преступлений (электронный ресурс). URL: http://csaa.ru/sposoby-sovershenija-kompjuternyh-prestuplenij/. (дата обращения: 01.04.2021).

магнитных носителях. Актуальным направлением в науке криминалистике является разработка экспертных методов работы с такой группой следов[1].

На основании вышеизложенного можно сделать вывод, что обстановку совершения преступлений в сфере высоких технологий характеризует несоответствие места совершения преступления и места наступления общественно опасных последствий, а само место преступления характеризуется местонахождением в реальном пространстве и IP-адресом. Изучая различные научные труды, автором работы были выделены часто встречающиеся на практике способы совершения компьютерных преступлений, как: кардинг, фишинг, вишинг, фарминг, ботнет, скимминг и иные. Анализируя судебную практику по выделенным в данном параграфе способам, можно отметить, что большинство преступников узнают о самих способах совершения преступлений, о различных преступных схемах и устройствах на форумах сайтов сети Интернет от неустановленных лиц, которые могут выступать соучастниками преступлений и исходя из практики, так и остаются ненайденными. К орудиям совершения данных преступления относят: компьютерную технику, средства сотовой связи либо специальные устройства и приборы. Необходимо отметить, что важные следы преступлений в сфере высоких технологий закрепляются в виде информации на магнитных носителях, а вот второстепенное значение будут иметь следы рук и ног.

Наука не стоит на месте, появляются и совершенствуются технические средства, и способы, которые злоумышленники могут использовать в преступных целях, для получения имущественной выгоды, либо для нанесения ущерба репутации гражданина, юридического лица или государственной безопасности.

---

[1] Центр исследования проблем компьютерной преступности. Криминалистическая характеристика преступлений. (электронный ресурс). URL: http://www.crime-research.ru/library/Shatal.htm (дата обращения 01.04.2021).

ГЛАВА 2. ОСОБЕННОСТИ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1. Особенности возбуждения уголовного дела

Возбуждение уголовного дела – базовая стадия уголовного процесса: своевременность, профессионализм и слаженность действий правоохранительных органов на данной стадии определяют результативность и эффективность решения совокупности задач, которые стоят перед уголовным судопроизводством.

Трудности в раскрытии преступлений, совершенных при помощи компьютерных технологий, заключаются в использовании субъектами преступления различных способов сокрытия своих преступных действий.

В своих трудах И.Е. Мазуров утверждает, что расследование киберпреступлений, а также успешность его исхода обусловлены незамедлительными действиями по принятию решения о начале предварительного расследования. Грамотный подход и организация действий следователя, приводит к положительным результатам расследования уголовного дела. При проведении расследования, можно столкнуться с некоторыми сложностями, например, достаточно трудно исследовать начальную доказательную базу. Важно вовремя предпринять действия по возбуждению обоснованного уголовного дела. Зачастую именно затягивание и откладывание начала производства расследования

вызывает скорую потерю основных доказательств и приводит к безнаказанности киберпреступников[1].

Согласно ст. 144 УПК РФ, любое сообщение о совершенном или готовящемся преступлении подлежит проверке. Главная задача процессуальной проверки состоит в уяснении наличия или отсутствия в преступном деянии признаков состава преступления.

Сотрудники правоохранительных органов, в рамках установленной законом компетенции, при наличии определенного в законе повода и при достаточности оснований, решают вопрос о возбуждении уголовного дела. Принятие решения о возбуждении уголовного дела оформляется постановлением. На основании изложенного, можно сделать вывод, что для того, чтобы принять законное и обоснованное решение о возбуждении уголовного дела нужно два элемента: повод и основание[2].

Основанием для возбуждения уголовного дела признаются сведения подтверждающие наличие определенных признаков киберпреступления. Нередко это объективные признаки преступления. Поводами для возбуждения уголовных дел, касающихся компьютерных преступлений признаются:

1) заявления о совершенном киберпреступлении;

2) выявленные сотрудниками правоохранительных органов признаки преступления:

— По итогам проведения проверки в связи с поступившей информацией о готовящемся или уже совершенном преступлении, переданной оперативными работниками;

---

[1] Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: диссертация (электронный ресурс). URL: https://рюи.мвд.рф/upload/site138/document_file/MAZUROV_I.E._Dissertaciya_2017.pdf (дата обращения: 01.04.2021).

[2] Трубачинов А.В. Особенности возбуждения уголовного дела и планирования на первоначальном этапе расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ // Вестник Волгоградской академии МВД России. – 2019. – №1 (48). – С. 153.

— Во время производства специальных оперативно-технических мероприятий;

— По итогу исследования документальных и иных проверок;

— При задержании лица на месте преступления с поличынм.

3) выявленное сотрудниками правоохранительных органов признаков преступления при расследовании других преступлений;

4) новостные сводки, в том числе в сети Интернет о конкретных случаях нарушения прав граждан киберпреступниками[1].

Именно заявления потерпевших о совершенных преступлениях зачастую и являются поводами для возбуждения уголовных дел[2].

С теоретической точки зрения возможна и явка с повинной лица, совершившего компьютерное преступление, но на практике следователи с этим практически не сталкиваются[3]. Данный вывод подтверждается и в работе Е.С. Шевченко, где при исследовании вопроса об источнике информации о совершенном киберпреступлении, опрашиваемые респонденты указали, что явка с повинной источником информации по киберпреступлениям не является[4].

На этапе проверки заявления возможно проведение различных действий, в том числе осмотр места происшествия. Целью следственных действий на стадии проверки будет являться обнаружение криминалистических признаков киберпреступления и фиксация и изъятие следов преступления, а также выявление круша лиц, которые подлежат в дальнейшем допросу.

---

[1] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ соч. С. 28-29.
[2] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Указ. соч. С. 126.
[3] Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий: конспект лекций. (электронный ресурс). URL: http://procuror.spb.ru/izdanija/2007_02_02.pdf (дата обращения: 01.04.2021).
[4] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: диссертация (электронный ресурс). URL: https://www.msal.ru/common/upload/SHevchenko_E.S.pdf(дата обращения: 01.04.2021).

В процессе предварительной проверки необходимо отыскать такие факты как: была ли нарушена целостность информации компьютера, системы или сети; наступили ли вредные последствия в результате совершения преступления; необходимо определить причинно-следственную связь между противоправными действиями и наступившими последствиями; каков размер причиненного ущерба[1].

В ходе проверки заявлений потерпевших или иной информации о совершенном киберпреступлении, стоит определить: время несанкционированного доступа в компьютер и его сети, и компьютерную информацию; местонахождение информации, которая была подвергнута кибератаке; время, место формирования, пользования и распространения вредоносной компьютерной программы; способы и средства совершения несанкционированного проникновения или нарушения правил эксплуатации компьютера, а также последствия таких действий; способы преодоление компьютерной защиты информации; данные о субъекте преступления[2].

В процессе проверки поступивших заявлений и к моменту возбуждения уголовного дела следователю необходимо подготовить ряд документов, например, рапорт сотрудника об обнаружении признаков преступления; документы, касающиеся эксплуатации компьютера и его системы; данные сотрудников, осуществляющих оперативно-розыскную деятельность и иные[3].

Помимо всего прочего, необходимо организовать взаимодействие следователя с Управлением «К» МВД России, а также, немаловажно консультироваться со специалистами в данной области, а именно с

---

[1] Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий: конспект лекций. (электронный ресурс). URL: http://procuror.spb.ru/izdanija/2007_02_02.pdf (дата обращения: 01.04.2021).

[2] Там же.

[3] Филиппов А.Г. Криминалистика: учеб. пособие, 2014. (электронный ресурс). URL: https://studme.org/90885/pravo/osobennosti_vozbuzhdeniya_ugolovnogo_dela_tipichnye_situatsii_pervonachalnogo_etapa_rassledovaniya_deystv (дата обращения: 01.04.2021).

работниками организаций, имеющих высокий уровень квалификации и работающих в области компьютерных технологий.

Так, предпочтение необходимо давать сотрудникам Федеральной службы по техническому и экспортному контролю; экспертам, специализирующимся на судебных компьютерно-технических экспертизах; работникам служб безопасности, в том числе информационной; сотрудникам учебных учреждений и исследовательских заведений[1].

Типичными ошибками, которые совершаются следователями на изучаемой стадии расследования дела признаются не выяснение достаточных обстоятельств преступления, утеря письменных и вещественных доказательств, различные технические ошибки и др. Так, например, следственное управление МВД по Нижегородской области сообщило о факте дублирования уголовных дел по одному факту хищения, поскольку гражданин может подать несколько заявлений в разные государственные подразделения. Подобного рода недостатки и ошибки непосредственно влияют на объективность, полноту и качество предварительного следствия[2].

Помимо этого, выделяют и такие проблемные аспекты как: низкий уровень доследственной проверки. В материалах проверок зачастую отсутствуют объяснения лиц, на которых зарегистрированы абонентские номера и IP- адреса, и их данные вообще. Также, проблемой является и поведение заявителей, которые, например, стремятся преодолеть преступные действия своими силами, иногда удаляют вредоносные программы и ссылки на их источник. Помимо этого, отмечается и

[1] Илюшин Д.А. Особенности возбуждения уголовных дел о преступлениях, совершаемых в сфере предоставления услуг «Интернет» // Вестник Самарского государственного университета. – 2007. – №1 (51). – С. 16.
[2] Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Указ. соч. С. 120-121.

недостаточная материально-техническая обеспеченность подразделений ОВД компьютерной техникой необходимого технического уровня[1].

Таким образом, стадия возбуждения уголовного дела не случайно признана фундаментальной стадией уголовного процесса. Любая поступившая информация о киберпреступлении должна подлежать проверке, а для принятия обоснованного и законного решения о возбуждении уголовного дела по факту совершения преступления, в сфере компьютерных технологий, обязательны повод и основание. Следователь изучает необходимую информацию и материалы, а также находит наиболее приемлемый момент для возбуждения дела, устанавливая характер и последовательность первоначальных следственных действий, организационных и других мероприятий. При расследовании изучаемых преступлений, следователю стоит консультироваться с опытными специалистами в сфере IT-технологий. Этап возбуждения уголовных дел по киберпреступления включает в себя совокупность особенностей и определенных сложностей. На мой взгляд, ряд трудностей связан с моментом совершения преступления, так как потерпевший не всегда может заметить факт совершенного в отношении него преступления.

2.2. Типичные следственные ситуации

Следственная ситуация – это основополагающий элемент тактико-криминалистического обеспечения деятельности следователя в процессе расследования преступлений. Следует отметить, что понятие следственной

[1] Зайцев А.А., Смолин А.В. Типичные следственные ситуации, складывающиеся при расследовании киберпреступлений // Актуальные проблемы криминалистики и судебной экспертизы: Материалы междунар. науч.-практ. конф. Восточно-Сибирский институт МВД РФ, – 2020. – С. 53-54.

ситуации является дискуссионным, однако общепринятое определение звучит так – совокупность условий, в которых в данный момент осуществляется расследование, т. е. та обстановка в которой протекает процесс доказывания[1].

В.Я. Карлов указывает, что следственная ситуация – это существующая в данный момент реальность, те условия, в которых действует следователь[2].

Ряд ученых считает, что следственная ситуация это совокупность фактических данных, отражающие черты события[3]. В настоящее время широко используется определение указанное Т.С. Волчецкой, которая определила следственную ситуацию как степень информационной осведомленности следователя о преступлении, а также состояние процесса расследования, сложившееся на любой определенный момент времени, анализ и оценка которого позволяет следователю принять наиболее целесообразные по делу решения[4].

Первоначальный этап расследования характеризуется работой с информацией, а именно ее восприятие, анализ, систематизация и др., и на основании переработки имеющейся информации выдвигаются версии, определяются задачи расследования, следователь принимает решения, организует их выполнение и осуществляет контроль за исполнением всеми участниками процесса.

С учетом комплекса исходной информации, полученной при проведении проверочных действий, на первоначальном этапе

---

[1] Зайцев А.А. Смолин А.В. Указ. соч. С. 52.

[2] Карлов В.Я. Криминалистика: тезаурус-словарь и схемы // учебное пособие./ В.Я. Карлов. М.: Альфа-Пресс, 2011. С.36.

[3] Гавло В.К. О следственной ситуации в методике расследования хищений, совершенных с участием должностных лиц // Вопросы криминалистической методологии, тактики и методики расследования. М., 1973. С. 90.

[4] Волчецкая Т.С. Криминалистическая ситуалогия: монография / Т.С. Волчецкая. М.; Калининград, 1997. С. 93.

расследования могут складываться следующие типичные следственные ситуации:

1. Установлен неправомерный доступ к компьютерной информации, есть следы, есть подозреваемый, который дает правдивые показания.

2. Установлен неправомерный доступ к компьютерной информации, имеются следы, прямо указывающие на конкретного подозреваемого, но он отрицает свою причастность к совершению преступления.

3. Установлен неправомерный доступ к компьютерной информации, известны лица, совершившие преступление, но обстоятельства доступа не установлены.

4. Установлен факт неправомерного доступа к компьютерной информации, совершить который и воспользоваться его результатами могли только лица из определенного круга (по своему положению, профессиональным навыкам и знаниям), либо известны лица (фирмы, организации), заинтересованные в получении данной информации. Последняя следственная ситуация является наиболее сложной, поскольку отсутствуют сведения о виновном лице, следы преступления, неизвестен способ совершения преступления и др.[1]

В независимости от ситуации, анализ исходной информации осуществляется на основе обобщения имеющихся в материале сведений о криминалистических признаках, указывающих на совершение киберпреступления. Так, признаками являются: сбои в работе ЭВМ, системе ЭВМ или локальной вычислительной сети собственника или правообладателя; уничтожение, блокирование, модификация или копирование компьютерной конфиденциальной информации; утрата значительных массивов информации или баз данных; необычные проявления в работе ЭВМ: замедленная или необычная загрузка операционной системы, замедление работы машины с внешними

[1] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 27.

устройствами, неадекватные реакции ЭВМ на команды пользователя и пр.; копии чужих файлов в файловой системе правообладателя; файлы с вредоносными программами; наличие программного обеспечения подбора паролей для неправомерного доступа в Интернет либо иного проникновения в компьютерные сети, а также содержащего функции по уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; внесение в конструкцию компьютера встроенных устройств, дополнительных жестких дисков, устройств для расширения оперативной памяти, считывания оптических дисков и т. д.; наличие нестандартных периферийных устройств; изменения в оперативном запоминающем устройстве, зафиксированные при задержании подозреваемого с поличным в момент работы на компьютере при совершении неправомерного доступа к компьютерной информации; улики поведения подозреваемого; другие признаки. Анализируя указанные признаки, следователь выдвигает общие и частные типовые версии[1].

На основании вышеуказанных типичных следственных ситуаций на первоначальном этапе расследования преступлений рассматриваемого вида можно выделить следующие общие версии:

1. Состав преступления отсутствует, поскольку происшедшее событие является следствием непреодолимых факторов (самопроизвольный сбой в работе программных или аппаратных составляющих средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, сетей электропитания и связи, средств защиты информации; выход из строя машинного носителя информации по

[1] Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий: конспект лекций. (электронный ресурс). URL: http://procuror.spb.ru/izdanija/2007_02_02.pdf (дата обращения: 01.04.2021).

причине естественного износа и старения; саморазрушение отдельных электронных компонентов компьютерных устройств и др.).

2. Совершено неумышленное преступление по причине халатности лица, ответственного за соблюдение режима конфиденциальности соответствующей компьютерной информации.

3. Преступление совершено с целью наживы лицом, имеющим доступ к конфиденциальной информации в силу исполнения им своих служебных обязанностей, – сотрудником потерпевшего.

4. Преступление совершено лицом, знакомым с условиями обработки и защиты конкретной конфиденциальной компьютерной информации потерпевшим.

5. Преступление совершено дистанционно с использованием специальных технических средств, предназначенных (приспособленных, разработанных, запрограммированных) для негласного получения конфиденциальной информации.

При выдвижении версий совершения преступлений в сфере компьютерной информации необходимо учитывать, что они совершаются обычно группой из двух и более человек, хотя не исключена возможность работы преступника – одиночки[1].

При этом выдвигаются типовые частные версии по каждому из обстоятельств, подлежащих доказыванию, в зависимости от того, какие из них не установлены к данному моменту. В результате сопоставления обстоятельств, подлежащих установлению и уже установленных, формулируются задачи расследования и определяются средства их решения[2].

В ходе расследования основные следственные задачи целесообразно решать в такой последовательности:

---

[1] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 28.

[2] Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий: конспект лекций. (электронный ресурс). URL: http://procuror.spb.ru/izdanija/2007_02_02.pdf (дата обращения: 01.04.2021).

1. Установление факта неправомерного доступа к информации в компьютерной системе или сети.

2. Установление места несанкционированного проникновения в компьютерную систему или сеть.

3. Установление времени совершения преступления.

4. Установление способа несанкционированного доступа.

5. Установление лиц, совершивших неправомерный доступ, их виновности и мотивов преступления.

6. Установление вредных последствий преступления.

7. Выявление обстоятельств, способствовавших преступлению, и в том числе установление надежности средств защиты компьютерной информации[1].

При расследовании компьютерных преступлений, связанных с созданием, использованием и распространением вредоносных программ для ПК, разумно применять следующую последовательность действий:

1. Установление факта использования и распространения вредоносной программы.

2. Установление факта и способа создания вредоносной программы.

3. Установление лиц, виновных в создании, использовании и распространении вредоносных программ.

4. Установление вреда, причиненного данным преступлением.

5. Установление обстоятельств, способствовавших совершению расследуемого преступления[2].

Таким образом формируется план расследования по делу в целом, отдельным эпизодам и обстоятельствам. По мере его выполнения и получения новой информации вносятся коррективы в имеющийся план, и вновь проводится анализ и формулирование дальнейших задач расследования.

---

[1] Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Указ. соч. С. 29-30.
[2] Там же. С. 30.

Таким образом, под следственной ситуацией понимается совокупность условий, в которых осуществляется расследование. Зачастую в преступлениях, совершенных с использованием компьютерных технологий выделяют такие типичные следственные ситуации как: установлена вся необходимая информация; установлен неправомерный доступ к компьютерной информации, имеются следы, но лицо, совершившее преступление не установлено; известна вся информация помимо обстоятельств доступа к компьютерной информации; отсутствуют сведения о виновном лице, следы преступления, неизвестен способ совершения преступления. Следственная ситуация обуславливает выдвижение общих и частных криминалистических версий, имеется прямая связь следственной ситуации с планированием. Следует отметить, что в случае оторванности от следственной ситуации планирование теряет практическую значимость и целесообразность.

2.3. Тактические особенности производства следственных действий на первоначальном этапе расследования

В случае, когда в следственных ситуациях нет данных о причинах возникновения киберпреступления, способе его совершения, а также личности субъекта преступления, или, когда отсутствуют лишь некоторые данные, то зачастую, следователь осуществляет такие действия и мероприятия как:

— Допрос потерпевших, свидетелей, подозреваемых;

— Принятие решения о необходимости задержания злоумышленника с поличным и проведения в связи с этим определенных мероприятий;

— Приглашение специалистов для участия в осмотре места происшествия и сам осмотр;

— Проведение оперативно-розыскных мероприятий для определения причин совершения киберпреступления, выявление лиц их совершивших, а также следов и иных вещественных доказательств;

— Выемка и дальнейший осмотр средств компьютерной техники, различных документов и предметов;

— Обыск рабочих мест и по месту проживания подозреваемых;

— Назначение различного рода экспертиз[1].

Когда известны причины возникновения преступления, способы его совершения и способы его сокрытия, личность злоумышленника и иные факты, предусмотрена следующая схема расследования на первоначальном этапе:

— Исследование материалов дела, их полноты, юридической грамотности применения норм уголовно-процессуального закона, а также принятие мер к получению недостающих данных;

— Возбуждение уголовного дела;

— Приглашение специалистов;

— Осмотр места происшествия;

— Личные обыски преступников, их места жительства и рабочих мест;

— Допрос подозреваемых, свидетелей;

— Выемка и осмотр вещественных и письменных доказательств;

— Изъятие и осмотр подлинных документов, лиц;

[1] Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий // практическое пособие / сост. И.Е. Мазуров. Казань: КЮИ МВД России, 2015. С. 30-31.

— Истребование, а при необходимости, производство выемки нормативных актов и документов, определяющих порядок и координацию работы в организации;

— Анализ найденных данных и решение вопроса о назначении дополнительных экспертиз[1]. Далее будут рассмотрены детально особенности производства отдельных следственных действий.

На начальном этапе расследования киберпреступлений ключевым следственным действием по праву признается осмотр места происшествия. При подготовке к осмотру или обыску, следует найти и изучить информацию о виде и конфигурации используемого компьютера. В связи с тем, что информацию, содержащуюся в компьютере можно с легкостью уничтожить, основополагающее значение будет иметь неотложность и внезапность вышеуказанных следственных действий[2].

Один из тактических приемов следователю при производстве осмотра места происшествия необходим к применению – «от центра к периферии», в случае если перемещение по осматриваемой зоне производится по развертывающейся спирали. Центральной точкой осмотра места происшествия, в зависимости от вида этого места, будет признаваться: либо электронный терминал, посредством которого было осуществлено преступление (когда производится осмотр места обнаружения признаков преступления или было совершено преступление); либо рабочее место, на котором было создано средство совершения преступления (при производстве осмотра места подготовки к преступным деяниям)[3].

---

[1] Там же. С. 31-32.

[2] Балашов Д.Н. Криминалистика: учебник. 2015 (электронный ресурс). URL: https://studref.com/590744/pravo/kriminalistika (дата обращения 01.04.2021).

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

В протоколе делается надпись о том, где находится компьютер и схематично изображается. Кроме того, указывается «иерархия» соединений, а также должны быть установлены способы объединения, например, через локальные сети, и способы связи компьютеров, например, через Интернет, и приборы, посредством которых это происходит. Должно быть подвергнуто проверке нахождение компьютера «в сети» или самостоятельная работа, может быть исследован определенный домен. Задача следователя, выявить конкретный терминал, с которого и происходит управления остальными и в последующем, следует осуществлять последующий осмотр конкретных персональных компьютеров именно с компьютера-сервера.

Осмотр персональных компьютеров предполагает фиксацию выведенной на дисплей информации, а также проверку работы различных компьютерных программ. Следователю необходимо остановить работу компьютерной программы, далее зафиксировать результат прекращения работы такой программы. Производится осмотр, с указанием в протоколе, о внешних устройствах, присоединенных к компьютеру, такие как принтер, веб-камера и иные. Выявляется модель компьютера и его тип, а также внешние устройства ввода и вывода. Подлежит проверке использование запоминающих устройств[1].

Обязательно копироваться на внешний жесткий диск должна информация, которая содержится в компьютере, а именно файлы, необходимые для работы операционной системы и файлы с записями о событиях, расположенные в хронологическом порядке. Обязательна проверка электронной почты или иных программ, посредством которых происходит онлайн или офлайн общение.

Производится проверка, фиксирующаяся в протоколе, о присутствии следов пальцев рук, микрочастиц и иных трасологических следов на

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

кнопке включения/ выключения компьютера, тачпада или компьютерной мыши, а также на клавиатуре наибольшая вероятность их обнаружить.

Изымать персональный компьютер со всеми его комплектующими внешними устройствами следует, когда изучению он уже подвергнуть полностью, например, когда был установлен пароль BIOS при входе в систему, а также, если следователь не имеет возможности скопировать 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, поскольку высока вероятность повредить и нарушить их нормальное функционирование. При производстве осмотра электронных документов, устанавливаются их местоположение, время его создания или модификации, а также формат, например, pdf, html, объем файлов. В открытом документе изучается содержащаяся информация[1].

Стоит отметить, что ошибкой будет являться использование при опечатывании жидкого клея или других веществ, которые могут послужить причиной поломки компьютера. Однако необходимо:

1. Выключить компьютер.

2. Отключить его от сети.

3. Отсоединить от всех разъемов, которые в дальнейшем должны быть опечатаны.

4. На бумажную ленту ставятся подписи следователя, специалиста, понятых, и иных 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.

[1] Там же. С. 227.

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[1].

При производстве допроса потерпевших и свидетелей должно быть установлено время и обстоятельства обнаружения киберпреступления, а также признаки, по которым было обнаружено такое преступление. Необходимо установить лиц, которые имели или могли иметь доступ к компьютеру, а также лиц, имеющих образование в сфере высоких технологий, занимающихся программированием или тех, кто уже совершал преступления с использованием компьютерных технологий и др. Могут подвергнуться допросу руководители юридического лица или индивидуальный предприниматель, являющимися потерпевшими от киберпреступления, а также инженерно-технические работники, например, программисты, сотрудники непосредственно работающие на компьютере, подвергнувшемуся кибератаке или иному преступному воздействию.

Что касается хищений денежных средств, совершенных с использованием вредоносных программ, то в протоколе допроса потерпевшего обязательно указываются реквизиты счета потерпевшего, с которых были списаны деньги, всю информацию о том, как потерпевший обнаружил такое противоправное списание, сумму причиненного преступными действиями ущерба, была ли подключена услуга банка по смс-уведомлению обо всех операциях по счету и др.[2]

---

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

[2] Закатов А.А., Намнясев В.В. Особенности первоначального этапа расследования хищений денежных средств, совершенных с использованием вредоносных компьютерных программ // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – №4 (40). – С. 132.

Допрос подозреваемого происходит следующим образом: следователю необходимо установить данные о личности подозреваемого, его отношения с сотрудниками и приятелями по работе, друзьями, выяснить сведения о его физиологическом и психологическом состоянии, образовательном уровне в сфере высоких технологий и знаний, опыте программирования, узнать о причинах и способах и средствах совершения киберпреступления, и иных лицах, участвующих в совершении преступления и другие сведения. Необходимо так же изучение архивных уголовных дел, содержащих в себе информацию о ранее совершенных подозреваемым преступлениях и киберпреступлениях[1]

В некоторых случаях, например в деле о хищениях денег с платежных карт или иных банковских счетов, посредством вредоносных программ, при расследовании и допросе подозреваемого стоит проанализировать ответы на запросы в разные организации, например выписки по счету, а также должны быть проанализированы локальные акты (должностные инструкции) служащих банка[2].

Для успешного производства обыска по месту жительства или работы подозреваемого, необходимо перекрыть доступ пользователя к персональным компьютерам. В случае установление функционирования программ по ликвидации информации, содержащейся на компьютере, необходимо в срочном порядке отключить компьютер, отсоединив его от электропитания. Исследование компьютерных устройств осуществляется по аналогии с проведением осмотра.

При производстве обыска необходимо обнаружить и изъять как компьютеры и их комплектующие, так и напечатанные на принтере листы, различные записи, написанные от руки, поскольку именно на таких данных в дальнейшем могут быть найдены сведения о плане совершения

[1] Тактика допроса подозреваемого по преступлениям совершаемым с использованием интернет-технологий (на примере статьи 272 УК РФ): метод. рекомендации. Омск, 2014. (электронный ресурс). URL: http:// мвд.рф/%0D (дата обращения: 01.04.2021).
[2] Савельева М.В., Смушкин А.Б. Указ. соч. С. 228.

киберпреступления, попытках подобрать пароли и др. Должны быть изъяты контрафактное программное обеспечение. Стоит акцентировать внимание на специальные книги и пособия по программированию, созданию вредоносных программ и т.д.[1]

Выемка журналов регистрации, а также истребование данных у провайдера Интернета необходимы для получения информации о времени доступа в сеть и времени о длительности пребывания в сети.

Ряд ученых включают производство компьютерно-технических экспертиз в неотложные следственные действия обязательных для первоначального этапа расследования[2]. Автор работы согласен с исследователями, поскольку, именно на первоначальном этапе расследования важно установить как можно более полную доказательственную базу и «картину» произошедшего деяния, во избежание ошибок в процессе расследования.

Например, в преступлениях с использованием вредоносных программ, экспертиза назначается для установления типа и алгоритма действия таких программ, а также источника ее распространения. Когда деньги посредством перевода со счета поступили во владения преступника, то методы расследования уголовных дел базируется на определении конечного получателя такого перечисления. На данный момент, похищенные денежные средства киберпреступники отсылают на различные сервисы электронных платежей, например, «Яндекс. Деньги», которые позже снимаются со счетов, либо производится оплата за товары и услуги. Для того, чтобы получить сведения о получателе денег стоит запросить сведения технического характера у оператора сотовой связи, а также представителя сервисов электронных платежей. Стоит отметить, что переводы денежных средств между счетами, закрепленными за разными лицами могут использоваться для оплаты товаров и услуг между лицами,

[1] Савельева М.В., Смушкин А.Б. Указ. соч. С. 228.
[2] Алексеров В.И., Колокольчикова О.Н. Указ. соч. С 86.

отбывающими наказания в исправительных учреждениях. В подобных случаях стоит запрашивать информацию у оператора связи, а именно: определенные сведения, например, IP-адреса, что даст возможность обнаружить неустановленного лица[1].

На основании всего вышеизложенного можно прийти к выводу, что фундаментальными следственными действиями на первоначальном этапе расследования преступления в сфере компьютерной информации признаются осмотр места происшествия, компьютерного оборудования и информации, обыск и выемка для выявления и фиксации, и изъятия компьютерной информации и компьютерных средств, а также допрос потерпевших, свидетелей и подозреваемых. Масштабность и распространенность киберпреступления в стране подталкивает следователя к более кропотливому изучению технических возможностей имеющихся компьютерных систем, а также их применения и использования в борьбе с преступлениями в изучаемой сфере.

[1] Закатов А.А., Намнясев В.В. Указ. соч. С. 133-134.

ГЛАВА 3. ОСОБЕННОСТИ ПОСЛЕДУЮЩЕГО И ЗАКЛЮЧИТЕЛЬНОГО ЭТАПОВ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

3.1. Особенности производства следственных действий на последующем и заключительном этапах расследования

Основным и решающим этапом работы по уголовному делу принято считать последующий этап расследования. Как и на первоначальном, ход расследования при последующем этапе обусловлен количеством информации и ее достоверностью[1]. Что касается заключительного этапа расследования, то характеризуется он подведением итогов проделанной работы, а также тем, что следователем формулируется и выражается в процессуальных документах внутреннее убеждение по каждому доказательству и обстоятельству дела, выявляются различные пробелы и противоречия[2]. Стоит отметить, что и в целом, и по рассматриваемой теме заключительный этап редко подвергается рассмотрению в видовых методиках. Аналитической работе следователя учеными не уделяется столь пристального внимания, однако данный этап играет довольно важную роль в процессе расследования и именно от него зависит, как судом будем рассмотрено уголовное дело.

На последующем этапе расследования киберпреступлений выделяются различные следственные ситуации, при которых:

1. Данных о личности субъекта преступления не имеется;

---

[1] Кардашевская М.В., Шипилова Е.С. Этапы процесса расследования и их характеристика // Таврический научный обозреватель. – 2015. – №2. – С.11-12.

[2] Химичева Г.П. Прекращение уголовного дела и (или) уголовного преследования как форма окончания предварительного расследования // Черные дыры в Российском законодательстве. – 2003. – № 1. – С. 213.

2. Обвиняемый полностью признает вину, и его показания обоснованы имеющимися доказательствами;

3. Обвиняемый полностью отрицает факты совершения преступлений и не дает показания;

4. Обвиняемый признает вину частично;

5. Обвиняемый признается в компьютерных преступлениях, но отрицает свою причастность к другим, например, к вымогательству[1].

Более кратко описал в своей работе следственные ситуации на данном этапе В.В. Поляков: признание вины обвиняемым; полное отрицание вины; частичное отрицание вины[2].

Проанализировав следственные действия по каждой следственной ситуации можно сделать вывод, что следователем в первую очередь проверяется анализ и осуществляется глубокая проверка исходных данных, которые были получены в рамках первоначального этапа, в том числе проводятся повторные и дополнительные допросы, экспертизы, проверяются старые и выдвигаются новые следственные версии, следователем предпринимается комплекс мер, направленный на поиск преступника, это и наведение справок, и наблюдение, и прочесывание местности, и др. Помимо прочего, последующий этап характеризуется такими следственными действиями как: очная ставка, следственные эксперименты, а также различного рода экспертизы.

При значительных разногласиях в даче показаний между соучастниками, подозреваемыми (обвиняемыми), свидетелями или потерпевшими киберпреступления, есть большая вероятность проведения

---

[1] Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий. (электронный ресурс). URL: https://рюи.мвд.рф/upload/site138/document_file/MAZUROV_I.E._Dissertaciya_2017.pdf (дата обращения: 01.04.2021).

[2] Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – №1 (21). – С.48.

очной ставки сотрудником правоохранительных органов[1]. Очная ставка – это специфическая разновидность допроса, суть которой применение следователем различных тактических приемов и способов установления истины по уголовному делу. При очной ставке может применяться дополнительное психологическое воздействие на добросовестного свидетеля, дающего неистинные показания.

Основной тактический прием – это предъявление доказательств. Это могут быть как документы, так и различные вещественные доказательства. Для начала допроса участникам очной ставки следователю необходимо задавать короткие и конкретные вопросы в рамках рассматриваемого уголовного дела. Вышеуказанный прием характеризуется тем, что недобросовестному участнику будет сложно подвергать изменению определенные несоответствия в своих показаниях, при этом лицо, «выдает» самого себя. Следующий тактический прием именуется обострением противоречий, цель которого нивелировать противоречия в показаниях соучастников. Так, следователь указывает участникам на какое-либо спорное обстоятельство, при этом делая акцент на противоречия между ними, а в последующем необходимо наращивать и обострять их. Итогом применения приема может быть, например, признание следователю о совершенном преступлении. Помимо прочего следователь, при проведении очной ставки может столкнуться с таким явлением как добросовестное заблуждение, при котором лицо, дающее показания может забыть о каких-то деталях или исказить их. В данных случаях, следователю необходимо вызвать у заблуждающегося лица ассоциации с истинным событием[2].

[1] Савельева М.В., Смушкин А.Б. Указ. соч. С. 228.
[2] Маркосян Г.А. Следственные действия при расследовании преступлений, связанных с созданием и распространением вредоносных программ, после предъявления обвинения // Юридический вестник Кубанского государственного университета. – 2019. – №3. – С.49-50.

В соответствии со ст.181 УПК РФ, следователем может быть осуществлен следственный эксперимент, если это требуется для раскрытия уголовного дела. Осуществляется он, посредством восстановления обстоятельств прошедших событий, действий лиц[1]. При расследовании компьютерных преступлений проведение следственного эксперимента будет способствовать обнаружению профессиональных навыков подозреваемого (обвиняемого), например, выявление способности к незаконному проникновению к компьютерной информации, созданию вирусных программ, возможности сделать вышеперечисленное определенным способом, возможность вызвать нарушения в работе компьютера и др. Важно, использовать компьютеры и программное обеспечение сходные с объектами или же средствами совершения преступления. Посредством следственного эксперимента возможна проверка работы защитных механизмов и программ некоторых устройств[2].

Назначение экспертизы, как важнейшего следственного действия на последующем этапе расследования компьютерных преступлений, необходимо. Следователем могут быть назначены: компьютерно-техническая, судебно-медицинская, судебно-бухгалтерская, криминалистическая, комплексная медико-криминалистическая и иная экспертиза[3].

Говоря о заключительном этапе расследования, стоит отметить, что характеризуется он формированием целостного представления об обстоятельствах, которые облегчили несанкционированный доступ к

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 №174-ФЗ // СПС «КонсультантПлюс».
[2] Савельева М.В., Смушкин А.Б. Указ. соч. С. 228.
[3] Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий. (электронный ресурс). URL: https://рюи.мвд.рф/upload/site138/document_file/MAZUROV_I.E._Dissertaciya_2017.pdf (дата обращения: 01.04.2021).

компьютерной информации[1]. Заключительный этап возникает с момента прекращения производства следственных действий, а заканчивается составлением обвинительного заключения (акта) или вынесением постановления о прекращении уголовного дела. По содержанию он включает в себя производство дополнительных и повторных действий и определение порядка окончания расследования[2].

Таким образом, последующий и заключительный этап расследования преступлений в сфере компьютерной информации отличается доказательственной определенностью и информативностью, относительно первоначального этапа, но являясь центральным, следователю необходимо усердно и скрупулезно работать. Препятствия, с которыми может столкнуться следователь на данном этапе расследования, это упущенные на раннее моменты, связанные расследованием уголовного дела, которые влияют на его исход. Назначение различного рода экспертиз, очных ставок или же следственного эксперимента подразумевает обладание следователем специальных знаний в области компьютерных информационных технологий, а также познаний в психологии. Отсутствие должной квалификации следователя и вышеизложенных знаний на достойном уровне приводит к затягиванию расследования преступления. Таким образом, от четкой, последовательной и методичной работы следователя на каждом этапе расследования компьютерного преступления зависит справедливость решения по уголовному делу.

---

[1] Методика расследования преступлений в сфере компьютерной информации (электронный ресурс). URL: https://be5.biz/pravo/k011/43.html (дата обращения: 01.04.2021).

[2] Кубанов В.В. Криминалистическая тактика. Криминалистическая методика (электронный ресурс). URL: https://studref.com/558928/pravo/kriminalisticheskaya_taktika_kriminalisticheskaya_metodika (дата обращения: 01.04.2021).

3.2. Возможности судебных экспертиз при расследовании преступлений в сфере компьютерной информации

Нормальное расследование компьютерных преступлений и привлечение к уголовной ответственности лица без грамотного экспертного заключение становится проблематичным.

На текущий момент, посредством судебных экспертиз могут быть решены такие задачи как:

— воссоздание и восстановление компьютерной информации или ее части, которая ранее была удалена или изменена;

— выяснение даты и времени создания, модификации, удаления, копирования информации;

— декодирование информации, возможность подобрать пароли и раскрыть систему защиты СВТ;

— изучение СВТ на присутствие в них программно-аппаратных модулей, компьютерных вирусов и модификаций;

— выяснение автора, места и средства подготовки, а также способ изготовления программ и файлов, включенных в компьютер или носитель информации;

— обнаружение данных о каналах утечки информации из компьютерной сети;

— обнаружение технических неисправностей, оценка износа СВТ;

— определение уровня специальной подготовки некоторых участников преступления;

— установление конкретных лиц, проигнорировавших соблюдение правил эксплуатации компьютера, его системы и сети;

— выяснение причин и условий, способствовавших совершению киберпреступления[1].

В процессе расследования киберпреступлений возможно назначение стандартных дактилоскопических и трасологических, почерковедческих экспертиз, так и специальных экспертиз, например, фоноскопической, в случаях, когда на компьютере содержатся звуковые файлы, или финансово-экономической, в случае потребности в установлении конкретного размера ущерба, причиненного совершенным преступлением[2].

Также к специфическим экспертизам относят компьютерно-техническую экспертизу, которую некоторые ученые классифицируют таким образом: аппаратно-компьютерная экспертиза; программно-компьютерная экспертиза; информационно-компьютерная экспертиза; компьютерно-сетевая экспертиза[3].

Аппаратно-компьютерная экспертиза необходима для изучения аппаратных компьютерных средств, установлении модели и различных технических параметров, функциональных возможностей определенного компьютера, исходного технического состояния и сравнение такого состояния на момент исследования компьютера.

При назначении программно-компьютерной экспертизы преследуется цель установления общей характеристики программного обеспечения компьютера, назначения программ и устройств, их версии, типа и вида, определения внесения модификаций в исследуемый объект и при положительной ответе, установление времени, цели и совокупности таких изменений.

---

[1] Катков С.А., Собецкий И.В., Федоров А.Л. Подготовка и назначение программно-технической экспертизы // Информационный бюллетень СК МВД России. – 1995. – № 4 (85). – С. 93-94.

[2] Савельева М.В., Смушкин А.Б. Указ. соч. С. 228.

[3] Россинская Е.Р. Судебная экспертиза в гражданском, административном и уголовном процессе. – М.: Норма, 2005, С. 458.

Ведущим видом специальных экспертиз признается информационно-компьютерная, при которой происходит поиск, анализ и оценивание информации, созданной пользователем или программами для координации информационных процессов в компьютерной системе.

Последняя, компьютерно-сетевая экспертиза предназначена для исследования функционального назначения ряда компьютерных средств, которые реализуют определенную сетевую технологию[1].

Стоит отметить, что лица, расследующие компьютерные преступления довольно часто сталкиваются с проблемами, причинами которых является, как уже неоднократно упоминалось выше, низкий уровень узкоспециальных, а иногда и общих знаний в области компьютерной информации, что может привести к неверной постановке вопросов эксперту, соответственно, и таких же некорректных ответов.

Еще одной проблемой является незначительное количество специализированных экспертных учреждений. По мнению О.Ю. Зеленкиной, с которой невозможно не согласиться, для решения данной проблемы необходимо внедрение единого специального криминалистического учета, в котором бы содержались ключи шифрования, данные о программно-техническом обеспечении и другая информация. Необходимо это для упрощения процесса расследования, а также процесса сбора и анализа статистических данных[2]. На современном этапе, новейшие способы совершения киберпреступлений выявляются постоянно. Полагаю, создание всероссийских, а целесообразнее и международных информационных баз данных будет способствовать, во-первых, быстроте расследования уголовных дел, экономии времени, которой так не хватает следователям, во-вторых, изучению и

[1] Россинская Е.Р. Указ. соч. С. 458-467.

[2] Зеленкина О.Ю. Особенности расследования преступлений в сфере компьютерной информации (электронный ресурс). URL: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения:01.04.2020).

профилактике новейших преступных схем. Предоставляя доступ к подобному единому специализированному криминалистическому учёту высшими учебными заведениями, при обучении курсантов и студентов юридических вузов, система правоохранительных органов получит более подготовленных специалистов в области расследования преступлений в сфере компьютерной информации.

Таким образом, современные возможности судебных экспертиз при расследовании компьютерных преступлений, дают возможность сбора достоверной информации, формирования доказательственной базы следователем. Полагаем, именно компьютерно-техническая экспертиза является основным и наиболее эффективным способом в расследовании преступлений.

Заключение

Рост количества киберпреступлений и в России, и в мире с каждым годом увеличивается, при этом уровень раскрываемости данных преступлений правоохранительными органами довольно низок. Это связано как с непрекращающимся научно-техническим прогрессом, с созданием новейших способов совершения преступлений в области высоких технологий, так и невероятной нехваткой квалифицированных сотрудников правоохранительных органов, а именно их знаний и умений в области информационных технологий.

Исследовав актуальные проблемы данной темы, проанализировав теоретические источники и судебно-следственную практику по преступлениям в сфере компьютерной информации, полагаю цель выпускной квалификационной достигнута.

Так, в работе выявлено, что типичным преступником, совершающим преступления в данной сфере, в основном является мужчина в возрасте от 18 до 40 лет, житель города, имеющий среднее специальное, незаконченное высшее или высшее образование, учащийся, работающий или временно безработный, ранее не судимый, являющийся активным пользователем сети Интернет, не женатый, замкнутый человек.

Обстановку совершения киберпреступлений отличает несоответствие места совершения преступления и наступления общественно опасных последствий, а само место преступления характеризуется местоположением в реальном пространстве и IP-адресом. Были выделены способы совершения таких преступлений, как: кардинг, фишинг, вишинг, фарминг, ботнет, скимминг и иные. Анализ судебной практики по выделенным способам показал, что большинство преступников узнают о способах совершения преступлений, о различных преступных схемах и устройствах на форумах сайтов сети Интернет от

неустановленных лиц, которые могут выступать соучастниками преступлений и исходя из практики, так и остаются ненайденными. К орудиям совершения данных преступлений относят: компьютерную технику, средства сотовой связи либо специальное оборудование.

Для того, чтобы принять решение о возбуждении уголовного дела необходимо два элемента: повод и основание. Типичными ошибками, совершаемыми на стадии возбуждения уголовного дела, являются не выяснение определенных обстоятельств киберпреступления, утеря доказательств, различные технические ошибки следователя, а также низкий уровень доследственной проверки. Важнейшими следственными действиями на первоначальном этапе расследования киберпреступлений являются осмотр места происшествия, компьютеров и информации, обыск и выемка, цель которых выявление, фиксация и изъятия компьютерной информации и средств, непосредственно связанных с расследуемым уголовным делом, а также допрос потерпевших, свидетелей и подозреваемых.

Последующий и заключительный этап расследования преступлений в сфере компьютерной информации отличается доказательственной определенностью и информативностью, относительно первоначального этапа, но являясь центральным, следователю необходимо усердно и скрупулезно работать. Препятствия, с которыми может столкнуться следователь на данном этапе расследования, это упущенные на раннее моменты, связанные расследованием уголовного дела, которые влияют на его исход. Назначение различного рода экспертиз, очных ставок или же следственного эксперимента подразумевает обладание следователем специальных знаний в области компьютерных информационных технологий, а также познаний в психологии.

В процессе расследования преступления могут назначаться как дактилоскопические и трасологические экспертизы, почерковедческие, так и специфические, называемые компьютерно-технические экспертизы. Для

решения проблемы нехватки специализированных экспертных учреждений необходимо создание всероссийских, а целесообразнее и международных информационных баз данных, что будет способствовать, во-первых, быстроте расследования уголовных дел, во-вторых, изучению и профилактике новейших преступных схем.

На основании изложенного можно сделать вывод, что проблема роста киберпреступлений и их раскрываемости остается довольно острой, актуальной и требует решения на законодательном уровне. Проблему некомпетентности следователей, нехватки времени для нормального расследования дела можно решить путем расширения штата сотрудников специализированных следственных подразделений, занимающихся расследованием киберпреступлений, а также созданием узконаправленных специализированных Вузов, где курсантов будут обучать помимо юриспруденции, информационным наукам и технологиям.

Трансграничный характер компьютерных преступлений, а также порядок международного сотрудничества государств препятствует оперативности в действиях сотрудников правоохранительных органов, влияет на своевременность фиксации следов преступления, а иногда и вовсе блокирует расследование за пределами территории РФ. Ряд авторов полагают, что решением данных проблем будет являться созданием международного ведомства по борьбе с киберпреступлениями[1].

Некоторыми учеными для борьбы с киберпреступлениями предлагается ведение института государственно частного партнерства, однако для этого как и для всего вышеперечисленного следует кардинально изменять действующую законодательную базу[2].

---

[1] Торичко Р.С., Клишина Н.Е. Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпрестулений // Вестник экономической безопасности. – 2018. – №3. – С.179-180.

[2] Мещеряков В.А., Пидусов Е.А. Государственно-частное партнерство в сфере противодействия киберпреступности: шаг вперед или реальная угроза // Вестник Воронежского института МВД России. – 2019. – №3. – С. 162.

Библиографический список

Нормативные правовые акты и иные официальные документы:

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ // СПС «КонсультантПлюс».
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс».
3. Об информации, информационных технологиях и защите информации: федеральный закон от 27.07.2006 г. № 149-ФЗ // СПС «КонсультантПлюс».
4. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: федеральный закон от 01.10.2008 г. № 164-ФЗ // СПС «КонсультантПлюс».

Монографии, учебники, учебные пособия:

1. Алексеров В.И., Колокольчикова О.Н. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации: учебно-практическое пособие / В.И. Алексеров, О.Н. Колокольчикова. М.: ВИПК МВД России, 2016. – 166 с.
2. Балашов Д.Н. Криминалистика: учебник. 2015 (электронный ресурс). URL: https://studref.com/590744/pravo/kriminalistika (дата обращения 01.04.2021).
3. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: ООО «Издательство «Юрлитинформ», 2001. – 314 с.
4. Волохова О.В., Егоров Н.Н., Жижина М.В. и др. Криминалистика: учебное пособие / под ред. Е.П. Ищенко. М.: Проспект, 2011. – 349 с.

5. Волчецкая Т.С. Криминалистическая ситуалогия: монография / Т.С. Волчецкая. М.; Калининград, 1997. – 249 с.

6. Гавло В.К. О следственной ситуации в методике расследования хищений, совершенных с участием должностных лиц // Вопросы криминалистической методологии, тактики и методики расследования. М., 1973. – 90 с.

7. Карлов В.Я. Криминалистика: тезаурус-словарь и схемы // учебное пособие. / В.Я. Карлов. М.: Альфа-Пресс, 2011. – 267 с.

8. Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий: конспект лекций. (электронный ресурс). URL: http://procuror.spb.ru/izdanija/2007_02_02.pdf (дата обращения: 01.04.2021).

9. Лелетова М.В. Особенности расследования преступлений, совершаемых с использованием средств сотовой связи // отчет о НИР (заключительный) /сост. М.В. Лелетова. Нижний Новгород: НА МВД России, 2015. – 77 с.

10. Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий // практическое пособие / сост. И.Е. Мазуров. Казань: КЮИ МВД России, 2015. – 78 с.

11. Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: диссертация (электронный ресурс).URL:https://рюи.мвд.рф/upload/site138/document_file/MAZUROV_I.E._Dissertaciya_2017.pdf (дата обращения: 01.04.2021).

12. Миронов С.Н. и др. Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации, предусмотренных статьей 159.6 Уголовного кодекса Российской Федерации: методические рекомендации / С.Н. Миронов и др. Казань: КЮИ МВД России, 2017. – 65 с.

13. Петраков С.В., Миронов И.А., Карнаухова О.Г., Попов А.А. Раскрытие и расследование мошенничеств, связанных с неправомерным доступом к компьютерной информации и списанием денежных средств с

расчетных счетов граждан // отчет о НИР (заключительный) /сост. С.В. Петраков и др. СПб: СПбУ МВД России, 2016. – 115 с.

14. Россинская Е.Р. Судебная экспертиза в гражданском, административном и уголовном процессе.- М.: Норма, 2005. – 656 с.

15. Савельева М.В., Смушкин А.Б. Криминалистика: учебник / под. ред. М.В. Савельева, А.Б. Смушкин М. : Издательство Издательский дом «Дашков и К», 2009. – 608 с.

16. Филлипов А.Г. Криминалистика: учеб. пособие 2014. (электронный ресурс). URL: https://studme.org/90885/pravo/osobennosti_vozbuzhdeniya_ugolovnogo_dela_tipichnye_situatsii_pervonachalnogo_etapa_rassledovaniya_deystv (дата обращения: 01.04.2021).

17. Шевко Н.Р., Турутина Е.Э., Панченко В.В., Каримов А.М. Методические рекомендации по предупреждению, пресечению, раскрытию и расследованию преступлений, совершенных с использованием высоких технологий и коммуникаций: учебное пособие / Н.Р. Шевко, Е.Э. Турутина, В.В. Панченко, А.М. Каримов. Казань: КЮИ МВД России, 2016. – 92 с.

18. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : диссертация. (электронный ресурс). URL: https://www.msal.ru/common/upload/SHevchenko_E.S.pdf(дата обращения: 01.04.2021).

19. Шмонин А.В., Ефремова Е.А., Баранов В.В., Казюлин А.В. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий : учебно-практическое пособие / А.В. Шмонин, Е.А. Ефремова, В.В. Баранов, А.В. Казюлин. М.:АУ МВД России, 2016. – 203 с.

20. Яблоков Н. П. Криминалистика: учебник / отв. ред. Н.П. Яблоков. М.: ЛексЭст, 2006. – 781 с.

21. Яджин Н.В., Егоров В.А. Особенности расследования корыстных преступлений, совершаемых с использованием средств сотовой связи // отчет о НИР (заключительный) / сост. Н.В. Яджин, В.А. Егоров. Тюмень: ТИПК МВД России, 2016. – 33 с.

Научные публикации и статьи в иных периодических изданиях интернет-ресурсы:

1. Баринов С.В. Криминалистическая характеристика личности преступника, совершающего преступные нарушения неприкосновенности частной жизни в киберпространстве (электронный ресурс). URL: https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-lichnosti prestupnika-soveshayuschego-prestupnye-narusheniya-neprikosnovennosti-chastnoy (дата обращения: 01.04.2021).

2. Бурданова В.С. Криминалистическая характеристика преступлений, связанных с незаконным оборотом наркотиков // Прокурорско-следственный работник. –1998. – №3. – С.7–16.

3. Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь, 2004 – № 7 – С. 2–5.

4. Головинов О. Н, Погорелов А. В. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. – 2016. – № 6 (1). – С. 73–88.

5. Данные официального сайта МВД России. URL: https://мвд.рф (дата обращения: 01.04.2021).

6. Закатов А.А. Намнясев В.В. Особенности первоначального этапа расследования хищений денежных средств, совершенных с использованием вредоносных компьютерных программ // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – №4 (40). – С. 130–134.

7. Зайцев А.А. Смолин А.В. Типичные следственные ситуации, складывающиеся при расследовании киберпреступлений // Актуальные проблемы криминалистики и судебной экспертизы: Материалы междунар. науч.-практ. конф. Восточно-Сибирский институт МВД РФ, – 2020. – С. 52–56.

8. Зеленкина О.Ю. Особенности расследования преступлений в сфере компьютерной информации (электронный ресурс). URL: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения:01.04.2020).

9. Илюшин Д.А. Особенности возбуждения уголовных дел о преступлениях, совершаемых в сфере предоставления услуг «Интернет» // Вестник Самарского государственного университета. – 2007. – №1 (51). – С. 9–16.

10. Кардашевская М.В., Шипилова Е.С. Этапы процесса расследования и их характеристика// Таврический научный обозреватель. – 2015. – №2. – С.8–14.

11. Катков С.А., Собецкий И.В., Федоров А.Л. Подготовка и назначение программно-технической экспертизы // Информационный бюллетень СК МВД России. – 1995. – № 4 (85). – С. 87–96.

12. Кредитки в руках кибермошенников. (электронный ресурс) URL: https://www.sravni.ru/text/2010/9/9/kreditki-v-rukah-kibermoshennikov/ (дата обращения: 01.04.2021).

13. Кубанов В.В. Криминалистическая тактика. Криминалистическая методика (электронный ресурс). URL: https://studref.com/558928/pravo/kriminalisticheskaya_taktika_kriminalisticheskaya_metodika (дата обращения: 01.04.2021).

14. Лакомов А.С. Киберпреступность: современные тенденции // Академическая мысль. – 2019. – №2 (7). – С. 53–56.

15. Маркосян Г.А. Следственные действия при расследовании преступлений, связанных с созданием и распространением вредоносных программ, после предъявления обвинения // Юридический вестник Кубанского государственного университета. – 2019. – №3. – С.48–52.

16. Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Среднерусский вестник общественных наук. – 2014. – № 1 (31). – С. 114–121.

17. Мерзлов Ю.А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. – 2015. – № 4 (7). – С. 56–61.

18. Методика расследования преступлений в сфере компьютерной информации (электронный ресурс). URL: https://be5.biz/pravo/k011/43.html (дата обращения: 01.04.2021).

19. Мещеряков В.А., Пидусов Е.А. Государственно-частное партнерство в сфере противодействия киберпреступности: шаг вперед или реальная угроза // Вестник Воронежского института МВД России. – 2019. – №3. – С. 161–166.

20. Мобильный контент. Новый вирус для мобильных телефонов (электронный ресурс).URL: http://www.procontent.ru/news/4864.html (дата обращения: 01.04.2021).

21. Олиндер Н.В. Время и место совершения преступления как элемент криминалистической характеристики преступлений, совершенных с использованием электронных платежных средств и систем // Вестник Самарского государственного университета. – 2014. – № 11-1. – С. 89–93.

22. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114–116.

23. Поляков В.В., Попов Л.А. Особенности личности компьютерных преступников // Известия Алтайского государственного университета. – 2018. – №6 (104). – С. 256–259.

24. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – №1 (21). – С.46–50.

25. Проблемы кибербезопасности в России и пути их решения (электронный ресурс). URL: https://www.garant.ru/article/520694/ (дата обращения: 01.04.2021).

26. Способы совершения компьютерных преступлений (электронный ресурс). URL: http://csaa.ru/sposoby-sovershenija-kompjuternyh-prestuplenij/. (дата обращения: 01.04.2021).

27. Торичко Р.С., Клишина Н.Е. Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпрестулений // Вестник экономической безопасности. – 2018. – №3. – С.179–184.

28. Трубачинов А.В. Особенности возбуждения уголовного дела и планирования на первоначальном этапе расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ // Вестник Волгоградской академии МВД России. – 2019. – №1 (48). – С. 153–159.

29. Химичева Г.П. Прекращение уголовного дела и (или) уголовного преследования как форма окончания предварительного расследования // Черные дыры в Российском законодательстве. – 2003. – № 1. – С. 213–240.

30. Центр исследования проблем компьютерной преступности. Криминалистическая характеристика компьютерных преступлений

(электронный ресурс). URL: http://www.crime-research.ru/library/Shatal.htm (дата обращения 01.04.2021).

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

32. Что такое фишинг в сети, какую цель он преследует, и как защититься? (электронный ресурс).URL: https://stolohov.com/poleznye-stati/chto-takoe-fishing-v-seti.html#i-15 (дата обращения: 01.04.2021).

33. Шаталов А.С., Пархоменко А.Н. Криминалистическая характеристика компьютерных преступлений (электронный ресурс). URL: http://www.crime-research.ru/library/Shatal.htm (дата обращения: 01.04.2021).

34. Яблоков Н.П. Криминалистическая характеристика преступлений и типичные следственные ситуации как важные факторы разработки методики расследования преступлений / Н.П. Яблоков // Вопросы борьбы с преступностью. – 1979. – № 30. – С. 110–122.

Эмпирические материалы:

1. Апелляционное постановление Верховного Суда Республики Марий Эл от 26 ноября 2018 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

2. Апелляционное постановление Красноярского краевого суда от 26 сентября 2017 года (электронный ресурс). Режим доступа URL: https://sudact.ru (дата обращения: 01.04.2021).

3. Приговор Верхнепышминского городского суда от 7 июня 2011 года (электронный ресурс). Режим доступа: URL. http://docs.pravo.ru/document/view/18392970/. (дата обращения 01.04.2021).

4. Приговор Чертановского районного суда г. Москвы от 7 сентября 2012 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021)

5. Приговор Курганского городского суда от 22 августа 2013 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

6. Приговор Калининского районного суда г. Челябинска от 23 декабря 2014 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

7. Приговор Заельцовского районного суда города Новосибирска от 24 марта 2015 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

8. Приговор Кировского районного суда г. Саратова от 9 августа 2016 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

9. Приговор Воркутинского городского суда от 21 ноября 2019 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

10. Приговор Кировского районного суда г. Омска от 26 декабря 2019 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).

11. Приговор Урицкого районного суда п. Нарышкино от 11 февраля 2020 года (электронный ресурс). Режим доступа: URL: https://sudact.ru (дата обращения: 01.04.2021).