Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Юридический институт
Магистратура

УДК 343.98

Егорова Ирина Александровна

# ПЕРВОНАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

**МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ**

на соискание степени магистра
по направлению подготовки
40.04.01 – «Юриспруденция»

Руководитель ВКР:
канд. юрид. наук, доцент
_____ И.С. Фоминых
«11» мая 2020 г.

Автор работы:
_____ И.А. Егорова

Томск–2020

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Магистратура

**«СОГЛАСОВАНО»**
**Зав. магистратурой ЮИ НИ ТГУ**
**_____О.В. Воронин**
«____» _____ 20__ г.

ЗАДАНИЕ
по подготовке выпускной квалификационной (магистерской) работы

студенту Егоровой Ирине Александровне

Тема выпускной(квалификационной)работы Первоначальный этап расследования преступлений в сфере компьютерной информации

Утверждена_____
Руководитель работы: Фоминых И.С.

Сроки выполнения выпускной (квалификационной) работы:

1). Составление предварительного плана и графика написания выпускной (квалификационной) работы
с «15» октября 2018г. по «18» октября 2018г.

2). Подбор и изучение необходимых нормативных документов, актов и специальной литературы с «01» ноября 2018г. по «10» ноября 2018г.

3). Сбор и анализ практического материала с «01» января 2019г. по «15» января 2019г.

4). Составление окончательного плана выпускной (квалификационной) работы
с «20» января 2020г. по «30» января 2020г.

5). Написание и оформление выпускной (квалификационной) работы
с «30» января 2020г. по «15» марта 2020г.

Если работа выполняется по заданию организации указать ее_____

Встречи дипломника с научным руководителем – ежемесячно (последняя неделя месяца в часы консультаций).
Научный руководитель Фоминых И.С. Фоминых И.С.

С положением о порядке организации и оформления выпускных (квалификационных) работ ознакомлен, задание принял к исполнению Егорова И.А.

**Аннотация**

магистерской диссертации

на тему: «Первоначальный этап расследования преступлений в сфере компьютерной информации»

Актуальность выбранной темы обусловлена тем, что в современном мире наблюдается устойчивый рост количества противоправных действий, совершаемых лицами путём использования современных информационных технологий и специализированных знаний в области защиты компьютерной информации.

Предметом исследования выступают закономерности организации расследования преступлений в сфере компьютерной информации, а также деятельность органа предварительного следствия и дознания, складывающиеся в сфере выявления, раскрытия и расследования данного вида преступной деятельности.

Объектом исследования стала практика расследования и предупреждения преступлений в сфере компьютерной информации, научная и учебная литература.

Целью данной работы является комплексная криминалистическая характеристика преступлений в сфере компьютерной информации, их классификация; изучение организации расследования преступлений данной категории; рассмотрение некоторых современных проблем борьбы с преступлениями в сфере компьютерной информации.

Для достижения поставленных в настоящей работе целей и задач применялись общенаучные и частно-научные методы познания.

По структуре работа включает в себя введение, три главы, заключение и список использованных источников и литературы.

Во введении обосновывается актуальность выбранной для диссертационной работы темы, уточняется степень научной разработанности данного исследования, объект и предмет исследования, его цель, задачи, методологическая, теоретическая, эмпирическая и нормативно-правовая

основы.

В первой главе предполагается рассмотрение вопросов одного из важнейших элементов частной криминалистической методики – криминалистической характеристики.

Во второй главе планируется изложить типичные следственные ситуации первоначального этапа расследования и проводимые оперативно-розыскные мероприятия. Одно из центральных положений в этой части диссертационной работы принадлежит вопросам следственных ситуаций, складывающихся на первоначальном этапе расследования указанных преступлений.

В третьей главе должны получить рассмотрение особенности тактики производства отдельных следственных действий. В частности, речь пойдет о тактике производства вербальных и невербальных следственных действиях.

Заключение предполагает краткое подведение итогов магистерской диссертации.

Объем дипломной работы составляет 84 страницы. При написании работы использовалось 76 источников.

Автор работы Егорова И.А.

ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

Современному обществу как никогда свойственны интенсивный темп научно-технического прогресса и быстрое развитие компьютерных технологий, в том числе, бурное развитие компьютерной техники и средств телекоммуникаций. Широчайшее их распространение практически во все сферы человеческой деятельности обуславливает возникновение и рост преступности в сфере компьютерной информации, она же – киберпреступность.

Термин «преступления в сфере компьютерной информации» используется наравне с терминами «киберпреступность» и «компьютерные преступления», их употребляют как синонимы. Различные подходы, ведущие к определению данных понятий, провоцируют большое количество обсуждений.

На период первого квартала 2010 года количество раскрытых преступлений было на 1430 меньше, чем официально зарегистрированных-11918. Отчетность с января по апрель 2015 года зафиксировала случаи 629 компьютерных преступлений, раскрыто всего236[1]. В 2019 году зарегистрировано более 294 тысяч преступлений, половина преступлений совершается с использованием сети «Интернет», а более трети – средств мобильной связи. В январе 2020 года зарегистрировано 28,1 тыс. преступлений, совершённых в сфере компьютерной информации, что на 75,2% выше, чем за такой же период прошедшего года[2].

При всем этом нужно учесть, что преступления этой категории обладают высочайшей латентностью и наносят огромный экономический ущерб государству и организациям, и расследование таких преступлений неизбежно связано с множеством трудностей для сотрудников правоохранительных органов.

С целью увеличения эффективности работы правоохранительных органов необходимы рекомендации криминалистической науки, которые могут

[1] Евдокимов К. Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. 2016. № 1 (35) С. 91.

[2] Состояние преступности в Российской Федерации за январь-апрель 2017 года [Электронный ресурс] // Министерство внутренних дел Российской Федерации. Электрон. дан. [Б. м.], 2020. URL: https://мвд.рф/folder/101762/item/10287274/ (дата обращения: 08.03.2020).

положительно воздействовать на качество предварительного расследования, повысить уровень его организационно-тактического и технического обеспечения и внедрение в практику актуальных криминалистических разработок, которые отвечают современному уровню развития науки, что позволит вести более эффективную борьбу с преступностью.

Актуальность, сложность проблем борьбы с преступлениями в сфере компьютерной информации, теоретическая и практическая значимость вопросов, которые возникают в процессе расследования компьютерной преступности, обусловили интерес к ним российских и зарубежных исследователей.

Проблемы расследования компьютерных преступлений привлекли внимание таких учёных, как В. Б. Вехов, В. В. Крылов, Н. С. Полевой, Н. А. Селиванов, В. Ю. Рогозин, Ананиана Л. Л., Борчевой Н.А., Зубовой М. А., Ивановой И.Г., Козлова В.Е., Мещерикова А., Панфиловой Е.И. и Попова А.Н., Петрухина В.Ю. и Авраменко В.П., Полякова В.В., Степанова В.В. и Бабаковой М.А. Однако, несмотря на существующие публикации, продолжают отсутствовать полные, научно- обоснованные рекомендации по расследованию преступлений в сфере компьютерной информации, которые были разработаны с учетом постоянно развивающихся методов их совершения и сокрытия, типичных следственных ситуаций. Многие работы носят обзорный характер, зачастую содержат вопросы уголовного права и не содержат каких-либо практических рекомендаций и советов по расследованию данного вида преступлений. Это, в свою очередь, создает трудности в правоприменительной практике.

Объектом исследования выступают преступная деятельность в форме неправомерного доступа к компьютерной информации и деятельность по расследованию данных преступлений. Предметом исследования определены взаимосвязанные закономерности двух видов: многообразие способов совершения данного преступления и закономерности расследования этого преступления.

Целью данной диссертационной работы является криминалистическая характеристика преступлений в сфере компьютерной информации, их классификация; изучение организации расследовании данных преступлений; рассмотрение некоторых современных проблем борьбы с киберпреступностью.

Для достижения данной цели, необходимо решить определенные задачи:

1) провести анализ различных подходов к определению понятия «преступления в сфере компьютерной информации», соотнести данное понятие с понятиями «киберпреступления», «компьютерные преступления»;

2) провести анализ понятия средств совершения преступлений в сфере компьютерной информации (киберпреступлений), а также изучить их классификацию и виды;

3) рассмотреть основные элементы криминалистической характеристики преступлений в сфере компьютерной информации, такие как способ и обстановка совершения преступления;

4) изучить личность киберпреступника;

5) изучить основы организации расследования преступлений в сфере компьютерной информации (киберпреступлений);

6) рассмотреть современные проблемы борьбы с киберпреступностью.

Методологическую основу диссертационного исследования составляет диалектический метод научного исследования, на его базе был применён логический метод осмысления, который заключается, в изложении материла, формировании выводов, а так же на выдвижении предложений и рекомендаций.

Теоретическую базу проведенных исследований составляют труды отечественных и зарубежных ученых, а также научные труды сотрудников Юридического института Национального исследовательского Томского государственного университета.

Эмпирическую основу образуют, прежде всего, изученные в ходе преддипломной практики аналогичные по характеру эмпирические данные, содержащиеся в литературных и иных источниках, в том числе приговоры судов различных уровней.

Исследовательская новизна диссертационной работы определяется, в первую очередь, выводами о некоторых особенностях личности преступника, задержания, производства осмотра места происшествия, допроса, а также обыска.

Структура диссертации обусловлена целями и задачами исследования. Диссертационная работа состоит из введения, трех глав, заключения и списка использованных источников и литературы.

# 1 Общие положения методики расследования преступлений в сфере компьютерной информации

## 1.1 Понятие преступлений в сфере компьютерной информации

На сегодняшний день компьютерные технологии стали неотъемлемой частью жизни человека. Это привело к появлению так называемого «информационного общества» - новый тип современной общественности. Но это сопутствовало и появлению новых видов преступлений, где глобально используются информационно-телекоммуникационные системы и сети. Преступники быстрее осваивают новые технологии, опережая законодательство и правоприменителей. Исходя из этого, число совершенных преступлений в сфере компьютерной информации возросло, и экономический ущерб ежегодно растёт с каждым их свершением[3]. Сегодня компьютерная преступность - один из самых опасных видов преступных посягательств.

В начале 60-х гг. XX века в иностранной литературе впервые возникло понятие «компьютерные преступления». В повседневной жизни широкое применение информационных технологий привело к повышению количества преступных посягательств.

В России уголовно-правовая наука не даёт четкого определения компьютерным преступлениям. Составы преступлений фиксируются Уголовным Кодексом РФ, включая в себя перечень определённых признаков, которые позволяют определить, что это опасное деяние, а так же перечисляются виды действий, которые относятся к преступлениям, посягающим на безопасность компьютерной информации.

В настоящее время в отечественной юридической науке существует несколько мнений различных групп ученых по поводу того, что следует понимать под данным термином.

Приверженцы одной из таких групп, как Ю. М. Батурин и А. М. Жодзишский, считают, что: «компьютерных преступлений, как преступлений

[3] Мнацаканян А. В. Преступления в сфере безопасности компьютерной информации как элемент системы Особенной части Уголовного Кодекса Российской Федерации // Пробелы в российском законодательстве. 2012. № 3. С. 158.

специфических в юридическом смысле, не существует»[4]. С точки зрения юриспруденции более корректно принимать во внимание компьютерные аспекты преступления. Основным аргументом в пользу этой точки зрения является тот факт, что совершённые противоправные действия не принято различать по видам технических средств, с помощью которых происходит их совершение.

В противопоставление предыдущей группе учёных и их точке зрения, существует противоположная, которая гласит о том, что термин “компьютерные преступления” достаточно давно присутствует в международной лексике и такие учёные, как В. Б. Вехов, Ю. И. Ляпунов, В. Ю. Максимов, Н. А. Селиванов аргументировано считают, что такая формулировка имеет полное право на существование. Учёными этой группы отмечается тот факт, что использование термина «компьютерные преступления» в области уголовно-правового регулирования неприемлемо, однако его употребление целесообразно в криминологическом и криминалистическом аспектах, то есть когда речь идет о личности преступника или способе совершения преступления[5].

Законодательным органом Российской Федерации было принято решение отказаться от понятия «компьютерные преступления», введя в Уголовный кодекс 1996 г. гл. 28 «Преступления в сфере компьютерной информации». В ходе принятия этого понятия в состав кодекса, законодательными органами власти также было проведено отождествление этого термина от других правонарушений по характеристике объекта совершаемого преступления. В рассматриваемом случае, компьютеры и электронные устройства не являются объектом орудия, с помощью которого совершается правонарушение в изучаемой категории преступлений. Орудием преступления в данном случае являются информационные отношения, складывающиеся в процессе создания, обработки, накопления, хранения, поиска, распространения и предоставления

[4] Батурин Ю. М, Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. М., 1991. С. 30-31.

[5] Вехов В. Б. Компьютерные преступления : Способы совершения, методики расследования. М., 1996. С. 24–25.

потребителю компьютерной информации, а также создания и использования информационных технологий, средств их обеспечения и, главным образом, защиты охраняемой законом компьютерной информации.

Российское уголовное законодательство под преступлениями в сфере компьютерной информации предусматривает общественно опасные деяния, определенные в гл. 28 Уголовного кодекса РФ: «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[6].

На настоящее время, глава 28 Уголовного кодекса РФ включает в себя четыре состава:

• Статья 272. Неправомерный доступ к компьютерной информации;

• Статья 273. Создание, использование и распространение вредоносных компьютерных программ;

• Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

• Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

В литературных источниках, имеющих актуальность на данное время, понятие “преступления в сфере компьютерной информации” считается абсолютно аналогичным и взаимозаменяемым термину «компьютерные преступления», но существует позиция, согласно которой, термин «компьютерные преступления» обладает намного более широким смыслом. В смысловой охват этого термина входят такие преступления, в которых применяется использование электронных устройств, компьютерной техники, информационных программ, компьютерной информации и цифровыми каналами связи. В данном случае, все эти действия, материальные и

[6] Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон от 13 июня 1996 г. № 63-ФЗ : (в ред. от 17 апр. 2017 г.) // КонсультантПлюс : справ. правовая система. Версия Проф. Электрон. дан. М., 2020. Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

нематериальные предметы являются орудиями совершения преступления или объектом посягательства. В круг таких правонарушений относят такие операции, как: мошенничество с использованием пластиковых банковских карт (carding), мошенничество с выманиванием персональных данных (fishing), незаконное пользование услугами связи и иной обман в области предоставления услуг связи, корпоративный промышленный и иной шпионаж, где информационные системы выступают в роли объекта преступления.

В иностранных литературных источниках и в большинстве официальных документов термин «computer crime» зачастую заменён термином «cyber crime» – киберпреступность, киберпреступление. Существует несколько определений этого термина, в том числе, они подразделяются на определения в широком смысле и узком.

Часть группы исследователей в данной области привязывают киберпреступность к преступлениям, совершаемых в различных информационных сетях. Так, по мнению А.В. Суслопарова : «термин "киберпреступность" оправдан, если мы говорим о совершении компьютерных преступлений в рамках компьютерной сети, в частности, сети Интернет»[7].

Высказана также точка зрения, согласно которой, «киберпреступность относят к преступлениям, совершаемым посредством компьютерной техники против различных прав и благ человека»[8] - такой позиции придерживается В.А. Номоконов.

В.А. Номоконов и Т.Л. Тропина обращаются к толковым словарям Оксфордского и Кембриджского университетов, и определяют приставку кибер (cyber) как «относящийся к информационным технологиям, сети Интернет, виртуальной реальности» и «включающий в себя использование компьютеров или относящийся к компьютерам, особенно к сети Интернет»[9].

Существует также группа учёных, по мнению которых, все эти понятия,

[7] Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера : дис. … канд. юрид. наук : 12.00.08. Красноярск, 2010. С. 24.

[8] Номоконов В. А. Актуальные проблемы борьбы с киберпреступностью // Компьютерная преступность и кибертерроризм. Запорожье, 2004. Вып. 1. С. 77.

[9] Номоконов В. А., Тропина Л. В. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 47.

трактовки и термины можно объединить в одну смысловую группу. Согласно Т.Л. Тропиной, киберпреступность – это «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных»[10].

## 1.2 Структура и состояние преступлений в сфере компьютерной информации в Российской Федерации

В сети Интернет и в сфере высоких технологий ежегодно фиксируется огромное количество преступлений. Способы и формы преступных посягательств постоянно совершенствуются.

Наибольшей популярностью у правонарушителей пользуются такие деяния как распространение вирусных программ, взлом аккаунтов в социальных сетях, хищение платежных реквизитов банковских карт (номер карты, срок действия, имя владельца, CVV-код и пр.). Сеть Интернет активно используется и для совершения иных преступлений. Так, в сети в последнее время участились случаи краж и мошенничеств, продажи наркотических веществ, распространения клеветы и персональных данных, а также распространения иной противоправной информации, в том числе экстремистского и порнографического характера.

С позиции криминалистики способы неправомерного доступа к компьютерной информации могут быть классифицированы на три группы:

- способы непосредственного доступа, когда преступник имеет доступ к чужому электронному устройству и совершает преступление непосредственно на нем;
- способы удаленного доступа, когда преступник совершает преступление посредством локальной сети или Сети Интернет;
- комплексные способы, предполагающие сочетание непосредственного

[10] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовноправовые меры борьбы : автореф. дис. ... канд. юрид. наук : 12.00.08. Владивосток, 2005. С. 9.

и удаленного доступа.

Лиц, совершающих компьютерные преступления (киберпреступления), в криминалистической литературе разделяют на несколько категорий. Традиционно выделяют следующие типы преступников:

а) обычные нарушители правил пользования ЭВМ – лица, не имеющие особых навыков в использовании компьютерной техники, но в силу ряда причин совершающие преступления (испытывающие чувство обиды сотрудники компаний, учащиеся образовательных учреждений);

б) лица, имеющие профессиональные познания в сфере информационных технологий:

- «беловоротниковые» преступники - лица, выступающие в роли представителей государства, бизнеса, должностных лиц и чиновников;
- «компьютерные шпионы» - подготовленные профессионалы, целью которых является получение важных стратегических данных о противнике в экономической, политической, технической и других сферах;
- «хакеры» («одержимые программисты») – технически подготовленные лица, которые, совершая преступления, часто не преследуют при этом прямых материальных выгод (для них имеет значение самоутверждение, месть за обиду, желание подшутить и тому подобное)[11].

Потерпевшими от преступлений подобного рода чаще всего являются юридические лица, и гораздо реже – физические лица. Это обусловлено прежде всего тем, что юридические лица в большей степени охвачены процессом компьютеризации и технологизации, нежели рядовые граждане. Обычно называют три категории потерпевших от преступлений в сфере компьютерной

[11] Прудиус Е. В. Криминалистическая характеристика преступлений в сфере компьютерной информации // Евразийский союз ученых. 2017. №. 11–2 (44). С. 96.

информации:

1) собственники электронно-вычислительных устройств и систем;
2) клиенты, пользующиеся их услугами,
3) иные лица.

Число совершенных преступлений с помощью информационных технологий растет с каждым годом. Характеризуя состояние преступности, отмечаем, что по данным портала Право.ру, за первое полугодие 2019 года в Российской Федерации было зарегистрировано 117 640 преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации, что на 47 % больше по сравнению с аналогичным периодом 2018 года. А уже в январе 2020 года на 75/2% (28,14 тысяч) стало больше подобных преступлений, чем в январе 2019 года. Предварительно расследовано 6,15 тысяч преступлений из общего числа, что на 51,7% выше уровня 2019 года.

В начале 2019 года государственная корпорация «Ростелеком» опубликовала данные, из которых следует, что в 2018 году специалистами Центра мониторинга и реагирования на кибератаки «Ростелекома» Solar JSOC было зарегистрировано более 700 тысяч кибератак, что на 90 % больше, чем в 2017 году. Жертвами большинства кибератак были кредитно-финансовые организации, а также предприятия в сфере электронной коммерции и игрового бизнеса. Доход хакеров составил порядка 2 млрд. рублей[12].

В 2020 году уже стали появляться отделы по борьбе с киберпреступлениями. Но быстро добиться кардинальных улучшений в раскрытии таких преступлений не возможно, так как отсутствует единый алгоритм раскрытия, очень много схем их совершения. И для этого обходимо не только, открывать новые подразделения с большим количеством кадров, но и обеспечивать их современными технологиями.

Исследователи отмечают, что причинами роста преступности в сфере компьютерной информации и ИКТ являются в том числе:

[12] Шмырова В. Киберпреступность в России растет быстрее любых других видов преступлений [Электронный ресурс] // Интернет-издание о высоких технологиях – CNews. Электрон. дан. [Б. м.], 1995–2020. URL: https://safe.cnews.ru/news/top/2019-09-27_kiberprestupnost_v_rossii (дата обращения: 08.03.2020).

а) несоответствие правового регулирования отношений в сфере компьютерной информации уровню технологического развития;
б) неправильная организация в учреждениях доступа к охраняемой законом информации (государственной, коммерческой тайне):
    1) предоставление всем сотрудникам бесконтрольного доступа к охраняемой законом тайне, в том числе к финансово-хозяйственной информации ограниченного доступа;
    2) отсутствие категорий допуска сотрудников к соответствующей информации;
    3) некомпетентность или отсутствие ответственного лица или специального отдела, отвечающего за предоставление доступа к охраняемой законом информации и обеспечение ее защиты;
    4) отсутствие или несовершенство договоров с сотрудниками о неразглашении охраняемой законом информации;
в) несовершенство используемого программного обеспечения (ПО):
    1) наличие уязвимостей в ПО;
    2) несовершенство парольной системы защиты ПО или ее полное отсутствие[13].

Стоит отметить, что преступления в сфере компьютерной информации и информационно-коммуникационных технологий отличаются крайне высокой латентностью. По разным оценкам, количество совершенных, но незарегистрированных преступлений в данной сфере минимум в три-четыре раза превышает официальные показатели. В качестве основных причин латентности данной категории преступлений называют:

- отсутствие у потерпевших особых познаний в сфере информационно-коммуникационных технологий. Как правило, обычный пользователь не замечает того факта, что к его устройству осуществлен несанкционированный доступ посторонних лиц, поскольку

[13] Кесареева Т. П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет : дис. ... канд. юрид. наук : 12.00.08. М., 2002. С. 15.

большинство процессов протекает в обычном режиме;

- неготовность потерпевших, обнаруживших утечку информации, обращаться в правоохранительные органы и производить обнародование факта утечки. Как правило, подобное наиболее характерно для кредитных организаций и крупных хозяйствующих субъектов. Это объясняется тем, что организации не готовы нести репутационные потери и терпеть убытки в связи с производством предварительного расследования (например, изъятие оргтехники, вызовы на допросы руководителей и сотрудников фактически могут заблокировать привычную хозяйственную деятельность);
- недоверие потерпевших к деятельности правоохранительных органов, отсутствие у них уверенности в раскрытии преступления и наказании виновных (возмещении убытков);
- незнание потерпевшими своих прав и неготовность отстаивать их законными методами.

Расследование подобного рода преступлений также сопровождается большими сложностями для правоохранительных органов. Такими проблемами, в частности являются[14]:

- оперативное и умелое сокрытие следов преступления. Для правонарушителей, имеющих специальные познания и навыки в области информационных технологий, как правило, не составляет большого труда сокрыть следы преступления или замаскировать их;
- значительный временной промежуток между совершением преступления и его обнаружением. Как правило, преступления в сфере высоких технологий обнаруживаются спустя недели, а то и месяцы, с момента их совершения. За это время преступник успевает не только уничтожить улики, но и убежать от следствия посредством переезда в другой регион или страну;
- значительные сложности в квалификации содеянного. Они

[14] Репин М. Е., Афанасьев А. Ю. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия // Молодой ученый. 2015. № 15. С. 461.

обусловлены не только проблемами законодательной техники и отсутствием внятных разъяснений от судебных инстанций, но и транснациональным характером данного вида преступности. К сожалению, правовой статус пользователей сети Интернет недостаточно урегулирован на международном уровне, а потому при совершении преступлении в сети неизбежно возникает вопрос о применимом уголовном праве и о юрисдикции;

- разнотипность телекоммуникационных систем и наличие огромного количества пользователей, подключенных к разным информационным системам, а также отсутствие единой системы защиты компьютерной информации;
- отсутствие у правоохранительных органов единой методики расследования подобных преступлений, несоответствие имеющихся локальных методик требованиям обстановки и времени;
- отсутствие у сотрудников правоохранительных органов специальных познаний в сфере информационно-коммуникационных технологий[15];
- отсутствие единого понятийного аппарата и значительные терминологические различия в базовых документах, определяющих порядок и ход расследования компьютерных преступлений.

Некоторые авторы также упоминают проблему «отсутствия должного статистического учета попыток несанкционированного доступа к информационным ресурсам любого характера и уровня. Отсутствие статистики приводит к ошибкам в оценке финансовых потерь, являющихся следствием недостаточной защиты компьютерной сети»[16].

Таким образом, недостаток комплексных мер противодействия, их противоречивость и фрагментарность, высокая латентность преступности в сфере компьютерной информации приводят к неэффективности их

[15] Матмуратов Б. Д. К вопросу об объекте посягательства и предмете хищения компьютерной информации // Вестн. Каракалп. фил. АН УзССР. 1987. № 3. С. 59.

[16] Репин М. Е., Афанасьев А. Ю. Преступления в сфере компьютерной информации… С. 462 ; Афанасьев А. Ю., Репин М. Е. Некоторые особенности расследования компьютерных преступлений // Студенческие южно-уральские криминалистические чтения. Уфа, 2015. С. 34.

предупреждения и расследования, обуславливая трудности в противодействии и борьбе с данным видом общественно опасных деяний.

## 1.3 Классификация преступлений в сфере компьютерной информации и способы их совершения

Направленные усилия многих государств на борьбу с преступлениями в сфере компьютерной информации не способствуют их сокращению. Исходя, из этого в настоящее время актуальным является исследования типологий подобных информационных преступлений и проводится анализ по выявлению способов их совершения.

В настоящее время наиболее распространена классификация компьютерных преступлений, основанная на Конвенции Совета Европы о киберпреступности.

23 ноября 2001 г. в Будапеште была подписана Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185[17]. Она была подписана государствами-членами Совета Европы, а также США и Японией. В настоящий момент Россия не подписала Конвенцию. Тем не менее, Конвенция содержит важные положения и проводит классификацию киберпреступлений, выделяя их виды в 5 групп.

Первая группа: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, такие как незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему.

Как показывает практика при оценке неправомерного доступа компьютерной информации, возникают трудности, так как информация находится в открытом доступе, разрешена к копированию. Таким образом, данные действия будут наказуемы только при условии доступа к информации, охраняемой законом. Преступления, относящиеся к первой группе являются самыми распространенными (78,4% от общего числа «компьютерных» преступлений за 2015г., 91,8% - за 2016г., 90,7% - за 2017г., 88,2% - за 2018г.)

[17] Convention on Cybercrime [Electronic resource] // Counsil of Europe. Electronic data. [S. l.], 2020. URL: https://www.coe.int/en/web/conventions/ full-list/-/conventions/treaty/185/ (access date: 20.10.2019).

Вторая группа: преступления, связанные с использованием компьютера, как средства совершения преступлений – а именно, как средство манипуляций с информацией. Шевченко Е.С. в своей работе указывает, что: « в эту группу входят компьютерное мошенничество и компьютерный подлог[18]».

Третья группа: преступления, связанные с содержанием информации, размещаемой в сети Интернет. «Самый распространенный и наказуемый практически во всех государствах вид этих киберпреступлений – преступления, связанные с детской порнографией», - считает О.В. Лисина[19].

Четвертая группа: преступления, связанные с нарушением авторского права и смежных прав. Однако установление таких правонарушений Конвенцией отнесено к компетенции национальных законодательств государств.

Пятая группа: преступления, связанные с распространением расистских и ксенофобских материалов в сети Интернет.

Анализируя уголовные дела по преступлениям в сфере компьютерной информации и изучая работы отечественных ученых в сфере киберпреступлений, возможно выделение более 20 основных способов совершения компьютерных преступлений.

На наш взгляд, их можно объединить в три основные группы:

1. Это способ совершения преступления связанный с непосредственным доступом, при этом информация либо уничтожается, либо блокируется, либо модифицируется, либо копируется, также нарушается работа компьютеров, на которых находится информация.

Совершают такие преступления либо сами работники, которые имеют отношение к этой работе, либо лица, которые специально проникли на охраняемую территорию, что на данный момент уже не актуально.

Уничтожение информации – это когда информация не может быть

[18] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений : автореф. дис. … канд. юрид. наук : 12.00.12. М., 2016. С. 28.

[19] Лисина О.В. Проблемы противодействия молодежному киберэкстремизму в условиях интернетсоциализации: вопрос нравственного здоровья подрастающего поколения // Теория и практика общественного развития. 2017. № 1. С. 49.

восстановлена.

Блокирование информации – создание условий, при которых возникает невозможность осуществления информацией своих функций.

Модификация информации – изменение содержания первоначальной индификации.

Копирование – изготовление одного или более дубликатов оригинала информации. Нарушения работы ЭВМ, системы ЭВМ или их сети (любая ситуация, которая препятствует нормальному функционированию вычислительной технике).

Непосредственный доступ может совершаться как лицами, работающими с информацией (имеют отношение к этой работе), так и лицами, специально проникающими в закрытые зоны и помещения, где обрабатывается информация.

Указанный способ в настоящее время не используется широко из-за децентрализации обработки компьютерной информации. Другими словами, именно во время передачи по телекоммуникационным каналам и компьютерным сетям эти данные легко заполучить, нежели путём фактического пребывания в помещении.

Зачастую преступник, имея цель изъять информацию, оставленную пользователями после работы ЭВМ, осматривают рабочие места, дабы найти черновые записи. Восстановление стертых программ имеют ту же цель.

2. Это способ удаленного доступа к компьютерной информации, который совершается через компьютерные сети с другого компьютера путем:

- Подключения к линиям связи (например, к телефонной линии) и получение доступа к системе.
- Проникновение к чужим информационным сетям путем автоматического перебирания абонентских номеров с последующим соединением с тем или иным компьютером (перебирание совершается до тех пор, пока на противоположном конце линии не “отзовется” чужой компьютер).

Не трудно обнаружить несанкционированного пользователя при совершении попытки незаконного доступа. Поэтому «взлом системы» происходит не с одного компьютера, а нескольких. Система защиты отсекает несколько «атакующих» компьютеров, тем самым давая другим доступ. Компьютер, который смог преодолеть защиту, блокирует систему статистики, фиксирующую все попытки заполучить доступ.

Это даёт возможность другим компьютерам оставаться не замеченными. Часть из них работает над взломом нужного сектора сети, остальные - нарушают работу предприятия и прикладывают усилия, чтобы сокрыть преступление.

- Подбора паролей с целью доступа в чужой компьютер. Для реализации такого подбора существуют уже специально разработанные программы, которые можно приобрести на “черном” компьютерном рынке.

Чтобы подобрать восьмизначный пароль - потребуется не более суток. После злоумышленник получает доступ к необходимой информации и возможность совершать те или иные действия как законный пользователь, такие как: копирование, модифицированием, уничтожение, проводить денежные операции, фальсифицировать платежные документы и т.д.

3. Смешанные способы:

• введение (тайное) в чужую программу таких команд, которые помогают ей совершить новые, незапланированные функции, сохраняя при этом ее работоспособность (программа выполняет копирование файлов, но одновременно уничтожает данные о финансовой деятельности предприятия);

• модификация программ путем тайного размещения в программе набора команд, которые должны сработать в определенных условиях через некоторое время. Например, как только программа незаконно перечислит денежные средства на так называемый подставной счет, она самоуничтожится и уничтожит при этом всю информацию о совершенной операции;

• совершение доступа к базам данных и файлам законного пользователя

через слабые места в системах защиты. В случае их выявления, появляется возможность читать и анализировать содержащуюся в системе информацию, копировать ее, обращаться к ней в случае необходимости. Таким образом можно обращаться к базе данных конкурирующей фирмы и иметь возможность не только анализировать ее финансовое положение, но и получать информацию о перспективах развития. Получение такой информации дает возможность получить явные преимущества в конкурентной борьбе;

• использование ошибок логики построения программы и обнаружение “брешей”. При этом программа “разрывается” и в нее вводится необходимое количество определенных команд, помогающих ей совершать новые, незапланированные функции, сохраняя при этом ее начальную работоспособность. Именно таким образом можно переводить деньги на подставные счета, получать информацию о недвижимости, персональных данных и т.д.

## 1.4 Основные элементы криминалистической характеристики преступлений в сфере компьютерной информации

### 1.4.1 Личность преступника

Знания о личности преступника очень важны в следственной практике, в связи с тем, что помогают существенно сузить круг подозреваемых, предположить, какие мотивы сподвигли на совершение преступного деяния, дать основания для предположения о месте нахождения преступника. Изучение следственной практики позволяет прийти к выводу о том, что чем сложнее примененный способ совершения преступления, тем уже круг подозреваемых лиц, которые могут обладать такого уровня специальными знаниями.

Появлению новых правоотношений между людьми поспособствовало такое явление как научно-технический прогресс. Отрицательная тенденция роста преступности в сфере компьютерных технологий стала следствием данного прогресса.

В процессе расследования подобных преступлений специалисты

сталкиваются с проблемами, которые обусловлены своеобразностью данного вида деяния, то есть средства и способы, применяемые, касательно этой категории имеют недоработанный вид, что является допущением криминалистической науки. Для устранения данной проблемы «в криминалистической литературе уделяется повышенное внимание методике расследования компьютерных преступлений, в данной области еще остается ряд нерешенных и дискуссионных вопросов. А именно, нуждается в уточнении криминалистической характеристики лиц, которые совершают преступления в сфере компьютерной информации»[20].

В криминалистической науке существует огромное количество классификаций лиц, которые совершают преступления в сфере компьютерной информации.

Стоит обратить внимание на Классификацию А.В Кузнецова, с ее помощью данных преступников можно разделить на три категории:

- первая группа это лица, имеющие устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма, изобретательности. Средства компьютерной техники принимается за вызов их творческим и профессиональным знаниям, умениям и навыкам;

- вторая группа лиц, страдающих новым видом психических заболеваний: информационными или компьютерными фобиями;

- в третью группу входят профессиональные «компьютерные» преступники, имеющие корыстные мотивы.

Автор считает, что указанная группа является наиболее опасной для общества[21]. Поэтому мы можем придти к выводу, что преступником данного вида преступления может быть не только специалист со стажем работы в сфере компьютерной информации, но и в зависимости от цели им может выступать

[20] Головин А. Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации [Электронный ресурс] // Центр исследования проблем компьютерной преступности. Электрон. дан. [Б. м.], 2001–2002. URL: http://www.crime-research.org/library/Golovin.htm (дата обращения: 07.01.2018).

[21] Кузнецов А. В. Некоторые вопросы расследования преступлений в сфере компьютерной информации // Информационный бюллетень следственного комитета МВД РФ. 1998. № 2. С. 42-48.

любой человек, который обладает хотя бы минимум базовыми знаниями.

Целью такой категории преступлений являются корыстные побуждения, которые выражаются в краже, реализации похищенного программного обеспечения, получение охраняемой законом информации и передача ее третьим лицам за определенное вознаграждение, неправомерный доступ к бесплатным каналам связи, совершение экономических преступлений посредством информационных технологий. Особое внимание можно уделить преступлениям из хулиганских побуждений, которые не имеют цель личного интереса, а только нанесение вреда какому либо лицу[22].

Стоит отметить, что возраст преступников данной категории преступлений от 15 до 45 лет. К примеру, по данным некоторых исследователей, на момент совершения преступления возраст 13% преступников старше 40 лет, 33% - не превышал 20 лет и 54% - 20-40 лет.

Так же было отмечено, что из 100% данных преступлений только 1% совершают лица женского пола. Виновные в преступлении ранее не привлекались к уголовной ответственности.

Стоит выделить, что 87% преступников - это служащие предприятий, организаций у которых работа была связана с информатизацией. Преступники в данной области в большинстве случаях – добросовестные работники, с положительными характеристиками, ответственные, состоящие в браке и имеющие детей.

Как показывает статистика в период с 2014 по 2016 год из 34 привлеченных к уголовной ответственности, только 8 граждан осуждено (это 23,5%), по остальным лицам дела были прекращены по основаниям, предусмотренным Уголовно- процессуальным кодексом РФ. К осужденным применялись следующие виды наказания:

- штраф;
- ограничение свободы и штраф;

[22] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М., 2002. С. 161.

- условное лишение свободы и штраф.

Практика показывает, что судьи вынося, решение о назначении наказания руководствуются требованием ст. ст. 6, 60 УК РФ, учитывают степень опасности содеянного, смягчающие и отягчающие обстоятельства наказания, данные о личности виновного. Судами не выносились приговоры назначения наказания с реальным отбыванием срока в колониях.

Так, приговором Гусь-Хрустального городского суда Владимирской области от 30 марта 2015 года Л. осужден за совершение преступлений, предусмотренных ч. 1 ст. 272, ч. 1 ст. 273, ч. 1 ст. 272, ч. 1 ст. 273, ч. 1 ст. 272, ч. 1 ст. 273 УК РФ, ч. 2 ст. 69 УК РФ, к наказанию в виде штрафа в размере 35 000 рублей. Определяя виновному наказание суд учел, смягчающие наказание Л. обстоятельства и отсутствие отягчающих. Принял во внимание, что Л. трижды совершил преступления небольшой и средней тяжести, ранее не судим, к административной ответственности не привлекался, по месту жительства характеризуется положительно. Суд посчитал необходимым применить положения ст. 64 УК РФ по ч. 1 ст. 273 УК РФ (по каждому эпизоду) и назначить Л. более мягкое наказание, чем предусмотрено санкцией указанной статьи.

Г.Т. Мегрелишвили автор работы «Криминологический и психологический портрет личности преступников в сфере высоких технологий» делит киберпреступников на несколько групп:

1. К первой группе автор относит лиц, отличительной особенностью которых является сочетание профессионализма и фанатизма в области компьютерной техники и программирования». Такие лица не имеют четкого противоправного намерения, действуют исключительно для проявления своих профессиональных и интеллектуальных способностей. Они любознательны и азартны. Повышение мер по обеспечению компьютерной безопасности рассматривают как вызов их способностям.

Главной особенностью совершения преступлений в сфере компьютерной информации данной группой лиц является то, что отсутствует подготовка и

план действий, оригинальность способа совершения

2. Вторая группа – лица, страдающие новым видом психических расстройств, признанные Всемирной организацией здравоохранения: информационные заболевания, компьютерные фобии.

3. Третью группу лиц – являются высококвалифицированными специалистами, чаще всего имеющими высшее техническое образование. Но, в отличие от первой группы, это профессионалы с устойчивыми преступными навыками и ярко выраженными корыстными целями. Совершают компьютерные преступления многократно и принимают меры по сокрытию своих действий[23].

Степанов В.В. и Бабакова М.А. в зависимости от сферы (направления) преступной деятельности выделяют:

1. хакеров (hackers);

2. крэкеров (crackers);

3. кардеров (carders);

4. фишеров (fishers);

5. спамеров (spammers).

Само возникновение преступлений в сфере компьютерной информации можно связать с деятельностью компьютерных взломщиков, получивших название «хакеры». Этот термин является неофициальным, и можно встретить различные его толкования. Одни авторы утверждают, что ха́кер – это чрезвычайно квалифицированный специалист, человек, который понимает самые основы работы компьютерных систем и не причастен к компьютерным преступлениям.

Яблоков Н.П. же считает, что: «хакер (англ. «hack» – разрубать) — пользователь вычислительной системы, занимающийся поиском незаконных способов получения несанкционированного доступа к компьютерным данным в совокупности с их несанкционированным использованием в корыстных

[23] Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий // Вестн. Том. гос. ун-та. 2007. № 299. С. 180–181.

целях»[24].

На сегодняшней день хакер – это не просто какой-либо человек со специальными знаниями и навыками, это – образ жизни, своя субкультура со своими правилами. Хакеры обычно обладают достаточно высокими специальными познаниями и практическими навыками в области новых компьютерных технологий. Обычно, это увлеченные компьютерной техникой школьники, студенты и молодые специалисты, совершенствующиеся на данном виде деятельности.

Большая часть людей, занимающиеся хакерской деятельностью, специализируются, как правило, в какой-либо конкретной области.

По роду занятий можно выделить следующие типы хакеров:

1. Хакер сетевой (network hacker) – занимается исследованием программного обеспечения, установленного на серверах (или в локальных сетях), с целью получения несанкционированного доступа к серверу или нарушения его работы. Для такого вида деятельности необходимо хорошее знание сетевых протоколов и архитектуры операционных систем.

2. Кракер (cracker) – занимается взломом прикладного программного обеспечения с целью получения доступа к информации ради ознакомления.

3. Фрикер (phreaker) – исследует телекоммуникационные сети с целью найти возможность звонить и пользоваться каналами связи бесплатно.

4. Кардер (carder) – занимается нелегальным получением номеров кредитных карт и сведений об их владельцах. Кардерство считается наиболее серьезным преступлением, и поэтому является самым опасным видом хакерской деятельности.

5. Вирусописатель (virus maker). Само утверждение о том, относится ли написание вирусов к хакерской деятельности, весьма спорно, так как «кодекс» хакеров запрещает использование своих знаний во вред пользователям. Однако уже сегодня известно множество случаев создания вирусов, которые можно использовать, например, в корыстных целях. Наиболее известный на

[24] Яблоков Н. П. Криминалистика. М., 2005. С. 406.

сегодняшний день случай – это заражение вредоносной программой «WannaCry», созданной с целью шифрования данных и вымогательства определённой суммы с пользователей за возможность восстановить свои файлы, сотен тысяч ПК (в более чем 150 странах, в России пострадали МВД России, МегаФон, РЖД) под управлением операционной системы Microsoft Windows.

Атаки хакеров происходят во всем мире каждые 14 секунд, а к 2021 году их частота возрастет до 11 секунд.

Утечка конфиденциальной информации увеличивается с каждым годом. Только за прошлый год утекло более 14 млрд. записей. Рост числа утечек во всем мире увеличился на 10%, в России – более чем на 40% по сравнению с 2018 годом. Но общее число, зарегистрированных киберпреступлений составляет 10 – 12% от фактического числа, так как граждане или организации не обращаются за помощью правоохранительные органы из-за боязни, что украденную информацию опубликуют. Среди самых крупных утечек данных в России в 2019 году была утечка из компании «Билайн», когда сведения около 9млн. абонентов (ФИО, мобильные и домашние телефоны) выложили в сеть.

«Мы считаем верным утверждение, что причиной девиантного поведения компьютерных пользователей является влияние, которое оказывает на их сознание киберпространство». Данная теория была предложена профессором Джоном Сулером (США). Им было введено понятие «эффект онлайн дезингибиции»[25]. Сущность данного эффекта заключается в том, что в условиях анонимности в киберпространстве люди отделяют свои действия и свою реальную личность, полагая, что может не брать на себя ответственность за свои действия, совершенные в киберпространстве.

При расследовании компьютерных преступлений необходимо применение юридической психологии в силу отсутствия достаточного количества материальных следов преступника, множественности возможных

[25] Suler J. The Psychology of Cyberspace [Electronic resource] // Rider University. Electronic data. [S. l., s. a.]. URL: http://users.rider.edu/~suler/ psycyber/psycyber (access date: 30.11.2018).

мотивов киберпреступников, невозможность установления определенного круга лиц, которые могли совершить преступление, также потенциально большой ущерб, который может нанести киберпреступление.

### 1.4.2 Обстановка совершения преступлений в сфере компьютерной информации

Изучение обстановки совершения преступления необходимо для криминалистической характеристики киберпреступлений. В настоящее время данный вопрос в литературе недостаточно разработан и требует дальнейшего изучения и исследования[26].

Обстановка совершения преступлений включает в себя взаимодействующие между собой до и в момент преступления объекты, процессы и явления, характеризующие время, место, вещественные и иные условия окружающей среды, поведение непрямых участников преступления и другие факторы, определяющие возможность, условия и обстоятельства совершения преступления. Обобщенные знания об обстановке преступления, находящейся во взаимосвязи с другими элементами криминалистической характеристики, позволяют акцентировать внимание следствия на более эффективный поиск и установление обстоятельств, входящих в предмет доказывания[27].

Особенностью обстановки преступления является ее динамичность. Преступник всегда оценивает существующую обстановку до и в момент совершения преступления как благоприятную или неблагоприятную, причем не всегда верно[28]. Следствие же, наоборот, при ретроспективной направленности расследования встречается с обстановкой, сложившейся после совершения преступления и зачастую измененной естественными, производственными,

[26] Поляков В. В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. … канд. юрид. наук : 12.00.09. Барнаул, 2009. С. 112.

[27] Поляков В. В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Изв. Алтайского гос. ун-та. 2013. № 2 (78). С. 114.

[28] Гавло В. К. Обстановка преступления как структурный компонент криминалистической характеристики преступления // Проблемы совершенствования тактики и методики расследования преступлений : сб. науч. трудов. Иркутск, 1980. С. 49.

случайными и иными факторами. Так, при осмотре места происшествия следователь встречается со следами преступника, затертыми посторонними лицами[29].

Специфика составляющей обстановки совершения киберпреступлений – время и место совершения. Действия происходят в виртуальном пространстве и использованием телекоммуникационных сетей, причем одновременно злоумышленником могут быть задействовано несколько компьютеров, находящихся в разных местах (порой в разных государствах)[30]. Каждое из таких мест имеет свою обстановку.

Следует отметить, что преступник действует не только в конкретной обстановке, но и в конкретное время, порой в значительной мере влияющее на его поведение. Работа некоторых программ связана со временем, установленным на компьютере, которое может быть изменено по желанию преступника. Установление точного времени совершения преступления является сложной задачей, разрешение которой не всегда возможно.

Обстановка сильно влияет на киберпреступников. Как показывает практика, в большинстве случаев проводится основательная подготовка к совершению преступления[31]. Проводится сбор и изучение необходимой информации, имеющихся технологиях, в частности о средствах защиты и их характеристиках. Задачей злоумышленника становится адаптация и внедрение в коммуникационные системы.

Обстановка изменяется с использованием преступником специальных средств совершения преступления, таковыми являются программные, аппаратно-программные средства, а также с наличием или отсутствием средств защиты компьютерной информации.

В результате киберпреступления в обстановке могут оставаться характерные изменения – электронно-цифровые следы. Однако они обладают

---

[29] Поляков В. В. Обстановка совершения преступлений… С. 114.

[30] Агибалов А. Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. … канд. юрид. наук : 12.00.09. Воронеж, 2010. С. 21.

[31] Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы. Омск, 2009. С. 243–246.

спецификой, которая проявляется в том, что многие изменения остаются практически незаметными.

Киберпреступлениям во многом способствует низкая информационная безопасность, не только частная, и корпоративная. Еще один фактор отмеченный В.В. Поляковым «косвенным образом способствует противоправной деятельности преступников … недостаточный уровень квалификации правоохранительных органов в области расследования преступлений в сфере высоких информационных технологий»[32].

Обстановка преступлений в сфере компьютерной информации несет в себе большую информационную базу. Поэтому очень важно знать ее признаки, особенности влияния на преступления, чтобы в дальнейшем иметь возможность составлять характеристики киберпреступлений.

### 1.5 Актуальные проблемы выявления и раскрытия преступлений в сфере компьютерной информации

Компьютерные преступления отличаются от преступлений других категорий. Но в большинстве случаях следователи применяют практику расследования наиболее распространенных преступлений. Соответственно и следственные действия проводят в обычном режиме, как осмотр места происшествия, обыск, изъятие техники и ее экспертиза, допрос и т.д. Отсутствие определенных знаний ведет к многочисленным ошибкам при ведении уголовных дел в сфере киберпреступлений, а именно доказательства изымаются с ошибками, нередко повреждаются в ходе экспертиз.

Так при проведении опроса сотрудников правоохранительных органов г.Рязани и Рязанской области было установлено, что главной проблемой в сфере компьютерной информации является недостаточная «техническая уведомленность» названных сотрудников.

Так, 97,5 % респондентов имеют высшее юридическое образование, и только 5 % (4 человека) получили второе техническое образование по

[32] Поляков В. В. Обстановка совершения преступлений… С. 115.

следующим специальностям: 02.00.00 – компьютерные и информационные науки, 09.00.00 – информатика и вычислительная техника, 11.00.00 – электроника, радиотехника и системы связи.

Еще одной проблемой, которая уже была указана в данной работе, является несвоевременность выявления компьютерных преступлений. Проводя опрос оперативных сотрудников можно придти к выводу, что уровень владения компьютером не высок.

72% опрошенных, определили, что их уровень знаний «Средний». Они могут самостоятельно использовать компьютерную технику для решения повседневных задач.

23% сотрудников оценили свои знания выше среднего, способные самостоятельно переустанавливать или обновлять программы, восстанавливать утраченные файлы и т.д.

И только 5% опрошенные оценили свои знания выше среднего, но даже они не всегда обладают достаточными знаниями.

Киберпреступники всегда на шаг впереди следователей. Выявление и раскрытие преступлений в сфере компьютерной информации на данном этапе развития компьютерной криминалистики занимают длительное время. Важная для расследования информация может быть утрачена из-за несвоевременных действий следователей. В 49% случаев с момента преступления в сети и до поступления информации о совершаемом преступлении в полицию проходит много времени (более 10 суток).

Трудности в расследовании киберпреступлений возникают и в момент осмотра места происшествия, так как обычно оно отсутствует.

Получение и анализ доказательств по делам о преступлениях в сфере информационных технологий – одна из самых главных и трудно решаемых на практике задач для всех государств. Ее решение требует не только разработки специальной методики производства следственных и организационных мероприятий, но и наличия специальных знаний в области компьютерной техники и программного обеспечения, а также внесения изменений в

действующее уголовно- процессуальное законодательство[33].

Вследствие опроса было выявлено, что 84% случаев медленное реагирование сотрудников полиции на преступления в сфере компьютерной информации - это отсутствие квалифицированных специалистов. Большинство оперативных сотрудников придерживаются стандартных следственных действий, а именно осмотр места происшествия, обыск, изъятие компьютерной техники, допрос подозреваемого.

При опросе сотрудников выяснилось, что у 82% опрошенных возникают сложности с определением места происшествия.

Деятельность эксперта-криминалиста при расследовании данного рода преступлений, с учетом их особенностей, является ключевой. Для эффективного расследования киберпреступлений необходимо включать в работу только специалистов в области информационных технологий, так как для распознавания следов в киберпространстве, изучения данных на цифровых носителях и сети Интернет, необходимы определенные знания, навыки и умения.

При проведении осмотра места преступления целесообразно привлечение эксперта-криминалиста, системного администратора и других специалистов, отталкиваясь от вида киберпреступления. При производстве сложных следственных мероприятий, считаю необходимым создание специализированных групп, которые занимаются расследованием исключительно киберпреступлений.

При расследовании киберпреступлений, все свои действия, следователю необходимо согласовывать со специалистом, особенно по причине приобщения к делу электронных следов.

Следует отметить проблемы, возникающие в ходе экспертно-криминалистической деятельности.

При назначении компьютерно-технической экспертизы, следователи

[33] Протасевич А. А., Зверянская Л. П. Борьба с киберпреступностью как актуальная задача современной науки // Криминологический журнал Байкальского гос. ун-та экономики и права. 2011. № 3. С. 32.

неверно ставят вопросы перед экспертом. 78% опрошенных лиц подтвердили, что не смогли бы точно сформулировать вопросы эксперту. Причиной этому, опять же, является некомпетентность следователей в этой сфере.

Большинство следователей считают, что для правильной постановки вопросов перед экспертом, при назначении экспертизы, им мог бы помочь перечень типовых вопросов[34].

Недостаточное количество специалистов, способных провести качественную экспертизу компьютерных систем (в некоторых регионах стран такие эксперты отсутствуют вообще). Это приводит к тому, что технико-криминалистические экспертизы проводятся с нарушениями и требуют много времени. В итоге, результаты экспертизы оказываются неэффективными для расследования. Всегда возникает трудность при расшифровке результатов экспертизы.

Исследование средств совершения компьютерных преступлений с позиций криминалистики, их типизация и классификация позволит установить корреляционные связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

Из всего сказанного можно сделать вывод о том, что выявление и раскрытие данных преступлений остается одной из трудных задач для уголовного розыска. Это связано с целым рядом проблем, которые необходимо решать:

- отсутствие мониторинга следственной и судебной практики
- опыта работы
- подготовкой сотрудников к работе с киберпреступлениями
- отсутствие методических рекомендаций по расследованию преступлений в сфере высоких технологий

[34] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений : автореф. дис. … канд. юрид. наук : 12.00.12. М., 2016. С. 28.

## 2 Первоначальный этап расследования преступлений в сфере компьютерной информации

### 2.1 Обстоятельства, подлежащие установлению при расследовании преступлений в сфере компьютерной информации

При расследовании того или иного преступления перед следователем, в первую очередь, стоит проблема определения обстоятельств, которые подлежат установлению, так как именно они выступают базой для постановки общих и частных задач, которые необходимо решить в ходе расследования.

На признаки несанкционированного доступа или подготовки к нему могут указывать следующие явные обстоятельства: возникновение в компьютере фальшивых данных; не обновление в период длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств; частые сбои в ходе работы компьютеров; участившиеся жалобы клиентов компьютерной системы или сети; осуществление сверхурочных работ без видимых на то причин; немотивированные отказы некоторых работников, обслуживающих компьютерные системы или сети, от отпусков; неожиданное приобретение сотрудником домашнего дорогостоящего компьютера; носители информации, принесенные на работу сотрудниками компьютерной системы под сомнительным предлогом перезаписи программ для компьютерных игр; участившиеся случаи перезаписи некоторых данных без серьезных на то причин; чрезмерный интерес отдельных работников к содержанию чужих распечаток (листингов), которые выходят из принтеров.

Уголовно-процессуальный кодекс РФ (ч.1 ст. 73) содержит общий перечень обстоятельств, подлежащих доказыванию по любой категории дел[35].

Согласно ч. 1 ст. 272 УК РФ: «неправомерный доступ к охраняемой законом компьютерной информации, это деяние повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной

[35] Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс] : федер. закон от 18 дек. 2001 г. № 174-ФЗ : (в ред. от 7 июня 2017 г.) // КонсультантПлюс : справ. правовая система. Версия Проф. Электрон. дан. М., 2020. Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

информации[36]».

При расследовании неправомерного доступа к компьютерной информации (ст. 272 УК РФ) особое внимание необходимо уделить установлению направленности деяния преступника, а именно – на информацию, охраняемую законом, хранящуюся в компьютерной системе, в сети или на машинных носителях, либо передаваемую с использованием средств компьютерной связи. Кроме этого, нужно доказать наличие причинно-следственной связи между противоправными деяниями лица и наступившими последствиями в виде уничтожения, блокирования, модификации либо копирования информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

При расследовании преступлений, которые связаны с созданием, использованием и распространением вредоносных программ для ЭВМ, для наступления уголовной ответственности очень важно доказать понимание виновным назначения подобного рода средств в качестве инструментов, изначально приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. При расследовании разработки компьютерных программ установлению подлежит именно факт создания программ, отдельных их компонентов, подпрограмм, модулей.

«При расследовании преступлений, связанных с нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети, следует обратить внимание на наличие специального субъекта – лица, имеющего доступ к ЭВМ, системе ЭВМ или их сети, и правило наступления уголовной ответственности только в том случае, если неправомерные действия причинили существенный вред», - подчеркивает Е.П. Ищенко[37].

Итак, мы рассмотрели наиболее распространенные преступления, совершаемые в сфере компьютерной информации, и определили перечень наиболее важных обстоятельств, которые необходимы для пристального

[36] Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон от 13 июня 1996 г. № 63-ФЗ…

[37] Ищенко Е. П., Топорков А. А. Криминалистика. М., 2005. С. 733.

изучения и установления при расследовании: личность преступника, личность потерпевшего, материальные следы компьютерных преступлений, обстановку совершения преступления. Весь комплекс соответствующей информации и материалов поможет в успешном раскрытии преступлений. Способы совершения преступлений в сфере компьютерной информации постоянно усложняются. В связи с этим теоретикам и практикам нужно следить за их развитием и разрабатывать новые методы противодействия. Для этого необходимо изучать следственную практику, научную литературу, специальную литературу, информацию, которую выкладывают сами хакеры в сети Интернет для того, чтобы обмениваться опытом.

## 2.2. Типичные следственные ситуации первоначального этапа расследования

В криминалистической литературе понятие и содержание следственной ситуации относятся к дискуссионным вопросам. Впервые определение понятия следственной ситуации дал в 1967 г. А. Н. Колесниченко: «определенное положение в расследовании преступлений, характеризуемое наличием тех или иных доказательств и информационного материала и возникающими в связи с этим конкретными задачами его собирания и проверки[38]»

Л. Я. Драпкин, заложивший основы теории следственной ситуации, определяет ее как «мысленную динамическую модель, отражающую информационно-логическое, тактико-психологическое, тактико-управленческое и организационное состояние, сложившееся по уголовному делу и характеризующее благоприятный или неблагоприятный характер процесса расследования[39]».

Белкин Р.С. говорил о том, что «следственную ситуацию составляет совокупность условий, в которых на данный момент осуществляется расследование, т.е. обстановка, в которой проходит процесс расследования[40]».

[38] Колесниченко Д. Н. Научные и правовые основы методики расследования отдельных видов преступлений : дис. … д-ра юрид. наук. Харьков, 1967. С. 10.

[39] Драпкин Л. Я. Основы теории следственных ситуаций. Свердловск, 1987. С. 17.

[40] Белкин Р. С. Курс криминалистики. М., 1997. Т. 2. С. 135.

Из вышесказанного можно сделать вывод о том, что следственную ситуацию можно рассматривать с двух аспектов – познавательного и информационного. С точки зрения познавательного аспекта следственная ситуация — это оценочная категория, а с точки зрения информационного - совокупность материальных и идеальных источников, которые возникают в определенный момент расследования.

Общими для любой следственной ситуации элементами выступают следственные и оперативно-розыскные данные о способе и механизме преступления, личности преступника, обстановке, цели и мотиве преступного посягательства, данные об обстановке, в которой осуществляется расследование, сведения о факторах, затрудняющих следственные действия и которые препятствуют им и т.д.

Следственные ситуации подразделяются на типичную и конкретную следственную ситуацию. Базовым компонентом следственных ситуаций является типичная следственная ситуация. Она характеризуется комплексом признаков, которые включают в себя «общие черты хода и состояния расследования к определенному его моменту», отражающих общие черты криминалистической характеристики данного вида преступлений и наиболее вероятную обстановку их расследования. Типовая ситуация отличается от конкретной, формирующейся при расследовании определенного дела и характеризующейся частными индивидуальными особенностями обстановки и связями, возникающими при его расследовании.

В свою очередь типичные следственные ситуации делятся на общие и частные. Типичные общие следственные ситуации содержат информацию, которая раскрывает процесс расследования с точки зрения ее полноты и достоверности по отношению к характеру события и лицу, которое причастно к этому событию. Типичные частные следственные ситуации характеризуют процесс расследования с точки зрения иных, частных обстоятельств, например, оказываемого противодействия следователю и суду. Если говорить о конкретной следственной ситуации, то она отражает индивидуальность и

своеобразие того или иного момента расследования.

На досудебной стадии между следователем и участником уголовного судопроизводства складываются отношения. И если рассматривать характер этих отношений, то следственные ситуации делятся на конфликтные и бесконфликтные. При конфликтной ситуации интересы следователя и участника процесса расследования не совпадают, а при бесконфликтной ситуации интересы совпадают полностью.

Для начального этапа расследования преступлений в сфере компьютерной информации наиболее типичны следующие ситуации:

а) собственник или обладатель компьютерной информации самостоятельно выявил факт преступления и обнаружил лицо, его совершившее[41]. В таких случаях проводятся:
   1) задержание подозреваемого;
   2) допрос подозреваемого;
   3) обыск по месту работы (службы) и жительства подозреваемых или иных лиц, где могут находится объекты, имеющие значение для расследования;
   4) осмотр места происшествия;
   5) осмотр изъятых носителей информации;
   6) допрос свидетелей;
   7) назначение судебных экспертиз;
   8) следственный эксперимент;

г) собственник или обладатель компьютерной информации самостоятельно выявил факт преступления, но преступник неизвестен. Для этой ситуации характерно:
   1) допрос заявителя;
   2) признание собственника или правообладателя потерпевшим;
   3) осмотр места происшествия;

[41] Подольный Н. А. Отдельные проблемы расследования преступлений, совершённых с применением компьютерных технологий // Библиотека криминалиста. Научный журнал. 2013. № 5 (10). С. 117.

4) поручение органу, осуществляющему оперативно-розыскную деятельность, о поиске преступников и фактов, имеющих значение для дела;
5) допрос свидетелей;
6) анализ обстановки и выдвижение версий по каждому обстоятельству, подлежащему установлению;
7) назначениеэкспертиз;
8) установление субъекта преступления и его задержание;

д) преступление выявлено органом дознания в результате оперативно-розыскной деятельности. При этом обычно проводятся[42]:

1) осмотр места происшествия;
2) допрос свидетелей;
3) обыск с изъятием документов и носителей информации;
4) следственный эксперимент;
5) прослушивание телефонных переговоров;
6) назначение судебных экспертиз.

С учетом сложившейся следственной ситуации формируется план расследования по делу в целом, по проверке некоторых эпизодов и обстоятельств. Также немаловажно отметить, что целенаправленная деятельность сотрудников правоохранительных органов, особенно на первоначальном этапе расследования компьютерных преступлений, обеспечивает успех дальнейшего расследования уголовного дела.

### 2.3 Следственные действия и ОРМ

Исследование действий, проводимых сотрудниками правоохранительных органов, в ходе проведения расследований преступлений, совершённых в киберпространстве и сети интернет, показало, что подробное изучение персональных компьютеров злоумышленников и используемых ими электронных устройств, должно проводиться в специально оборудованной

[42] Подольный Н. А. Отдельные проблемы расследования преступлений… С. 117.

криминалистической лаборатории, квалифицированным обученным IT специалистом, обладающим должным уровнем компетенции и релевантным уровнем опыта работы с соответствующими устройствами.

Доказательства, выявленные на месте совершения преступления, связанные с характерными преступлениями в сфере компьютерной информации, легко заменяемы и изменяемы, например, в виде совершённой ошибки при изъятии технических устройств, либо в ходе их дальнейшего исследования. Выявление, изучение и изъятие технических устройств, а также носителей информации в процессе проведения следственных действий могут быть совершены не только при проведении следственного осмотра, но и при исполнении стандартных действий следственного характера: обыска, изъятие, визуализация обстоятельств и обстановки происшествия[43].

Также, существует важная проблема, связанная с возможным опровержением в ходе судебного слушанья идентичности программного обеспечения, представленного в виде доказательства, и программного обеспечения, находившемся на персональном компьютере в момент изъятия.

Во избежание подобных ситуаций, необходимо производить опечатывание персонального компьютера в присутствии понятых, без включения питания. Также можно выделить рекомендации, касающиеся проведения исследования персонального компьютера непосредственно на месте происшествия[44]:

- при нахождении на моменте осмотра компьютера во включенном состоянии, перед выключением питания необходимо завершить запущенные процессы и выполняемые программы;
- рекомендуется установить пароль доступа к закрытым программам;
- в случае оказания противодействия сотрудниками организации, в процессе изъятия компьютерной техники, требуется произвести

[43] Чуриков Н. А., Медведев С. С. Преступления в сфере компьютерной информации: проблемы квалификации и совершенствования уголовного законодательства в данной сфере // Образование и наука в современных реалиях: материалы Междунар. науч.-практ. конф. Чебоксары, 4 июня 2019 г. Чебоксары, 2019. Т. 2. С. 313.

[44] Там же. С. 314.

опечатывание и обесточивание всех компьютеров, расположенных на объекте, и произвести изъятие вместе с носителями информации для проведения лабораторного исследования специалистом;

- в случае получения необходимой информации от сотрудников организации, информацию рекомендуется получать из различных источников методом опроса или допроса;
- вместе с электронными устройствами целесообразно производить изъятие периферийных устройств и внешних носителей данных;
- составить перечень сотрудников предприятия, владеющих доступом к компьютерной технике, либо имеющих санкционированный допуск на посещение помещений, в которых установлены компьютеры.

В случае наличия возможности непосредственного доступа к компьютерам и исключения абсолютного большинства нежелательных ситуаций, приступить к исследованию персонального компьютера, объясняя все свои действия присутствующим при осмотре понятым. В ходе осмотра необходимо произвести определение[45]:

- конфигурации ПК с подробным описанием подключенных к нему устройств и носителей информации;
- названия моделей и серийные номера (при их наличии) каждого устройства, подлежащего осмотру и изъятию;
- инвентаризационные номера, присваиваемые бухгалтерией учреждения при постановке поступившего оборудования на баланс организации;
- другую информацию, имеющуюся на фабричных ярлыках.

Информация, полученная в ходе осмотра, подлежит внесению в протокол осмотра компьютерной техники и будет важной при проведении следственных действий.

Перед началом процесса транспортировки происходит фотографирование

[45] Нехорошева О. Изъятие компьютерной техники и информации // Законность. 2004. № 8. С. 22.

предметов, подлежащих изъятию, и происходит маркировка элементов компьютера. Фотографировать требуется переднюю и заднюю части системного блока. Фотографирование подобным способом дает возможность точного воссоздания состояния компьютерной техники в лаборатории.

Фотофиксация конфигурации системы в ходе данного этапа необходима для последующего корректного подсоединения всех элементов в условиях лабораторного анализа и исследования.

Опыт следственной практики показал, что при более сложной технической реализации проникновения в компьютерную систему, либо компьютерную сеть, более лёгким оказывается обнаружение злоумышленника, так как знаниями и навыками, позволяющими произвести несанкционированный доступ на таком уровне, обладает очень узкий круг лиц.

Основными подозреваемыми на первых этапах предварительного расследования выступают те сотрудники, которые удовлетворяют следующим критериям:

- знали или могли знать о том, что на данном устройстве хранится информация, представляющая определенную ценность;
- обладают высоким навыком и специальными знаниями, позволяющими или предположительно дающими возможность совершения данного преступления;

Особого внимания заслуживают специалисты, которые занимаются защитой информации от несанкционированного доступа, т.к. они, как правило, самостоятельно «пишут» программы, которые направлены на защиту информации и знают все их слабые и сильные стороны[46].

Следует принять во внимание, что процесс выявления, раскрытия и расследования преступлений в сфере компьютерной информации, совершенно невозможен при отсутствии применения приёмов тактики и специальных методов деятельности оперативно-розыскного характера, а так же проведения оперативно-розыскных мероприятий, закрепленных в ст. 6 Федерального

[46] Нехорошева О. Изъятие компьютерной техники и информации... С. 16.

закона от 12.08.1995 № 144 «Об оперативно-розыскной деятельности»[47]. Особое внимание следует обратить на такие оперативно-розыскные мероприятия, как наведение справок; сбор образцов для сравнительного исследования; произведение наблюдения; исследование предметов и документов; перехват информационного потока с помощью каналов обмена информацией; получение информации из сторонних источников.

Как мы уже отмечали ранее в главе 1 настоящей диссертации, одной из основных проблем расследования преступлений в сфере компьютерной информации является отсутствие следов материальной природы в процессе подготовки и совершения противоправных действий, многообразие и изощрённость путей совершения преступления, сложность и невозможность точного определения места, времени совершения преступления, обстоятельств, а также его события.

Вирус в сети может быть выгружен в сеть с одного персонального компьютера, а инициирован на совершенно другом, что делает установку территориальных границ и сектора невозможным. Компьютерная информация имеет возможность в одном случае являться доказательством следов преступного посягательства, а в другом – следами совершённых преступлений.

Специалисты, характеризуя следы преступлений в сфере компьютерной информации, не приходят к общему мнению относительно их понятия и сущности. Теория криминалистики и практика показывает, что к следа м совершения преступления можно отнести различные изменения в исследуемой среде, образовавшиеся в ходе противоправного деяния[48].

Следы совершённого преступления можно разделить на материальные и нематериальные. К материальным следам относятся : отпечатки на материальных физических объектах, предметах, документах, телах потерпевших и другое. К нематериальным следам относятся : отпечатки

[47] Об оперативно-розыскной деятельности [Электронный ресурс] : федер. закон от 12 авг. 1995 г. № 144-ФЗ (ред. от 2 авг. 2019 г.) // КонсультантПлюс : справ. правовая система. Версия Проф. Электрон. дан. М., 2020. Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

[48] Глушков Е. Л., Емельянов Д. Е. Оперативно-розыскная деятельность при расследовании и раскрытии преступлений в сфере компьютерной информации // Вестн. Белгород. юрид. ин-та МВД России им. И. Д. Путилина. 2019. № 2. С. 46.

(события) в памяти, сознании граждан (потерпевшего, свидетеля, преступника и других лиц).

Делая аналитический вывод из характерных особенностей возникновения следов при совершении преступлений в сфере компьютерной информации выясняется, что они не подходят к вышеперечисленным классификациям.

Поэтому некоторые ученые (В.А. Мещеряков и др.) сделали вывод о необходимости введения понятия «виртуальные следы» - среднего между материальными и идеальными[49]. Данную позицию поддерживают А.К. Шеметов[50], Ю.В. Гаврилин[51], В.А. Милашев[52], поэтому, возможно, есть потребность пересмотреть криминалистическую теорию образования следов.

Можно с уверенностью сделать вывод, что в ходе выявления, раскрытии, расследовании преступлений, связанных с компьютерной информацией, следы являются основным составляющим элементом в ходе исследования, специальных экспертиз, а также в восстановлении механизма и очерёдности совершения противоправных действий.

Анализируя практику выявления, процесса раскрытия и расследования преступлений возникает необходимость установления и исследования следов не только в самих технических средствах (компьютерах), например, исследование входящих и исходящих сообщений, дату, время, но и способ передачи данных (канал связи). К каналу связи относится информация об отправленных сообщениях, содержащуюся в оборудовании оператора, в LOG-файлах, различные протоколы соединений. Файлы могут содержать текстовую информацию, изображения, музыку, аудиоинформацию, программное обеспечение и др. Информацию, доступная для получения в качестве доказательства по преступлению, находящемуся в ходе подготовки или

[49] Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информационной безопасности. Томск, 2003. С. 102.

[50] Шеметов А. К. О понятии виртуальных следов в криминалистике // Рос. следователь. 2014. № 20. С. 53.

[51] Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации. М., 2001. С. 41.

[52] Милашев В. А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юрид. наук : 12.00.09. М., 2004. С. 11.

совершения, должна проверяться максимально точно[53].

В процессе сбора информации необходимо обращать внимание на получение сведений об имени, дате рождения, адресе регистрации, номере телефона, адресах иных лиц, адресах электронной почты, номере платёжного лицевого счета, справочных данных, IP-адресе и др.

Получение данных сведений требуется, в том числе, в рамках проведения оперативно-розыскных мероприятий, требующих судебного разрешения в соответствии со специализированными ведомственными нормативными правовыми актами.

Полученные оперативными подразделениями сведения предоставляются органу дознания, следователю или в суд в соответствии с Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд, утвержденной приказом МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013 г.[54]

Возбуждение уголовных дел по преступлениям в сфере компьютерной информации происходит по информации, получаемой в ходе оперативно-розыскных действий, либо по факту совершенного преступления.

В случае производства возбуждения уголовного дела по факту уже совершенного преступления, в течение определённого промежутка времени после совершения преступления, у поставщика услуг связи не сохраняется необходимадля следственных действий я информация (следы), соответственно, у следователя будет отсутствовать возможность воссоздания механизма совершения преступления в сфере компьютерной информации, а так же получение доказательств. Вследствие этого возникает наибольшая вероятность, что преступление никогда не будет раскрыто.

Аналогичная ситуация может возникнутьв случае, если уголовное дело

[53] Гладких В. И. Компьютерное мошенничество: а были ли основания для криминализации? // Рос. следователь. 2018. № 22. С. 26.

[54] Гладких В. И. Компьютерное мошенничество... С. 27.

возбуждается по результатам оперативно-розыскных действий, и в случае длительного хода разработки, информация (следы преступления) своевременно не будет получена вследствие ее утери или короткого срока хранения.

В связи с этим законодателем приняты определенные меры для исправления данной ситуации, а именно в ст. 64 Федерального закона от 07.07.2003 № 126 «О связи» включена нормаоб обязанностях операторов связи хранить информцию о фактах приема, передачи, доставки и обработки голосовой информации, текстовых сообщений пользователей услугами связи в течение трех лет, в отношении содержательной части (голосовой информации, фото, видео) установлен срок хранения до шести месяцев[55].

Указанные нововведения в законодательство необходимы при работе в ходе оперативно-розыскных мероприятий и следственных действий правоохранительными органами, деятельность которых направлена на противодействие преступлениям в сфере компьютерной информации.

В 2016 году ст. 6 Федерального закона «Об оперативно-розыскной деятельности» была дополнена пятнадцатым ОРМ «Получение компьютерной информации», однако до настоящего времени ведомственное нормативное регулирование порядка его проведения не закреплено[56].

Вследствие этого, практическая значимость рассматриваемого оперативно-розыскного мероприятия в ходе процесса выявления, раскрытия и расследования преступлений, которые связаны с компьютерной информацией, ничтожно мала, поэтому возникла очевидная необходимость в регламентации порядка и хода его осуществления.

От корректности и своевременности предупредительных действий правоохранительных органов в противодействии преступлениям, производимых в сфере компьютерной информации зависит экономическое и финансовое благосостояние России.

---

[55] О связи [Электронный ресурс] : федер. закон от 7 июля 2003 г. № 126-ФЗ ( в ред. от 6 июня 2019 г.; с изм. и доп., вступ. в силу с 1 ноября 2019 г.) // КонсультантПлюс : справ. правовая система. Версия Проф. Электрон. дан. М., 2020. Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

[56] Об оперативно-розыскной деятельности [Электронный ресурс] : федер. закон от 12 авг. 1995 г. № 144-ФЗ…

## 3 Особенности производства отдельных следственных действий

### 3.1 Тактика производства вербальных следственных действий при расследовании преступлений в сфере компьютерной информации

Допрос (ст. 189 УПК РФ) и очная ставка подозреваемых (обвиняемых) (ст. 192 УПК РФ), в том числе при расследовании киберпреступлений, проводятся в соответствии со ст. 164 УПК РФ (Общие правила проведения следственных действий), а также в соответствии со ст. 191 УПК РФ, если указанные следственные действия проводятся с участием несовершеннолетних.

Расшифровка теории научных исследований некоторых ученых говорит о том, что одним из сложных следственных мероприятий является допрос и очная ставка при расследовании киберпреступлений.

Определено следует принять во внимание тот факт, что среди исследователей, изучающих данный вопрос, не существует единого мнения относительно определения понятия очной ставки. Так, одна группа исследователей очную ставку характеризует как некоторый вид допроса. Например, А. А. Закатов, который относится к этой группе, видит очную ставку в виде допроса в присутствии друг друга ранее допрошенных лиц, в показаниях которых имеются существенные противоречия[57].

Другая группа ученых определяет очную, ставку, как самостоятельный следственный эксперимент. Так, В.Е. Коновалова говорят, что очная ставка-это следственное действие, которое заключается в получении доказательств по делу и в одновременном допросе двух лиц (двух свидетелей, двух обвиняемых, свидетеля и обвиняемого) судебно-следственными органами в целях устранения существенных противоречий, имеющихся в показаниях этих лиц, и установления истины[58].

Исходя из вышеперечисленных методов, очную ставку при раскрытии киберпреступлений можно отнести к вербальным следственным мероприятиям,

[57] Ефимичев, П. С., Ефимичев, С. П. Расследование преступлений: теория, практика, обеспечение прав личности. М., 2008. С. 144.

[58] Коновалова В. Е. Тактика производства очной ставки // Ученые записки Харьков. юрид. ин-та. 1955. Вып. 6. С. 23.

исследовать как одну из основных видов допроса и понимать, как одновременный допрос двух заранее допрошенных лиц (подозреваемых, обвиняемых), показания которых основываются на большом количестве взаимных противоречий.

Также следует отметить, что подготовительные действия к проведению допроса и очной ставки имеет свои отличительные характеристики и конкретную специфику. Если их не принимать во внимание, следователь определенно сталкивается с рядом трудностей и не сможет эффективно организовать указанные следственные мероприятия. Специфика действий по осуществлению допроса по уголовным делам данной категории, непременно зависит от характеристик методов совершения киберпреступлений и других как позитивных, так и негативных факторов. Необходимо учесть тот факт, что специфика допроса потерпевших и свидетелей по уголовным делам о киберпреступлениях будет значительно отличаться от методов допроса подозреваемых и обвиняемых, а характерные особенности, которые непосредственно связаны с методами преступления, влияют на определение тактики допроса.

Исследования и результаты опроса следователей по вопросам методик расследования киберпреступлений выявили проблемы при проведении, допроса и очной ставки у представителей правоохранительных органов.

У 71% опрошенных возникали трудности при расследовании, с терминологией, что влекло за собой не понимание мысли подозреваемого, а значит и не было контакта с ним.

Исходя из выше сказанного, можно разделить проблемы, которые необходимо решать в процессе подготовки к допросу (очной ставки) на группы:

1. вовлечение узких специалистов;

В процессе расследования киберпреступлений обязательны знания в области информационных систем, компьютерных технологий и компьютерной техники. Но практика показывает, что сотрудники не обладают необходимыми знаниями, а это влечет за собой не понимание ответов допрашиваемых лиц.

2. отсутствие специальных знаний у сотрудника часто приводит к существенному «интеллектуальному» противодействию расследования со стороны обвиняемого. На это указывает то, что подозреваемый (обвиняемый) раскрывает следователю о методе совершения преступления, используя максимальное количество высказываний и конкретных терминов, которые абсолютно не понятны для человека, не касающегося данной сферы деятельности. При этом чаще всего, этот способ не совпадает с реальным способом совершения данного преступления;

3. изучение большого объема информации, которая чаще всего излагается в электронном виде;

4. использование в течение допроса или очной ставки знаний юридической психологии;

Кроме всего этого, знание основ психологии преступников (в том числе киберпреступников) поможет сотруднику правоохранительных органов при выработке методик по устранению их противодействия, так как преступники достаточно часто применяют в своей преступной деятельности (так же и в процессе следственных мероприятий) психологические приемы, например, такой приём как манипулирование.

5. недостаток времени и постоянная изменчивость обстановки в сетевом окружении, которые характеризуются краткосрочностью существования и высокой скоростью реформирования конкретных видов доказательств, которые находятся в электронной форме.

С точки зрения криминологии, допрос (очная ставка) является способом эффективного решения определенных тактических задач – уличения во лжи лица, которое оказывает противодействие следствию; проверки достоверности предполагаемых версий; проверку на прочность позиций, занятых допрашиваемыми во время проведения следственных мероприятий; выявления ранее неизвестных обстоятельств, включая дополнительные эпизоды

преступной деятельности, и т.д.[59]

Существует три стадии допроса (очной ставки) – подготовительную, основную и заключительную, Каждая из них имеет определенные особенности при расследовании преступлений, связанных с использованием высоких информационных технологий.

Результаты анкетирования, проведенного среди сотрудников правоохранительных органов представлены в таблице 1.

Таблица 1 – Результаты анкетирования, проведенного среди сотрудников правоохранительных органов

| Особенности тактики допроса (очной ставки) | Значение |
|---|---|
| Подготовительная стадия | 68,4% |
| Изучение личности допрашиваемого | 58% |
| Составление вопросов с участием узкого специалиста | 63,1% |

Окончание таблицы 1

| Особенности тактики допроса (очной ставки) | Значение |
|---|---|
| Привлечение узкого специалиста к проведению следственного мероприятия | 36,8% |

Подготовительная стадия следственных действий играет большую роль в расследовании. К методике допроса можно отнести: информационное обеспечение допроса, изучение дела, подозреваемого, его личностных качеств и четкий план допроса.

Информационное обеспечение является важной составляющей в подготовке допроса обвиняемого при киберпреступлении. Насколько хорошо будет осведомлен следователь о совершенном преступлении, настолько под контролем будет ситуация, которая сложится на допросе. Следователь должен владеть всем собранным по делу материалам, должен понимать каким способом оно совершено какие последствия для общества принесло данное преступление, для того чтобы правильно квалифицировать киберпреступления.

[59] Образцов В. А., Топорков А. А. Подготовка и производство очной ставки // Следственные действия. Криминалистические рекомендации. Типовые образцы документов / С. Н. Богомолова [и др.]. М., 2001. С. 160.

П.В. Костин, отмечает, что: «преступления в сфере высоких информационных технологий редко встречаются в обособленном виде, обычно, они совершаются совместно с другими общественно опасными деяниями и имеют факультативный характер. Это объясняется тем, что при использовании информационных технологий в качестве основного средства совершения другого преступления она сама становится предметом общественно опасного действия».[60]

Наличие знание основ компьютерных технологий, а также правовой базы, которая определяет конкретную область нарушения прав, можно назвать следующим условием информационного обеспечения допроса при расследовании киберпреступления. К примеру, М.А. Романенко, описывая процесс допроса при расследовании преступных нарушений авторских прав в сфере информационного обеспечения, среди основных стадий подготовки к допросу чётко выделил: «необходимость изучения законодательства об авторском праве и подготовки вопросов, которые касаются как самого преступления, так и сути контрабанды экземпляров и сырья».[61]

Для того чтобы провести грамотно допрос (очную ставку) следователю необходимо: изучить специальную литературу, ознакомится со справочником по компьютерной терминологии, получить консультацию у узких специалистов. Как точно замечает М.М. Менжега, следователю, который не обладает специальными знаниями, самостоятельно будет сложно самостоятельно расследовать дело. Например, для него будет невозможно отличить сбой в работе аппаратуры или случайную ошибку администратора; определить возможные противоречия и ложь в показаниях, так как следователь может быть введен в заблуждение подозреваемым касаемо определенных терминов и возможностей компьютерных устройств. Кроме того, привлечение узкого специалиста позволит разделить такие технические вопросы, как, к примеру, осуществлялось ли копирование или модификация информации при

[60] Костин П. В. Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики : автореф. дис. ... канд. юрид. наук : 12.00.09. Н. Новгород, 2007. С. 6.

[61] Романенко М. А. Расследование преступных нарушений авторских прав в сфере программного обеспечения. Омск, 2008. С. 155–156.

выполнении определенного действия и другие.

Схожей позиции придерживаются и многие другие исследователи данного вопроса. Например, Третьяк М.И. предполагает, что: «при расследовании киберпреступлений, при осуществлении допроса (очной ставки) подозреваемых (обвиняемых) вероятно использование ими понятий, смысл которых представителю правоохранительных органов может быть непонятен, но они непосредственно указывают на специфичные способы совершения данных преступлений. Устранить данные неясности без помощи специалиста следователю в ходе допроса (очной ставки) представляется практически невозможно»[62].

Фактором, благотворно влияющим на выбор методики производства допроса, является наличие необходимого объема информации о совершенном преступлении, который приобретен из различных источников, например, из материалов доследственной проверки, оперативно-розыскных мероприятий и т.п. Более того, содержание преступление таково, что при определении обстоятельств его совершения нужны конкретные знания о характеристиках преступления, которые определенно зависят от применяемых для его реализации механизмах.

Таким образом, в связи с отсутствием у следователя специальных знаний это может вызвать трудности при решении основных задач допроса: выявление элементов состава киберпреступления, исходя из следовой информации; установление обстановки совершения киберпреступления (времени, места), способа и мотивов его совершения, сопутствующих обстоятельств; определение предмета преступного посягательства; определение размера причиненного ущерба; выделение детальных признаков вида киберпреступления; установление иных лиц, причастных к совершению киберпреступления, а также способа его сокрытия. Так, по рассматриваемым уголовным делам выделяют следующие способы сокрытия преступлений:

[62] Третьяк М. И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества // Уголовное право. 2016. № 2. С. 95 – 101.

шифровка (электронной почты; файлов, содержащих информацию, касающуюся совершённого киберпреступления, и прочего) – 5 %; удаление информации, находящейся в памяти компьютера и на машинных носителях – 13 %; установка пароля – 10 %; хранение информации, касающейся совершённого киберпреступления, в Облаке – 9 %; установка программ удалённого пользования, программ защиты информации от несанкционированного доступа – 8,2 %; использование вредоносных программ для удаления файлов – 8,3 %; использование ложного почтового адреса или анонимной почты – 10,7 %; использование программы смены (скрытия) IP-адреса компьютера – 5 % и другие. Поэтому при появлении новых обстоятельств следователю необходимо пересматривать дело, т.к. он может обнаружить важные данные в связи с новыми открывшимися обстоятельствами, которые он до этого не замечал[63].

Данное обстоятельство объясняет, почему важно, чтобы при осуществлении следственных действий присутствовал специалист в сфере высоких информационных технологий, который поможет следователю понять смысл неизвестных технических понятий, способы осуществления данного преступления, объяснить рабу устройств изъятых в процессе делопроизводства.

Кроме того, основным элементом, информационное обеспечение допроса является изучение характерных особенностей личности подозреваемого.

Следователь, готовивших к допросу при расследовании киберпреступлений, должен использовать по максимуму все источники, из которых можно получить информацию о личности допрашиваемого, а именно: изучение биографии личности; сбор независимых характеристик; анализ трудовой деятельности лица; анализ различного рода документов; назначение судебно-психологических экспертиз и учет их заключений; непосредственное наблюдение за человеком (эмоции, речь, характер оценки и др.)[64]. Также необходимо изучить страницы преступника в социальных сетях, благодаря

[63] Костин П. В. Исследование машинных носителей информации… С. 6.

[64] Питерцев С. К., Степанов А. А. Тактика допроса на предварительном следствии и в суде. СПб., 2001. С. 28.

чему следователь может выяснить: интересы, увлечения, круг его общения. Также, следователю необходимо посетить сайты, которые наиболее часто посещал допрашиваемый.

Следующим необходимым шагом на подготовительной стадии проведения следственных мероприятий будет выбор времени, места и способа вызова на допрос (очную ставку). Как говорит Е.Н. Быстряков: «в помещении, где проводится допрос (очная ставка), обязательно присутствие высокотехнологичной компьютерной техники, наличие которой позволяет наладить эмоциональный контакт с подозреваемыми, применить такой прием, как предъявление неоспоримых доказательств с технологической составляющей»[65].

Следственные мероприятия направленные на работу с обвиняемым по киберпреступлениям является необходимым этапом следствия по сбору и проверке как доказательственной, так и ориентирующей информации, которую сотрудник правоохранительных органов получает при помощи вербальных и невербальных коммуникаций[66].

При изучении криминалистической литературы, следственной и судебной практики, следственные мероприятия при расследовании преступлений, выполненных с использованием высоких информационных технологий, необходимо соблюдение некоторых этапов: выяснение нужной информации о личности подозреваемых, собственный рассказ подозреваемых, стадия, которая включает в себя, фиксация хода и анализ результатов следственного мероприятия.

При проведении следственных действий, направленных на выяснение информации по делу, основной целью является выявления фактов, которые связаны с виртуальными следами, а также другой имеющей отношение к расследуемому виду преступления.

Кроме того, следователю нужно брать во внимание, что

[65] Быстряков Е. Н., Иванов А. Н., Климов В. А. Расследование компьютерных преступлений. Саратов, 2000. С. 81.

[66] Тактика следственных действий / Е. Н. Быстряков [и др.]. Саратов, 2000. С. 90.

киберпространство достаточно сильно меняет восприятие человеком реальной действительности. В условиях киберпространства полностью изменяется психология взаимосвязей: преступник – предмет преступления (потерпевший), которые преобразуются во взаимосвязь: преступник – компьютерная техника (сети) – потерпевший (предмет преступления). Таким образом, киберпространство создает у человека впечатление возможности уклонения от какой-либо ответственности. Данное впечатление создается из-за анонимности в интернете, которая предоставляет возможность: создать образ, который не соответствует действительности.

Успех в расследовании киберпреступлений сильно зависит от умений выстраивать новые тактические ходы, их структуру на основе материалов, помогающих выстраивать психологические закономерности поведения подозреваемого, и применять стандартные приемы, но принимая во внимание индивидуальные особенности конкретного подозреваемого по конкретному преступлению.

Важным моментом для следователя при определении тактики проведения допроса является то, что лица, которые проходят подозреваемыми по делу, не имеют, как правило, антисоциальной установки. Из-за этого в процессе расследования преступления, особенно в сложных ситуациях используются такие методики, которые будут наиболее эффективны в данных условиях. А именно, убеждение, которое строится на возможности пересмотреть преступником личной позиции и активно помогать следствию. К таким приемам относятся: побуждение в ходе беседы к чистосердечному признанию, путем объяснения как вредных последствий отпирательства и лжи, так и хорошего выхода из ситуации после добровольного признания своей вины и оказания помощи в расследовании преступления; взаимодействие на положительные стороны характера допрашиваемого, учет его привязанностей, увлечений, склонение к честности подозреваемого, авторитету в кругу его общения, в рабочем коллективе или давление на слабые места личности и т.д.

Делая вывод из вышесказанного, можно определить, что следственные

моменты, которые выстраиваются в процессе допроса, делятся на бесконфликтные (простые), когда следователь имеет необходимую доказательную базу, обладает фактами, и конфликтной (сложные), когда он осуществляет следственные действия с целью их получения.

Как показывает практика, в большинстве случаев допросы подозреваемого (обвиняемого) по делам о киберпреступлениях проходят в конфликтных ситуациях. Допрашиваемые отказываются от дачи показаний или дают ложные показания, принижая свою вину или вообще отрицая участие в преступлении.

Характерной особенностью киберпреступлений, в основном, является их тщательная организованность, а также владение преступником необходимыми данными, которыми владеет следователь. Естественно, преступник для введения следствия в заблуждение, использует специфические термины, что в сою очередь сильно затрудняет работу по выявлению лжи.

Исходя из этого, сотруднику правоохранительных органов нужно подготовить необходимую тактику, которая будет применима в процессе проведения следственных мероприятий, и особенности фиксации конкретного следственного действия. Самым лучшим способом является дать возможность подозреваемому рассказать все обстоятельства дела, связанные непосредственно с обвинительными фактами, в порядке свободного рассказа, и только после этого, озвучить все, интересующие по делу конкретизирующие вопросы. Кроме этого, имеет смысл как на подготовительной стадии, так и самом ходе проведения допроса привлекать узкого специалиста в области информационных технологий, несмотря на то, что некоторые дознаватели считают, что это нерезультативно.

Привлечение узкого специалиста по данному вопросу, непосредственно к проведению следственного мероприятия позволит: верно задавать вопросы, исходя из информации, полученной в процессе допроса (очной ставки); выделить конкретные обстоятельства, которые умышленно искажают подозреваемые; точно формулировать данные, заносимые в протокол допроса, а

в некоторых случаях поможет создать психологическую связь с допрашиваемыми.

При проведении допроса подозреваемому (обвиняемому) сначала задаются общие вопросы (навык и уровень работы с компьютером, место работы, есть ли компьютер дома и на работе, что входит в обязанности допрашиваемого на работе (если преступление связано с рабочей деятельностью), каковы цели и мотивы допрашиваемого, имело ли место сокрытие преступления и пр.). Потом следователь ставит конкретные вопросы, затрагивающие непосредственно совершенное киберпреступление.

В ходе расследования преступлений сфере высоких информационных технологий, сотруднику правоохранительных органов, у обвиняемого необходимо узнать: какое программное обеспечение и прочие технические средства применялись для совершения преступления; каким образом преступник обошел установленные системы безопасности; каких образом была получена компьютерной информации; методы сокрытия неправомерного доступа; какая периодичность данных посягательств; использовались ли привилегии служебного положения при совершении преступления; сколько лиц было задействовано в совершении данного преступления.

При расследовании создания и использования вредоносных программ следователь должен поставить другие вопросы: самостоятельно ли злоумышленник занимался написанием программ или приобрел из каких-либо других источников; какое оборудование использовалось для разработки данного ПО и в какой операционной системе; на что нацелена данная программа; сколько единиц техники заражено; при помощи чего осуществлялось заражение и другие конкретные вопросы.

Исходя из вышеперечисленного, основываясь на результатах исследования научной литературы, общие вопросы при раскрытии любого киберпреступления будут типовыми. Но конкретные вопросы должны быть составлены при помощи узкого специалиста в данной сфере, в каждом конкретном случае индивидуально, с учетом характерных особенностей того

или иного совершенного преступления.

Как говорилось ранее, следственные действия, такие как допрос свидетелей, потерпевших имеет некоторые особенности, которые зависят не только от способа совершения киберпреступлений, но и от его последствий. В данном случае, нельзя не разделить точку зрения В. М. Быкова, который полагает, что: «тактика допроса должна строиться с учетом соответствующего криминалистического типа допрашиваемых. Исходя из позиции подозреваемых, в ходе подготовки к допросу, ученым были выделены следующие типы: активные и негативные, добросовестные потерпевшие, неустойчивые, недобросовестные потерпевшие[67]». Такую структуру можно отнести и к свидетелям.

Данная типизация может быть заложена в основу на подготовительном этапе допроса потерпевших и свидетелей. К примеру, допрашивая потерпевшую сторону (а также свидетелей), нужно выяснить конкретную информацию: какие компьютерные средства применялись потерпевшим или свидетелем; какой информацией о таких средствах они обладают; какими навыками работы на компьютере или ином технически сложном устройстве владеют; их знания о программном обеспечении, установленном на компьютере или ином технически сложном устройстве; с каким оператором (провайдером) заключен договор на услуги выхода в интернет, особенности условий данного договора; как потерпевший или свидетель узнал о совершенном преступлении, источники информации о нем; как осуществлялось взаимодействие между допрашиваемым лицом и преступником; может ли потерпевший или свидетель опознать подозреваемых и при каких условиях, имел ли место быть визуальный контакт. Если потерпевшим является юридическое лицо, то свидетелями по данному делу проходят все сотрудники предприятия, которые относятся к совершенному преступлению.

Психологическая сущность очной ставки – это налаживание психологической взаимосвязи между участниками проводимого следственного

[67] Быков В. М. Допрос потерпевшего // Законность. 2014. № 6. С. 27-32.

мероприятия. Сотруднику правоохранительных органов нужно принимать во внимание тот факт, что проведение очной ставки, обычно, предполагает конфликт между ее участниками. Обладая большой силой воздействия на лиц, чьи показания умышленно лживы, очная ставка часто играет роль завершающего, переломного пункта в их дальнейшем поведении на следствии»[68] - считает Васильев В.Л..

Следует подчеркнуть, что многолетнее изучение данного вопроса помогло составить рекомендации по установлению психологического контакта. Эти рекомендации содержатся в каждом учебнике криминалистики, учебных пособиях, издаваемых специально для работников следствия, отдельных научных работах. Несмотря на определённую степень изученности, проблема психологического контакта до сих пор остаётся предметом дискуссий, одним из наиболее актуальных и интересных, и в то же время спорных вопросов в следственной тактике. Более того, совершенно обоснованным представляется утверждение о том, что без психологического контакта нельзя обойтись ни в одном следственном действии.

Психологическая диагностика личности допрашиваемых необходима для определения их индивидуально-психологических особенностей, а также предотвращения получения от них заведомо ложных показаний.

Таким образом, при производстве допроса (очной ставки) между обвиняемыми в совершении киберпреступления особенно важно знать психологические особенности лиц, участвующих в производстве данных следственных действий, уметь применять правомерное психологического воздействие на ее участников, контролировать их состояние и психологическое влияние, оказываемое участниками очной ставки как на самого следователя, так и на друг друга.

Определенно, тактика допроса по уголовным делам категории информационных технологий сильно зависит от способа совершения преступления и других как позитивных, так и негативных факторов.

[68] Васильев В. Л. Юридическая психология. СПб., 2009. С. 483.

Исходя из вышеизложенного, можно совершенно точно полагать, что тактику проведения вербальных следственных мероприятий (допроса, очной ставки) сотруднику правоохранительных органов необходимо выбирать, исходя из: необходимости использования знаний узких специалистов в данной сфере, или применение собственных знаний в области информационных систем, компьютерных технологий и компьютерной техники; необходимости включения юридической психологии при анализе особенностей личности преступника; особенностей интеллектуального противодействия следствию со стороны преступника; исходя из конкретной информации, которая храниться на информационном носителе ПО, специальных компьютерных программ; дефицита времени и постоянной смены обстановки в киберпространстве. Допрос потерпевших и свидетелей по делам о преступлении с использованием высоких информационных технологий будет отличаться от допроса подозреваемых и обвиняемых, а характерные особенности, которые связаны с способом преступления, влияют на выбор тактики проведения следственных мероприятий.

### 3.2 Тактика производства невербальных следственных действий

К невербальным следственным мероприятиям относятся: осмотр места преступления (за исключением компьютерной техники, информационных объектов); применение судебных экспертиз (кроме компьютерно-технических экспертиз).

Осмотр места происшествия (местности, жилища, служебного или иного помещения, предметов и документов) производится в целях своевременного обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела (ст. 176 УПК РФ). В соответствии со ст. 177 УПК РФ осмотр следов преступления и иных обнаруженных предметов осуществляется на месте производства следственного действия, за исключением случаев, когда производство такого осмотра предположительно займёт много времени или процедура осмотра на месте затруднена. В таких

случаях предметы, подлежащие осмотру, изымаются. При этом в протоколе осмотра, по возможности, указываются индивидуальные признаки и особенности изымаемых предметов. При расследовании киберпреступлений осмотр места происшествия (местности, жилища, служебного или иного помещения, предметов и документов) является первоначальным и неотложным следственным действием.

Цель осмотра места происшествия в ходе расследования киберпреступлений - своевременное обнаружение, исследование, документирование, изъятие, и предварительное изучение в установленном законом порядке необходимой информации и различных видов следов (материальных, нематериальных, виртуальных) для получения требуемых сведений и доказательств происшествия, которые, в свою очередь, имеют большое значение для быстрого течения хода расследования и своевременного раскрытия правонарушений.

Одновременно с этим, по каждому виду преступлений данного рода методика осмотра места происшествия будет иметь свои специфические особенности. По высказыванию Степаненко Д.А.: «общей задачей осмотра места происшествия главным образом будет установление способа совершения преступления, учитывая все тонкости, то есть решение вопроса о том, что конкретно произошло, когда и каким образом»[69].

С учетом специфических характеристик рассматриваемых преступлений, сотруднику правоохранительных органов, необходимо учесть все материально-технические инструменты следственного действия, для получения максимально полного объема необходимой информации.

Сразу после прибытия следователя на место совершения преступления, сотрудник правоохранительных органов обязан обеспечить сохранения места совершения преступления в первозданном и нетронутом виде, обеспечить изоляцию места совершения преступления от посторонних лиц, не

[69] Степаненко Д. А. «Адаптивная модификация» криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности // Рос. следователь. 2015. №15. С. 18.

участвующих в ходе исследования и допроса, далее сотруднику следует организовать оцепление периметра места совершения преступления, для сохранения объектов и предметов, находящихся внутри охраняемого периметра в нетронутом виде. К примеру: все задействованные электронные устройства и компьютеры оставить в неизменяемом состоянии, без внесения изменений в работу системы без участия сторонних лиц, либо пользователей. Далее сотруднику необходимо подробно опросить потерпевшего о произошедшем и обстоятельствах совершённого посягательства. После этого сотрудником правоохранительных органов производится детальный осмотр места происшествия.

Существует метод, описанный Д. А. Илюшиным, в ходе применения которого, осмотр места происшествия сотрудником правоохранительных органов производится от центра, к краевым периферийным точкам исследуемой площади места совершения преступления. В зависимости от особенностей и индивидуальных характеристик места происшествия, выбор точки центра, как начала следственного мероприятия производится по следующему принципу: точкой может являться механизм, с помощью которого была реализована, либо запущена определённая последовательность действий. Таким устройством может являться техническое электронное устройство, с помощью которого производились действия, повлекшие ущерб для потерпевшего, либо группы потерпевших лиц. Отправной точкой также может являться определённая область, к примеру: мастерская, либо сборочный цех, в котором злоумышленник производил изготовление и программирование электронного устройства в ходе подготовки преступления.

В ходе осмотра места преступления, в первую очередь, сотруднику правоохранительных органов следует произвести детальный осмотр места происшествия. Осмотр можно разделить на две группы: обзорный осмотр и детальный осмотр. В ходе обзорного осмотра, следователь производит выяснение и определение места совершения преступления, сектора, либо области, подлежащей осмотру и исследованию. «При расследовании данного

рода преступлений осмотру подлежат: место обработки, хранения необходимой информации, которая использовалась при совершении преступления; место непосредственного применения злоумышленником компьютерного оборудования и сетей; место хранения информации в компьютере, компьютерной системе или их виртуальных копий, которая была изъята преступным путём из других систем и сетей; место обнаружения вредных последствий»[70] - излагает в своей работе Лапшин В.Е.

При визуальном осмотре помещения следователю необходимо точно определить границы осмотра места происшествия, выявить точное расположение проложенных локальных сетей в помещении, рабочего места преступника, компьютеров и (или) другого оборудования и средств, которые относятся к совершённому киберпреступлению, что поможет установить места хранения информации, документов, которые подлежат осмотру, а в некоторых случаях – исключить возможность повторного совершения преступления.

Проводя визуальный осмотр, необходимо выделить особенности осматриваемого помещения: где оно расположено (в административном здании, в жилом доме или это общественное место, либо служебное помещение), присутствуют ли системы охраны, сигнализации, есть ли камеры видеонаблюдения, в каком состоянии находятся окна и двери, надежно ли они закрываются.

При осмотре рабочего места, компьютеров или иного оборудования, при помощи которого было совершено данное преступление, сотрудник правоохранительных органов должен найти ответ на некоторые вопросы, необходимые для эффективного расследования:

1) имеет ли персональный компьютер подключение к локальной сети, присутствует ли распределительная коробка, имеются ли разветвления;

2) каким способом осуществляется подключение к сети, проводным или беспроводным (Wi-Fi);

[70] Лапшин В. Е. Теоретические основы экспертизы места происшествия // Эксперт-криминалист. 2009. № 3. С. 4.

3) Присутствуют ли в осматриваемом компьютере или сети устройства для удалённого доступа к другим компьютерам.

После проведённого визуального осмотра необходимо составить схему помещения и указать на ней места расположения компьютера или иного оборудования, при помощи которого было совершено киберпреступление, сети и точки связи с удалёнными системами. Так же необходимо сделать фотографию мета происшествия.

Изначально специалист по правилам обзорной фотосъёмки фотографирует общий вид осматриваемого помещения, затем по правилам узловой фотосъёмки фиксирует в кадре компьютеры, подключённые к ним устройства, и иные устройства, которые необходимы в расследовании преступления. Если оборудование вскрывалось, то по правилам детальной фотосъёмки, фиксируются его составные части.

Детальный осмотр места совершения преступления заключается в поэтапном осмотре всех составных частей оборудования, которое было использовано злоумышленником: компьютера и всех его деталей (если это стационарный ПК), компьютерных сетей, задействованных при совершении преступления, устройств связи, принтеров, сканеров, модемов, съемных носителей информации (флэш-карты, жёсткие диски, винчестеры и прочее), а необходимой документации, которая имеет отношение к делу.

В процессе детального осмотра для сохранения следов преступления, сотрудник, ведущий данное дело, в первую очередь, поручает специалисту-криминалисту найти и изъять материальные следы и другие вещественные доказательства, характерные данному киберпреступлению и присутствующую доказательную базу.

В ряде случаев бывает такое, что преступник оставляет следы преступления на компьютере, кабельных соединениях, периферийных устройствах, флэш-носителях, переносных жёстких дисках, винчестерах, модемах и пр. Так же существует такая вероятность, что преступником могут быть оставлены какие-либо личные документы, договора, блокноты и другие

бумажные носители информации, которые имеют непосредственное отношение к преступлению. В таком случае пристальное внимание необходимо обратить на исправления; дополнительные записи; вклеенные листы и другие возможные улики[71]. О необходимости изъятия в ходе следственного мероприятия указанных носителей информации, сотруднику правоохранительных органов необходимо проконсультироваться со специалистом по области высоких информационных технологий. Так же все найденные внешние носители информации в соответствии с п. 3.1 ст. 183 УПК РФ осматриваются специалистом, который устанавливает их связь с расследуемым преступлением, после чего, если это необходимо, они при помощи специалиста изымаются следователем и упаковываются с соблюдением процессуальных требований (ст.177 УПК РФ).

Общие характеристики места происшествия состоят из особенностей присутствующих тут объектов и следов, т. е. их качественной определённости и технических характеристик. Необходимо понимать, какое значение в противоправном деянии играли эти объекты и следы, для чего конкретно они применялись, а также выявить наличие или отсутствие каких-либо связей между данными объектами и следами – их взаиморасположение на месте происшествия.

Сущность обстановки места совершения преступления отражается в неоднократных проявлениях признаков явлений и предметов, которые непременно являются следствием преступных деяний правонарушителя и которые нужно распознать, т.е. диагностировать. Точное описание и исследование места преступления, построение схемы состоявшегося события, по высказываниям В. Е. Лапшина, –главная задача, которую необходимо решить следователю в процессе осмотра места происшествия. Грамотное, взвешенное решение поставленной задачи в необходимом объёме определяется рядом определенных факторов[72].

[71] Шевчук И. Б. Расширенная классификация информационных технологий: научно-теоретические и региональный подходы // Перспективы науки и образования. 2014. № 6 (12). С. 41-42.

[72] Лапшин В. Е. Теоретические основы экспертизы места происшествия… С. 2 – 5.

При этом, эффективность осмотра места преступления по киберпреступлениям содержит необходимые критерии: значителен в данной ситуации уровень квалификации следователя и его знания по основным способам и механизмам совершения преступлений данного характера; своевременностью привлечения узких специалистов; квалифицированным применением информационных средств; оперативностью приезда следователя на место совершения преступления; точное соблюдение всех процессуальных требований и криминалистических регламентов по обращению с вещественными доказательствами. При осмотре места происшествия необходимо создать специальные следственно-оперативные группы из компетентных в данном вопросе профессионалов.

Как подчёркивалось ранее, результативности осмотра места происшествия возможно добиться привлечением к участию в данном следственном действии специалистов, в частности – криминалиста. Однако при раскрытии и расследовании преступлений по горячим следам участие такого специалиста не решает проблему в силу ограниченности его функций и ряда указанных выше обстоятельств. Статистика раскрытия рассматриваемого рода преступлений свидетельствует о необходимости проведения в ряде случаев криминалистических экспертиз на месте происшествия, зачастую параллельно с производством осмотром. Исследование обстановки места совершения киберпреступления как объекта экспертизы позволяет эксперту выявить свойства и признаки не только других объектов обстановки места происшествия, но и глубже познать механизм следообразования, что, в свою очередь, несомненно, будет способствовать в дальнейшем более успешному решению экспертных задач.

Еще одним неотъемлемым из следственных мероприятий является назначение судебной экспертизы, которое играет большую роль в расследовании и раскрытии дел, связанных с компьютерными технологиями.

Признав обязательным мероприятием судебную экспертизу, сотрудник правоохранительных органов в соответствии со статьёй 195 УПК РФ, а также

статьями 19, 41 Закона о ГСЭД выносит постановление, о её назначении.

Ряд необходимых экспертиз, которые назначаются по делам такого рода преступлениях, достаточно обширен. В их число входит как стандартные криминалистические экспертизы, так и нестандартные. По каждому преступлению список экспертиз индивидуален, зависит от характера киберпреступления и обычно определяется необходимостью исследования конкретных следов совершения преступления (объектов)[73].

Типичными объектами экспертных исследований по киберпреступлениям являются: документы на цифровом носителе информации (пластиковые карты, электронные документы); машинограммы, и другие бумажные документы, которые изготовлены при помощи печатающих устройств компьютерной техники и иных современных технологий; средства ЭВМ – машинные носители предмета преступного характера и средства совершения преступления; средства электросвязи системы и компьютерной сети; отдельные технологии, процессы и операции, обеспечивающие создание, обработку и передачу компьютерной информации; объекты криминалистических экспертиз, типичных для расследования преступлений иных видов[74].

Исходя из вышеперечисленного, что количество стандартных судебных экспертиз большое, необходимо изучить наиболее сложные экспертные исследования.

Автороведческая экспертиза – ее применяют в таких случаях, когда необходимы определенные знания в области филологии для установления авторских прав текста путем изучения письменной речи, написанной на различных носителях, как электронных, так и бумажных. Объектов автороведческой экспертизы, которая назначается в процессе раскрытия преступлений экстремистской направленности, совершённых с использованием интернета, является письменная речь автора текста. Последняя, обычно, может кодироваться в текстовых файлах на web-сайтах или web-страницах, CD или

[73] Судебная экспертиза: типичные ошибки / Е. Р. Россинская [и др.]. М., 2013. С. 469 - 470.

[74] Попов В. Б., Илюшин В. В. Тактические особенности расследования преступлений в сфере компьютерной информации. М., 2004. С. 85.

DVD дисках, флэш-картах, в текстах, распечатанных с помощью принтеров, или в рукописных текстах – копиях текстовых файлов и т.п.

Автороведческая экспертиза помогает как идентифицировать, так и диагностировать характер преступления, в том числе находит и описывает письменно-речевые навыки автора; стиль исследуемого текста; факторы, которые непосредственно влияют на умышленное и неумышленное искажение текста; текстуальное сходство письменных текстов как продуктов речевой деятельности и др.

По анализу заключений автороведческих экспертиз, которые были назначены и проведены по делам экстремистской направленности, выделены повторяющиеся вопросы, которые выдвигаются следователями на разрешение эксперта-автороведа. Так, при решении идентификационных задач по установлению авторства текста экстремистской направленности выяснению подлежат следующие обстоятельства:

*Является ли А. автором электронного (письменного, машинописного, рукописного) текста, имеющегося на имеющимся носителе информации?*

*Является ли А. автором нескольких электронных текстов, имеющихся на представленных носителях?*

Для решения данных вопросов, которые связаны непосредственно с установлением социально-психологического портрета автора текста, особенностей владения автором речевыми средствами, особенностей его речевого поведения, иных, например: какой пол преступника, точный возраст, образование, родной язык, профессия, род занятий, уровень речевой культуры и языковой компетентности автора текста; в каком состоянии находился автор анализируемого текста при его составлении: в обычном или необычном эмоциональном состоянии, сотрудником правоохранительных органов, как правило, назначается комплексная психолого-лингвистическая экспертиза[75].

К проведению психолого-лингвистической экспертизы в качестве специалистов, как правило, привлекаются лица, профессионально владеющие

[75] Россинская Е. Р., Галяшина Е. И., Зинин А. М. Теория судебной экспертизы. М., 2016. С. 167-168.

необходимыми знаниями в области социальной психологии, судебной психологической экспертизы и лингвистики. В соответствии со ст. 201 УПК РФ и ст. 23 Закона о ГСЭД указанная экспертиза может проводиться как в одиночку, если он обладает достаточным объёмом знаний и методиками психологической лингвистики, так и составом комиссии из экспертов разных специальностей.

Культурологическая экспертиза назначается в том случае, если вопросы достоверности приведённых материалов отнесены к разряду иных специалистов: историков, религиоведов, политологов, этнологов, генетиков и др. Чаще всего в публикациях, выступлениях, возбуждающих национальную, расовую, религиозную вражду, широко применяются тщательно подобранные, извращённые факты, утверждения и представления, которые не имеют доказательной базы, отвергнутые современной наукой. Разнообразные слухи и мышления, переплетаясь с иными, иногда не существующими фактами, вводятся в контекст, где и применяются для создания отрицательного образа представителей какой-либо нации или религиозного общества, приписывают им враждебность, способствуют созданию атмосферы национальной или религиозной вражды. Лживая информация может говорить о сознательном (умышленном) использовании информаций, поэтому как следствие, возникают вопросы о правдивости приведённых автором фактов, достоверности использованных им источников, подлинности высказываний, обоснованности авторских утверждений и суждений, по существу.

В настоящее время в Российской Федерации не существует экспертного учреждения, специализирующегося на проведении культурологических экспертиз, в связи с чем для их производства в соответствии со ст. 57 УПК РФ следователи, как правило, привлекают специалистов в области социальной психологии, психолингвистики, культурологии, искусствоведения, философских, исторических, социологических, политических, географических, филологических и иных наук.

Почерковедческая экспертиза используется в том случае, если в процессе

следствия обнаружен рукописный текст, имеющий отношение к преступлению данного рода. Заключение почерковедческой судебной экспертизы, становится идентифицирующим (при исследовании образцов почерка, подписей) или диагностирующим (при установлении половой принадлежности, возраста, образования, профессии лица, оставившего рукописный текст). Во таком случае при необходимости установления личностных особенностей злоумышленника или иного лица, создавшего рукописный текст, назначается комплексная психолого-почерковедческая (графологическая) экспертиза.

При расследовании киберпреступлений очень эффективными являются психологическая и психиатрическая экспертизы, а также комплексная психолого- психиатрическая экспертиза.

Судебная психологическая экспертиза, являясь одной из способов применения определенных психологических знаний, нацелена на решение возникающих в ходе следствия психологических вопросов. В современности психологические судебные экспертизы используются достаточно часто, что обусловлено следующими факторами: развитием теоретических данных судебной психологии как науки; разработкой новых способов исследования психологических особенностей личности; ужесточением требований к качеству производства предварительного расследования в связи с реформами в уголовном и уголовно-процессуальном законодательстве; поиском мотивов совершения преступления и обстоятельств, которые дают точное описание личности обвиняемого[76].

Объектом экспертного исследования в рамках судебной психологической экспертизы выступает не только личность участника следствия, но и различного рода материалы (рисунки, аудио, видеозаписи и иные объекты), в определенной степени являющиеся продуктами его деятельности[77].

По делам данной категории эта экспертиза назначается для выявления

[76] Бакланцева А. А. Социальный контроль в русскоязычном интернет-пространстве в современных условиях медиатизации общества // Гуманитарные, социально-экономические и общественные науки. 2015. № 5. С. 17.

[77] Холопова Е. Н., Кравцова Г. К. Актуальные проблемы оценки показаний участников уголовного судопроизводства // Сб. материалов межвуз. конференции «Актуальные проблемы криминалистической науки». Калининград, 12 дек. 2014 г. Калининград, 2015. С. 48-57.

индивидуальных особенностей личности преступника, мотивов его действий, диагностирования определённых психопатологий, которые связаны с интернет-зависимостью, личностных характеристик пользователей сети Интернет.

С возрастающей статистикой увлекающихся Интернетом растёт и число потенциальных компьютерных аддиктов[78]. Речь идёт о так называемой интернетзависимости, проблеме, которая за рубежом стала актуальной ещё в конце 1980-х годов. Вопреки тому, что интернет-аддикция2 не диагностируется как самостоятельное заболевание и определяется психологами как феномен. В ближайшем будущем зависимость от Интернета, наряду с другими нехимическими аддикциями, будет рассматриваться как психическое расстройство, имеющее диагностические критерии. Как и людям с патологической тягой к азартным играм или игровым автоматам, интернет-аддиктам присущи неконтролируемость в пользовании компьютером, значительное стрессовое состояние, сопряжённость с финансовыми проблемами, социальные и образовательные трудности, провоцирующая симптоматика, характерная для гипомании, и т. п.

Судебная компьютерно-техническая экспертиза представляет собой исследование информации, зафиксированной в электронной форме, а также технических средств и ПО компьютерной системы в целях дачи заключения по фактам, имеющим значение для уголовного дела. Исследование проводится экспертом (специалистом) в порядке, установленном УПК РФ. Назначение судебной компьютерно-технической экспертизы входит в систему судебных экспертиз, проводимых по уголовным делам. При подготовке и назначении данной экспертизы зачастую возникают трудности с определением вида экспертизы, формулированием вопросов, выносимых на разрешение эксперта, оформлением материалов, предоставляемых эксперту[79]. Трудности обусловлены отсутствием опыта их проведения, отработанных методик и разработанных рекомендаций.

[78] Спиркина Т. С. Личностные особенности пользователей в сети Интернет, склонных к интернет-зависимости // Изв. Рос. гос. пед. ун-та им. А. И. Герцена. 2008. № 60. С. 474.

[79] Гаврилов Б. Я. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей. М., 2016. С. 69.

Значительную помощь оказывают специалисты региональных информационно-вычислительных центров МВД России. В Экспертно-криминалистическом центре МВД РФ существует и проводит компьютерно-технические экспертизы специальный отдел.

Компьютерно-технические экспертизы подразделяются на следующие виды: 1. аппаратно-компьютерная экспертиза – состоит в проведении исследования технических (аппаратных) средств компьютерной системы. Предметом данной экспертизы являются факты и обстоятельства, которые подлежат установлению на основе исследования закономерностей эксплуатации технических средств и материальных носителей информации; 2. программно-компьютерная экспертиза заключается в исследовании ПО. Предметом экспертизы являются закономерности разработки и применения ПО компьютерной системы. Цель исследования заключается в изучении функционального назначения, характеристик и реализуемых требований, алгоритма и особенной структуры, а также текущее состояние ПО; 3. информационно-компьютерная экспертиза данных состоит в исследовании компьютерной информации с целью поиска, обнаружения, анализа и оценки информации, подготовленной пользователем или созданной программами для организации информационных процессов в компьютерной системе; 4. компьютерно-сетевая экспертиза – исследуется функциональное назначение компьютерных средств, реализующих какую-либо информационную технологию. Ее предмет составляет исследование фактов и обстоятельств, связанных с использованием сетевых и телекоммуникационных технологий[80].

Анализ практики назначения судебных экспертиз в ходе расследования киберпреступлений по различным категориям показывает, что перечень экспертиз по каждому конкретному уголовному делу индивидуален, зависит от вида киберпреступления и чаще всего определяется острой необходимостью исследования конкретных следов (объектов) рассматриваемого вида правонарушений.

[80] Шурухнов Н. Г. Криминалистика в схемах и таблицах. М., 2016. С. 429.

Главным образом, вышеизложенное позволяет выделить особенности методов производства невербальных следственных действий при расследовании киберпреступлений в киберпространстве, которые заключаются в: определении примерной информационно-следовой картины места происшествия; в необходимости рассмотрения следовой информации, имеющей материальную и идеальную природу; ситуативной формы организации знаний (решение возникающих задач реализуется не с помощью алгоритмических процедур, а благодаря эвристике, требующей индуктивной логики); использование технико-криминалистических средств.

# ЗАКЛЮЧЕНИЕ

Мы живем в эпоху информационного общества, и наша жизнь тесно связана с различными технологиями и сетью Интернет. И практически каждый раз, взаимодействуя с компьютерными технологиями, мы подвергаем себя угрозе стать жертвой киберпреступников. Поэтому полноценное исследование компьютерных преступлений позволит разработать эффективные меры по их предупреждению и расследованию.

Диссертационное исследование выполнено с целью разработки на основе анализа теоретических положений и изучения правоприменительной практики научно- обоснованных рекомендаций, которые были направлены на совершенствование криминалистической деятельности, осуществляемой при расследовании преступлений в сфере компьютерной информации.

Подводя итог проведенного исследования, обозначим некоторые положения из целого ряда выводов, на которых обосновывается данная работа.

1) Введение законодателем в Уголовный кодекс термина "компьютерная информация" является новшеством. До этого в российском законодательстве, как мне известно, регулирующем информационные правоотношения, определения информации как "компьютерной" не существовало. Вероятней всего, определение "компьютерная" применительно к информации появилось для отграничения этого объекта посягательства от информационных преступлений, которые были предусмотрены иными разделами Уголовного кодекса Российской Федерации. Это требует внимательного изучения содержания данного понятия с целью дальнейшего точного его использования в криминалистической теории и практике.

2) В настоящее время среди компьютерных преступлений преобладают: мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ) нарушение авторских и смежных прав, совершенное с использованием компьютерных и телекоммуникационных

технологий (ст. 146 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 51 273 УК РФ); кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ).

3) Ввиду достаточно высокого уровня латентности исследуемого вида преступлений огромное значение приобретает деятельность правоохранительных органов по их выявлению. Говоря о расследовании этой категории дел, следует выделить, что расследование преступлений в сфере компьютерной информации, особенности некоторых следственных действий приобрели в последнее время особую актуальность, в связи с огромным количеством преступлений, которые были совершены в данной сфере.

4) Компьютерные преступления можно охарактеризовать следующими признаками, которые создают значительные трудности при расследовании:

- высокий уровень профессиональной подготовки и технической оснащенности преступников;
- трансграничность совершения преступления;
- постоянное совершенствование способов совершения преступлений;
- высокоорганизованность преступников и др.

В нашей стране отсутствует единая программа борьбы с преступлениями в сфере компьютерной информации. Для большей части работников органов предварительного расследования раскрытие и расследование компьютерных преступлений представляет сложность, которая связана с тем, что при сборе доказательств и доказывании в таких делах необходимо исследование «виртуального следа». При всем этом уровень специальной технической подготовки, которая необходима для расследования подобных дел в органах юстиции чрезвычайно низкий. К тому же отсутствует обобщенный материал следственной практики, методический материал и рекомендации по расследованию данного вида преступлений.

В итоге, научно-технический прогресс принес человечеству такие

незаменимые в современной жизни новшества, как компьютеры и Интернет. Распространение современных технологий повлекло за собой появление новых видов ресурсов - информационных. Однако новые технологии стимулировали возникновение и развитие и новых форм преступности, прежде всего компьютерных. Большую часть в данной отрасли совершается при помощи компьютерных сетей. В последние несколько лет специалистами замечена тенденция быстрого роста компьютерных преступлений посредством глобальной компьютерной сети Интернет.

Эффективная работа экспертных подразделений и криминалистов вероятна при условии разработки специальных тактик проведения следственных действий, систематизации методик расследования компьютерных преступлений, также подготовки специализированного кадрового состава. Все это, в общей сложности, будет способствовать раскрытию компьютерных преступлений, даст возможность получать доказательства для предъявления их в суде. Российским криминалистам еще предстоит детально провести исследование киберпространства, разработать эффективные тактические и методические подходы к выявлению и расследованию компьютерных преступлений, которые в условиях глобального масштабирования более чем актуальны.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Конституция Российской Федерации [Электронный ресурс] : принята всенар. голосованием от 12 дек. 1993 г. : (с учетом поправок от 30 дек. 2008 г. № 6-ФКЗ; от 30 дек. 2008 г. № 7-ФКЗ; от 5 февр. 2014 г. № 2-ФКЗ ; от 21 июля 2014 г. № 11-ФКЗ) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2020. – Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

2. Уголовный кодекс Российской Федерации [Электронный ресурс]: федер. закон от 13 июня 1996 г. № 63-ФЗ : (в ред. от 17 апр. 2017 г.) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2020. – Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

3. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс] : федер. закон от 18 дек. 2001 г. № 174-ФЗ : (в ред. от 7 июня 2017 г.) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2020. – Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

4. О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31. – Ст. 3451.

5. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31. – Ст. 3448.

6. Об оперативно-розыскной деятельности [Электронный ресурс] : федер. закон от 12 авг. 1995 г. № 144-ФЗ (ред. от 2 авг. 2019 г.) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2020. – Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

7. О связи [Электронный ресурс] : федер. закон от 7 июля 2003 г. № 126-ФЗ ( в ред. от 6 июня 2019 г.; с изм. и доп., вступ. в силу с 1 ноября 2019 г.) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2020. – Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

8. Агибалов А. Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. … канд. юрид. наук : 12.00.09 / А. Ю. Агибалов. – Воронеж, 2010. – 24 с.

9. Афанасьев А. Ю. Некоторые особенности расследования компьютерных преступлений / А. Ю. Афанасьев, М. Е. Репин // Студенческие южно-уральские криминалистические чтения : сб материалов науч.-практ. конф. – Уфа, 2015. – Вып. 3. – С. 26–34.

10. Бакланцева А. А. Социальный контроль в русскоязычном интернет-пространстве в современных условиях медиатизации общества // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 5. – С. 16–19.

11. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. М. : Юрид. лит., 1991. – 157 с.

12. Батурин Ю. М. Проблемы компьютерного права / Ю. М. Батурин. – М. : Юрид. лит., 1991. – 272 с.

13. Белкин Р. С. Курс криминалистики : в 3 т. / Р. С. Белкин. – М. : Юристъ, 1997. – Т. 2. – 464 с.

14. Быков В. М. Допрос потерпевшего // Законность. – 2014. – № 6. – С. 27–32.

15. Быстряков Е. Н. Расследование компьютерных преступлений : учеб. пособие / Е. Н. Быстряков, А. Н. Иванов, В. А. Климов. – Саратов : Саратов. гос. акад. права, 2000. – 81 с.

16. Васильев В. Л. Юридическая психология / В. Л. Васильев. – СПб. : Питер, 2009. – 483 с.

17. Вехов В. Б. Компьютерные преступления : Способы совершения, методики расследования / В. Б. Вехов. – М. : Право и закон, 1996. – 182 с.

18. Вехов В. Б. Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие / В. Б. Вехов, В. В. Попова, Д. А. Илюшин. – Самара : Офорт, 2003. – 188 с.

19. Гавло В. К. Обстановка преступления как структурный компонент криминалистической характеристики преступления // Проблемы совершенствования тактики и методики расследования преступлений : сб. науч. трудов. – Иркутск, 1980. – С. 49–55.

20. Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации / Ю. В. Гаврилин. – М. : Кн. мир, 2001. – 88 с.

21. Гаврилов Б. Я. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей : учеб. пособие / Б. Я. Гаврилов. – М. : Проспект, 2016. – 171 с.

22. Гладких В. И. Компьютерное мошенничество: а были ли основания его криминализации? // Рос. следователь. – 2018. – № 22. – С. 25–31.

23. Глушков Е. Л. Оперативно-розыскная деятельность при расследовании и раскрытии преступлений в сфере компьютерной информации / Е. Л. Глушков, Д. Е. Емельянов // Вестн. Белгород. юрид. ин-та МВД России им. И. Д. Путилина. – 2019. – № 2. – С. 45–49.

24. Головин А. Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации [Электронный ресурс] // Центр исследования проблем компьютерной преступности. – Электрон. дан. – [Б. м.], 2001–2002. – URL: http://www.crime-research.org/library/Golovin.htm (дата обращения: 07.01.2018).

25. Драпкин Л. Я. Основы теории следственных ситуаций / Л. Я. Драпкин. – Свердловск : Изд-во Урал, ун-та, 1987. – 164 с.

26. Евдокимов К. Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. – 2016. – № 1 (35). – С. 86–94.

27. Ефимичев П. С. Расследование преступлений: теория, практика, обеспечение прав личности / П. С. Ефимичев, С. П. Ефимичев. – М. : Юстицинформ, 2008. – 503 с.

28. Ищенко Е. П. Криминалистика : учебник для вузов / Е. П. Ищенко, А. А. Топорков ; под ред. Е. П. Ищенко. – М. : Инфра-М, 2005. – 784 с.

29. Кесареева Т. П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет : дис. ... канд. юрид. наук : 12.00.08 / Т. П. Кесареева. – М., 2002. – 195 с.

30. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. – М. : Горячая линия–Телеком, 2002. – 336 с.

31. Колесниченко Д. Н. Научные и правовые основы методики расследования отдельных видов преступлений : автореф. дис. … д-ра юрид. наук / Д. Н. Колесниченко. – Харьков, 1967. – 27 с.

32. Колесниченко Д. Н. Научные и правовые основы методики расследования отдельных видов преступлений : дис. … д-ра юрид. наук / Д. Н. Колесниченко. – Харьков, 1967. – 347 с.

33. Коновалова В. Е. Тактика производства очной ставки // Ученые записки Харьков. юрид. ин-та. – 1955. – Вып. 6. – С. 123–130.

34. Костин П. В. Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики : автореф. дис. ... канд. юрид. наук : 12.00.09 / П. В. Костин. – Н. Новгород, 2007. – 30 с.

35. Кузнецов А. В. Некоторые вопросы расследования преступлений в сфере компьютерной информации // Информационный бюллетень следственного комитета МВД РФ. – 1998. – № 2. – С. 42–48.

36. Лапшин В. Е. Теоретические основы экспертизы места происшествия // Эксперт-криминалист. – 2009. – № 3. – С. 2–5.

37. Лисина О. В. Проблемы противодействия молодежному киберэкстремизму в условиях интернетсоциализации: вопрос нравственного здоровья подрастающего поколения // Теория и практика общественного развития. – 2017. – № 1. – С. 46–49.

38. Матмуратов Б. Д. К вопросу об объекте посягательства и предмете хищения компьютерной информации // Вестн. Каракалп. фил. АН УзССР. – 1987. – № 3. – С. 58–62.

39. Мегрелишвили Г. Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий // Вестн. Том. гос.

ун-та. – 2007. – № 299. – С. 180–181.

40. Мещериков А. Неправомерный доступ к компьютерной информации // Российское правоведение: Трибуна молодого ученого. – 2009. – Вып. 9. – С. 164–166.

41. Мещеряков Р. В. Специальные вопросы информационной безопасности / Р. В. Мещеряков, А. А. Шелупанов. – Томск : Изд-во Ин-та оптики атмосферы, 2003. – 243 с.

42. Милашев В. А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юрид. наук : 12.00.09 / А. В. Милашев. – М., 2004. – 21 с.

43. Мнацаканян А. В. Преступления в сфере безопасности компьютерной информации как элемент системы Особенной части Уголовного Кодекса Российской Федерации // Пробелы в российском законодательстве. – 2012. – № 3. – С. 158–161.

44. Нехорошева О. Изъятие компьютерной техники и информации // Законность. – 2004. – № 8. – С. 15–18.

45. Номоконов В. А. Актуальные проблемы борьбы с киберпреступностью // Компьютерная преступность и кибертерроризм : сб. науч. работ. – Запорожье, 2004. – Вып. 1. – С. 77–110.

46. Номоконов В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Л. В. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 1 (24). – С. 45–55.

47. Образцов В. А. Подготовка и производство очной ставки / В. А. Образцов, А. А. Топорков // Следственные действия. Криминалистические рекомендации. Типовые образцы документов / С. Н. Богомолова [и др.]. – М., 2001. – С. 159–165.

48. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы : монография / А. Л. Осипенко. – Омск : Изд-во Омск. акад. МВД России, 2009. – 480 с.

49. Питерцев С. К. Тактика допроса на предварительном следствии и в

суде / С. К. Питерцев, А. А. Степанов. – СПб. : Питер, 2001. – 146 с.

50. Подольный Н. А. Отдельные проблемы расследования преступлений, совершённых с применением компьютерных технологий // Библиотека криминалиста. Научный журнал. – 2013. – № 5 (10). – С. 116–127.

51. Поляков В. В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Изв. Алтайского гос. ун-та. – 2013. – № 2 (78). – С. 114–116.

52. Поляков В. В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. … канд. юрид. наук : 12.00.09 / В. В. Поляков. – Барнаул, 2009. – 247 с.

53. Протасевич А. А. Борьба с киберпреступностью как актуальная задача современной науки / А. А. Протасевич, Л. П. Зверянская // Криминологический журнал Байкальского гос. ун-та экономики и права. – 2011. – № 3. – С. 28–33.

54. Прудиус Е. В. Криминалистическая характеристика преступлений в сфере компьютерной информации // Евразийский союз ученых. – 2017. – № 11–2 (44). – С. 96–98.

55. Репин М. Е. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия / М. Е. Репин, А. Ю. Афанасьев // Молодой ученый. – 2015. – № 15 (95). – С. 460–463.

56. Романенко М. А. Расследование преступных нарушений авторских прав в сфере программного обеспечения : монография / М. А. Романенко. – Омск : Изд-во Омск. гос. ун-та, 2008. – 232 с.

57. Россинская Е. Р. Теория судебной экспертизы / Е. Р. Россинская, Е. И. Галяшина, А. М. Зинин. – М. : Норма, 2016. – 368 с.

58. Следственные действия: криминалистические рекомендации. Типовые образцы документов / под ред. В. А. Образцова. – М. : Юристъ, 2001. – 502 с.

59. Состояние преступности в Российской Федерации за январь-апрель 2017 года [Электронный ресурс] // Министерство внутренних дел Российской

Федерации. – Электрон. дан. – [Б. м.], 2020. – URL: https://мвд.рф/folder/101762/item/10287274/ (дата обращения: 08.03.2020).

60. Спиркина Т. С. Личностные особенности пользователей в сети Интернет, склонных к интернет-зависимости // Изв. Рос. гос. пед. ун-та им. А. И. Герцена. – 2008. – № 60. – С. 473–478.

61. Степаненко Д. А. «Адаптивная модификация» криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности // Рос. следователь. – 2015. – № 15. – С. 17–20.

62. Судебная экспертиза: типичные ошибки / Е. Р. Россинская [и др.]. – М. : Проспект, 2013. – 544 с.

63. Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера : дис. … канд. юрид. наук : 12.00.08 / А. В. Суслопаров. – Красноярск, 2010. – 206 с.

64. Тактика следственных действий : учеб. пособие / Е. Н. Быстряков [и др.] ; под ред. В. И. Комиссарова. – Саратов : Изд-во Сарат. гос. акад. права, 2000. – 200 с.

65. Третьяк М. И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества // Уголовное право. – 2016. – № 2. – С. 95–101.

66. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовноправовые меры борьбы : автореф. дис. ... канд. юрид. наук : 12.00.08 / Т. Л. Тропина. – Владивосток, 2005. – 26 с.

67. Холопова Е. Н. Актуальные проблемы оценки показаний участников уголовного судопроизводства (на примере экспертизы психологической достоверности показаний) / Е. Н. Холопова, Г. К. Кравцова // Сб. материалов межвуз. конференции «Актуальные проблемы криминалистической науки». Калининград, 12 дек. 2014 г. – Калининград, 2015. – С. 48–57.

68. Чуриков Н. А. Преступления в сфере компьютерной информации: проблемы квалификации и совершенствования уголовного законодательства в данной сфере / Н. А. Чуриков, С. С. Медведев // Образование и наука в

современных реалиях : материалы Междунар. науч.-практ. конф. Чебоксары, 4 июня 2019 г. : в 2 т. – Чебоксары, 2017. – Т. 2. – С. 312–317.

69. Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений : автореф. дис. … канд. юрид. наук : 12.00.12 / Е. С. Шевченко. – М., 2016. – 29 с.

70. Шевчук И. Б. Расширенная классификация информационных технологий: научно-теоретические и региональный подходы // Перспективы науки и образования. – 2014. – № 6 (12). – С. 41–47.

71. Шеметов А. К. О понятии виртуальных следов в криминалистике // Рос. следователь. – 2014. – № 20. – С. 52–54.

72. Шмырова В. Киберпреступность в России растет быстрее любых других видов преступлений [Электронный ресурс] // Интернет-издание о высоких технологиях – CNews. – Электрон. дан. – [Б. м.], 1995–2020. – URL: https://safe.cnews.ru/news/top/2019-09-27_kiberprestupnost_v_rossii (дата обращения: 08.03.2020).

73. Шурухнов Н. Г. Криминалистика в схемах и таблицах / Н. Г. Шурухнов. – М. : Эксмо, 2016. – 459 с.

74. Яблоков Н. П. Криминалистика / Н. П. Яблоков. – 3-е изд., перераб. и доп. – М. : Юристь, 2005. – 781 с.

75. Convention on Cybercrime [Electronic resource] // Counsil of Europe. – Electronic data. – [S. l.], 2020. – URL: https://www.coe.int/en/web/ conventions/ full-list/-/conventions/treaty/185/ (access date: 20.10.2019).

76. Suler J. The Psychology of Cyberspace [Electronic resource] // Rider University. – Electronic data. – [S. l., s. a.]. – URL: http://users.rider.edu/~suler/ psycyber/psycyber (access date: 30.11.2018).