

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение  
высшего образования

«Уфимский юридический институт Министерства внутренних дел  
Российской Федерации»

Кафедра криминалистики

**ДИПЛОМНАЯ РАБОТА**

на тему «**ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ  
РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ  
ИНФОРМАЦИИ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО  
ОРГАНА ВНУТРЕННИХ ДЕЛ)**»

Выполнил  
Мамаев Иван Алексеевич  
обучающийся по специальности  
40.05.01 Правовое обеспечение  
национальной безопасности  
2017 года набора, 713 учебного взвода

Руководитель  
доцент кафедры,  
кандидат юридических наук  
Гайнелзянова Венера Равиловна

К защите рекомендуется  
рекомендуется / не рекомендуется

Начальник кафедры Э.Д. Нугаева  
подпись

Дата защиты « \_\_\_ » \_\_\_\_\_ 2022 г. Оценка \_\_\_\_\_

## ПЛАН

Введение.....	3
Глава 1. Теоретико-исторический экскурс расследования преступлений в сфере информационных технологий.....	5
§ 1. История возникновения и развития компьютерных преступлений (отечественный опыт) .....	5
§ 2. Общие положения специальных знаний в расследовании преступлений .....	12
§ 3. Базовые элементы криминалистической характеристики преступлений в сфере компьютерной информации.....	14
Глава 2. Организационно-тактические особенности использования специальных знаний при расследовании преступлений в сфере компьютерной информации.....	27
§ 1. Особенности использования специальных знаний при осуществлении следственных действий в ходе расследования преступлений в сфере компьютерной информации .....	27
§ 2. Судебные экспертизы назначаемые при расследовании преступлений в сфере компьютерной информации .....	38
§ 3. Проблемы использования специальных знаний в расследовании преступлений в сфере компьютерной информации .....	49
Заключение.....	54
Список использованной литературы.....	57

## ВВЕДЕНИЕ

В современном мире с каждым днем идёт процесс совершенствования компьютерных технологий, происходят всё новые открытия в информационных областях науки, промышленность вооружается новыми технологиями производства. Социум все чаще использует в своей жизнедеятельности информационно-коммуникационные технологии.

Перспектива появления в мире новых информационно-коммуникационных технологий способствовала не только развитию средств массовой автоматизации, но и упрощению действий в социальной, профессиональной и других сферах жизнедеятельности людей, а также появлению новых способов совершения преступлений. Данный вид преступлений характеризуется большой латентностью и низкой раскрываемостью.

На сегодняшний день большое количество исследований проводится в области компьютерной безопасности, но, несмотря на это, большинство вопросов остаются нерешенными. Притом компьютеризация и внедрение новых технологий способствует возникновению или изменению способов и механизмов совершения преступлений в сфере компьютерной информации. Кроме того, появляются новые методы сокрытия следов преступлений, что является серьезной проблемой для выявления расследования данных видов правонарушений. Вместе с тем, изучение информационных технологий требуют проявления постоянного интереса как со стороны науки, так накопления глубоких знаний особенно для лиц, занимающихся расследованием.

Исследуемая категория преступлений требует усовершенствования методов расследования преступлений в сфере компьютерной информации, внедрения новых технологий в систему МВД России с целью предупреждения указанной категории преступлений, а также понимание работы с ними.

Цель дипломной работы состоит в анализе правоприминительной практики использования специальных знаний при расследовании преступлений

в сфере компьютерной информации, литературы по данной проблеме и разработка на этой основе рекомендаций по совершенствованию методики их расследования.

Объектом исследования являются правоотношения, возникающие при расследование преступлений в сфере компьютерной информации, в частности использований специальных знаний в этой сфере.

Предметом исследования выступают теоретические и практические аспекты формирования специальных знаний, организационного и тактического обеспечения их использования при расследовании преступлений в сфере компьютерной информации.

При изучении данной темы мы ставили перед собой следующие задачи:

1. Рассмотреть теоретико-исторический экскурс преступлений в сфере информационных технологий.
2. Изучить общие положения специальных знаний в расследовании преступлений.
3. Раскрыть особенности проведения отдельных следственных действий в сфере компьютерной информации
4. Изучить специальные знания при расследовании преступлений в сфере компьютерной информации
5. Отразить проблемы, возникающие в ходе расследования преступлений в сфере компьютерной информации
6. Проанализировать практики преступлений в сфере компьютерной информации.

Выпускная квалификационная работа состоит из введения, основной части, включающей две главы, каждая из которых содержит ряд параграфов, заключения, списка использованной литературы.

# ГЛАВА 1. ТЕОРЕТИКО-ИСТОРИЧЕСКИЙ ЭКСКУРС РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## § 1. История возникновения и развития компьютерных преступлений (отечественный опыт)

Исследуя историческое развитие, отметим, что общение людей между собой осуществлялось посредством жестыкуляций, мимики, знаков. После чего в социальном обществе постепенно внедрялись письменность, книгопечатанье.

На этапе становления общественных социальных отношений все большее развитие стали получать: телеграф, телефон, радио, кино, телевидение и уже к концу XX века общество начало осваивать персональный компьютер.

Отметим, что распространение во многие сферы жизнедеятельности компьютерного оборудования повлияло как на координацию действий различных служб, органов, подразделений и организаций, а также на автоматизацию различных производственных и управленческих процессов, так и на состояние технического вооружения преступности в данной области. Информатизация современного общества привела к развертыванию новых усовершенствованных видов преступлений, в процессе совершения которых применяются вычислительные системы, в том числе новейшие средства негласного получения информации.

Что касается зарождения компьютерной преступлений, необходимо отметить само понятие «компьютерные преступления». Данное сочетание получило свое существование с 60-х годов прошлого столетия, где определяется, как «...любого рода незаконное или неразрешенное поведение, которое воздействует на автоматизированную обработку данных и (или) передачу данных». В юридической литературе различными авторами дается множество определений компьютерному преступлению. Так, Б. Б. Леонтьев определил, что «компьютерные преступления – это действия, совершаемые с

целью получения и использования информации в компьютерной сфере, которая может быть, как предметом, так и средством совершения преступления»<sup>1</sup>.

Но стоит сказать, что общество постоянно развивается со стороны информационных технологий, в современном мире практически во всех сферах жизнедеятельности будь то экономическая, политическая, социальная и т.д. закрепилось использование глобальной сети передачи данных «Интернет». Люди используют «всемирную паутину» не только познавательных или развлекательных целях, но и хранения личных данных на различных порталах (Госуслуги), личных фотографий и видеозаписей в «облачных» хранилищах, а также для осуществления финансовой деятельности – платежи, переводы, хранение денежных средств в различных электронных платежных системах. Соответственно и посягательства на перечисленные выше блага стимулирует развитие новых форм преступности.

В связи с этим, термин «компьютерные преступления» постепенно утрачивает свою актуальность, наиболее правильным считаю обозначить эти деяния как «преступления совершаемые с использованием информационно-телекоммуникационных технологий»

Рассматривая историю нашего государства можно отметить, что преступления с использованием компьютерных технологий впервые в России было совершено в 1991 году на территории РСФСР, когда были похищены 125,5 тысяч долларов США со счета Внешэкономбанка СССР сотрудником вычислительного центра вышеупомянутого корпорации.

Дальше тенденция преступности данного направления началась увеличиваться к концу XX века. По данным ГИЦ МВД России было зарегистрировано 7 преступлений в сфере компьютерной информации, в том числе 6 уголовных дел было возбуждено по ст. 272 УК РФ. В 1998 г. зарегистрировано 66 преступлений в сфере компьютерной информации, в том числе по ст. 272 УК РФ – 53. В 1999 г. зарегистрировано 294 преступления, из

---

<sup>1</sup> Леонтьев Б. К. Хакеры, взломщики и другие информационные убийцы 2-е изд. Москва: Майор, 2001. С. 74.

них по ст. 272 УК РФ - 209, по ст. 273 УК РФ - 85. В 2000 г. зарегистрировано 800 преступлений в сфере компьютерной информации, из них по ст. 272 - 584, по ст. 273 - 172, по ст. 274 - 44. К 2003 году в России было возбуждено 1602 уголовных дела по ст. 272 УК РФ. В 2004 году в РФ было выявлено 8739 компьютерных преступлений, из которых было раскрыто 96%. В 2005 году выявлено 10214 преступлений. Как следует из представленных данных, количество регистрируемых преступлений в сфере компьютерной информации представляет собой стабильно неуклонно растущую кривую.

Так, согласно характеристике состояния преступности МВД России общее число зарегистрированных в стране преступлений увеличилось на 1%, тяжких и особо тяжких – на 14%. Основное влияние на рост тяжких преступлений по итогам 2020-2021 года оказало увеличение количества криминальных деяний данной категории, совершенных с использованием информационно-телекоммуникационных технологий. В отчетном периоде число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%<sup>1</sup>.

Эксперт по информационной безопасности А. В. Лукацкий отмечает, причинами роста показателей киберпреступности могут быть самые разные факторы, начиная от улучшения раскрываемости преступлений в сфере высоких технологий, заканчивая просто увеличением числа преступлений, которые так или иначе доводятся до суда, но при этом преступники не наказываются<sup>2</sup>.

Параллельно рассматриваемой статистики необходимо сказать, что неоднократно были предприняты попытки закрепить ответственность за совершение компьютерных преступлений на законодательном уровне. Так, 6

---

<sup>1</sup> Состояние преступности в России за 2020-2021 года, Москва. 2022. URL: <https://мвд.рф/reports/item/28021552/> (дата обращения: 17.01.2022)

<sup>2</sup> Румянцева А. А. Причины роста числа преступлений в интернете, Москва. 2021. URL: <https://ru.rt.com/j3yg> (дата обращения: 16.03.2022).

декабря 1991 года был представлен Закон РСФСР «Об ответственности за правонарушения при работе с информацией» который должен был закрепить в Уголовном кодексе РСФСР нормы, устанавливающие ответственность за данный вид преступлений. В 1992 году был принят Закон РФ № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», но вопрос уголовной ответственности за компьютерные преступления в российском законодательстве решен не был.

Далее Верховный Совет Российской Федерации внес свои предложения Постановлением Верховного Совета РФ от 23.09.92 № 3524-1 «О порядке введения в действие Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» с целью внедрения дополнительных норм в Гражданский, Уголовный кодекс РСФСР другие законодательные акты, связанные с вопросами правовой охраны программ для электронных вычислительных машин и баз данных.

В 1995 году был опубликован проект Уголовного кодекса Российской Федерации (далее – УК РФ), в котором предусматривалась Глава 29 «Компьютерные Преступления», включавшая в себя следующие составы: самовольное проникновение в автоматизированную компьютерную систему (ст. 271); неправомерное завладение программами для ЭВМ, файлами или базами данных (ст. 272); самовольная модификация, повреждение, уничтожение баз данных или программ для ЭВМ (ст. 273); внесение или распространение вирусных программ для ЭВМ (ст. 274); нарушение правил, обеспечивающих безопасность информационной системы (ст. 275)<sup>1</sup>. Но в данной главе было отсутствие единой правовой концепции и слабая проработка статей о компьютерных преступлениях. 13 июня 1996 г. принят Федеральный закон № 63-ФЗ «Уголовный кодекс Российской Федерации»<sup>2</sup>, вступивший в законную силу с 1 января 1997 г., в главе 28 которого закреплена

---

<sup>1</sup> Уголовный кодекс РСФСР (утв. ВС РСФСР 27.10.1960; ред. от 30.07.1996) // Ведомости ВС РСФСР. 1960. № 40. Ст. 591 (утратил силу).

<sup>2</sup> Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 22.08.2021).



ответственность за компьютерные преступления. Основным средством борьбы компьютерными преступлениями должен был стать именно он.

В то время осуществляли свою преступную деятельность такие известные русские хакеры, как Алексей Иванов и Василий Горшков, которым удалось взломать известные платежные системы Western Union, Pay Pal и еще 40 компаний Соединенных Штатов Америки.

Первыми преступниками осужденными по статьям УК РФ о компьютерных преступлениях были Денис Степанов, Александр Петров, Иван Максаков: хакерская атака этой группировки была направлена на сайты букмекерских контор в Великобритании. В результате чего был причинен ущерб в 2 млн. долларов.

Развитие компьютерной преступности привело к необходимости создания подразделения в структуре МВД России, занимающегося раскрытием преступлений с использованием информационных технологий. Так в 1986 году для обеспечения радиоэлектронной безопасности органов внутренних дел, выявления специальных технических устройств, предназначенных для негласного съема информации, пресечения попыток проникновения в компьютерные сети и других противоправных действий в сфере компьютерной информации, в структуре МВД СССР было создано Управление радиоэлектронной борьбы (или Управление «Р»). В последующем 7 октября 1998 года Управление «Р» было преобразовано в Управление по борьбе с преступлениями в сфере высоких технологий (УБПСВТ).

В его структуре были выделены три направления деятельности:

- 1) борьба с преступлениями в сфере компьютерной информации;
- 2) борьба с преступлениями в сфере телекоммуникаций;
- 3) борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

В 1992 году было образовано ещё одно из подразделений МВД России – Бюро специальных технических мероприятий, одним из видов деятельности которого являлось борьба с преступлениями в сфере компьютерных

технологий.

Далее в истории подразделений происходил ряд преобразований в конечном результате подразделение приобрело итоговое наименование Управление «К» – подразделение Министерства внутренних дел России, борющееся с преступлениями в сфере информационных технологий, а также с незаконным оборотом радиоэлектронных средств и специальных технических средств, образованное 4 декабря 2017 года.

Основными задачами Управления «К» выступает выявление, предупреждение, пресечение и раскрытие:

1) Преступлений в сфере компьютерной информации:

- неправомерный доступ к охраняемой законом компьютерной информации;

- создание, использование и распространение вредоносных компьютерных программ;

- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей;

- мошенничество в сфере компьютерной информации.

2) Преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и направленных против здоровья несовершеннолетних и общественной нравственности:

- изготовление и распространение материалов или предметов с порнографическими изображениями несовершеннолетних;

- использование несовершеннолетнего в целях изготовления порнографических материалов или предметов.

3) Преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации.

4) Преступлений, связанных с незаконным использованием объектов авторского права или смежных прав.

При всем том, сегодня в МВД России предпринимаются много усилий

направлений по совершенствованию системы взаимодействий государственных органов с правоохранительными. Преобразование данной системы может быть достигнуто, когда будет регулироваться не только нормативно-правовая база, но и организационные аспекты с практической стороны, которая и позволит эффективно повлиять на угрозы в компьютерно-информационном пространстве.

Также стоит отметить, что важным направлением деятельности данной структуры является привлечение высококвалифицированных специалистов, создании системы подготовки и повышения квалификации кадров, использовании современных программных средств и передовых методик, с целью осуществления положительного опыта раскрытия и расследования преступлений.

## **§ 2. Общие положения специальных знаний в расследовании преступлений**

Словосочетание «специальные знания» остается до сих пор дискуссионным вопросом. Множество авторов по разному трактуют определение «специальные знания». Так, одним из первых данное понятие сформулировал А. В. Дулов, который отметил, что «специальные знания – это знания, которыми недостаточно владеют судьи»<sup>1</sup>. То есть специальные знания выступают недостаточным средством решения поставленных задач, возникающих в ходе судебного разбирательства. Это определение, на наш взгляд, не дает полного раскрытия данного понятия, так как специальные знания применяются не только на судебной стадии, но и на досудебном этапе.

Более полное представление «специальных знаний» в своих трудах отразил В. И. Шиканов, утверждая, что «специальные знания - это знания и полученный опыт, оказавшиеся необходимыми для объективного, полного и всестороннего установления обстоятельств, которые являются предметом

---

<sup>1</sup> Дулов А. В. Вопросы теории судебной экспертизы. Минск: изд-во Белгосуниверситета им. В. И. Ленина. 1959. С. 4.

доказывания делу»<sup>1</sup>.

Интерес вызывает выражение – «оказавшиеся необходимыми»: с одной стороны, можно рассматривать это как обязательность привлечения лиц, обладающих специальными знаниями, с другой, как обращение за помощью к лицу, без которого нельзя обойтись из-за неполного знания какой-либо сферы жизнедеятельности.

В свою очередь А. А. Эйсман разделял знания на «общедоступные и общеизвестные, не имеющие массового распространения, знания, которыми располагает ограниченный круг специалистов»<sup>2</sup>.

Из перечисленного выше списка определений мы можем сделать вывод, что специальные знания рассматриваются и описываются по-разному, имеется широкий спектр подходов к их исследованию. Каждый ученый делает упор на различные свойства и признаки этого явления.

Обобщая взгляды авторов можно выделить наиболее дискуссионные направления, относящиеся к самому понятию «специальных знаний»:

- 1) являются ли научными специальные знания;
- 2) входят ли познания в области права в специальные знания;
- 3) относятся ли к специальным знаниям только профессиональные знания.

Кроме того, немаловажно понимать разграничение между специальными и общеизвестными знаниями. Для одних лиц специальные знания могут выступать общедоступными, другим субъектам данные познания могут быть неизвестны. В судебной практике ориентиром будет выступать суд, то, что для него (суда) не будет выступать общеизвестным, будет составлять область специальных знаний.

Паритет специальных и общедоступных знаний достаточно неустойчив и зависит, в первую очередь от развитости общества и возможности внедрения

---

<sup>1</sup> Шиканов В. И. Проблемы использования специальных знаний и научно-технических новшеств в уголовном судопроизводстве : автореф. дис. ... д-ра юрид. наук. М., 1980. С. 11.

<sup>2</sup> Эйсман А. А. Заключение эксперта. Структура и научное обоснование. М., 1967. С. 91

научных знаний в обыденную жизнь. Отнесение знаний к общедоступным возможно в корреляции с интеллектуальными способностями человека.

Однако в современном обществе хотя и идет тенденция перерастания каких-либо знаний из специальных в общедоступные, количество проведенных экспертиз и привлечение лиц, обладающих специальными знаниями, только растет. На экспертизу выносятся не общедоступные вопросы, а задачи, требующие более широкого анализа.

Таким образом, специальные знания являются важным процессуальным институтом, устанавливающим основания участия сведущих лиц в расследовании преступлений, а также применения этих знаний в уголовном процессе.

### **§ 3. Базовые элементы криминалистической характеристики преступлений в сфере компьютерной информации**

Рассматривая элементы криминалистической характеристики преступлений в сфере компьютерной информации, отметим, что основными являются: орудия, способ совершения, механизм слеодообразования, личность подозреваемого, мотивы совершения указанной категории преступлений.

Орудиям (средства), используемыми при совершении компьютерных преступлений, отметим, является сам компьютер. Вместе с тем, орудиями преступлений в сфере компьютерной информации является не только компьютерная техника, но и специальные программные устройства, системное обеспечение. Так, выделим средства непосредственного и опосредованного (удаленного) доступа.

Орудие указанного вида преступлений будет зависеть от выбора способа совершаемого неправомерного доступа к компьютерной информации.

Орудиями, как правило, являются средства, с помощью которых преступники реализуют свои преступные действия. Так, средством непосредственного доступа к компьютерной информации будут являться,

электронные носители информации, например, USB-накопители, лазерные диски, а также средства преодоления системы защиты ЭВМ. В случае расположения ЭВМ в помещении, оснащено охранными системами, злоумышленнику необходимо будет позаботиться об изготовлении пропуска в данное место, в том числе выяснить идентификационные обозначения для осуществления входа в систему компьютера.

Средствами же опосредованного доступа однозначно будут являться сетевые оснащения, а также средства подхода в удаленные сети, например, модем. В связи с этим, злоумышленникам достаточно наличие соответствующих идентификационных паролей законных владельцев информации.

Следующим важным элементом криминалистической характеристики является способ совершения преступления. В компьютерных преступлениях имеются своеобразные действия по подготовке, совершению и сокрытия преступления. Часто такие действия включают в себя большой круг мероприятий, которые оставляют в обстановке своеобразное отражение, которое и формирует модель компьютерных преступлений.

Рассматривая же способы совершения преступлений в сфере компьютерной информации необходимо отметить их множественность. Их число прогрессивно растет в связи с постоянным изучением преступной средой новых компьютерных технологий, которые быстро набирают обороты в развитии.

Необходимо отметить, что из всех представленных обстоятельств, подлежащих установлению, наиболее сложным является установление способа совершения указанной категории преступления. Вместе с тем, чем сложнее способ совершения неправомерного доступа к компьютерной информации, тем проще разоблачение лица, его совершившего, ввиду ограниченного количества лиц, обладающих соответствующими специальными познаниями<sup>1</sup>

---

<sup>1</sup> Себякин А. Г. Современные возможности использования специальных знаний в области компьютерной техники при расследовании преступлений, связанных с доведением

Целесообразно будет разделить их на несколько групп:

Отмечая первую групп, можно сказать, что действия преступника направлены кражу чужого имущества, то есть на саму компьютерную технику, которая будет выступать как предмет преступного посягательства.

Вторая группа раскрывает способы получения данных с электронно-вычислительной техники с помощью использования разных методов перехвата, к таким методам относятся:

Активный перехват осуществляется с помощью подключения к телекоммуникационному оборудованию ЭВМ, например, к телефонному проводу канала связи, либо непосредственно через соответствующий порт персонального компьютера, в последующем вся полученная информация фиксируется на физический носитель и в последующем предоставляется злоумышленнику в удобной для него форме.

Пассивный (электромагнитный) перехват основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации (например, излучение электронно-лучевой трубки дисплея можно принимать с помощью специальных приборов на расстоянии до 1000 м).

Аудиоперехват, один из часто используемых способов, который подразделяется на два категории. В первую категорию входит установка подслушивающего устройства в электронно-вычислительную технику. Вторая категории включает установку подслушивающего устройства (микрофона) на различные инженерно-технические конструкции как за пределами охраняемого помещения (стены, двери, окна и т.п.), так и внутри помещения (шкафы, стулья, лампы и т.п.).

Видеоперехват осуществляется путем использования различной видеооптической техники (скрытые камеры видеонаблюдения) и может использоваться аналогично аудиоперехвату.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к информации. К ним относятся следующие:

- «Компьютерный абордаж» (hacking) – несанкционированный доступ в компьютер или компьютерную сеть без предоставления прав на это. Этот способ используется преступниками для проникновения в чужие информационные сети (например, подбор паролей);

- «Неспешный выбор» (browsing). При данном способе совершения преступления преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения уязвимых мест в ее защите, обнаружив его, лицо может прописать (ввести команду) которая повлечет за собой модификацию или копирование информации, например с помощью команды, лицо может закинуть на хостинг какую-либо картинку, а в последующем вымогать денежные средства с целью указания уязвимых мест в хостинге;

- «Люк» (trapdoor). Данный способ является практически аналогичным указанному выше способу. Различие заключается в том, что злоумышленник может задать выполнение команд к определенному времени, в последующем которые будут выполняться автоматически и не требуют нахождения преступного лица рядом с компьютерным устройством.

К четвертой группе способов совершения компьютерных преступлений относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники.

К этой группе относятся следующие способы совершения компьютерных преступлений, а именно написание таких программ как:

1. Написание программы, называемой «Троянский конь» заключается в том, что она проникает в компьютерную систему под видом правомерной, откуда и происходит название «троянский конь» в последующем она самостоятельно без участия лица, может собирать данные с компьютера



(различные файлы, фотографии), ограничивать доступ к другим приложениям и программам, а также нанести вред нормальному функционированию операционной системе.

2. «Вирус» – это вредоносное программное обеспечение, которое распространяет свои копии для того чтобы повредить или уничтожить данные имеющиеся на устройстве. Вирус может проникнуть на устройство двумя путями: через сторонние носители информации, либо посредством сети Интернет.

3. «Сетевой червь» – это программа с вредоносным кодом, которая атакует компьютеры в сети и распространяется через нее. Активный сетевой червь может снижать продуктивность устройства жертвы, удалять файлы или даже отключать определенные программы. Основным отличием различных типов червей является способ их распространения. Среди самых популярных – с помощью вложений или вредоносных ссылок в письмах электронной почты и программах для мгновенного обмена сообщениями. Кроме этого, угроза часто распространяется с помощью протоколов Интернета и локальных сетей.

4. «Захватчик паролей» – программа, специально предназначенная для воровства паролей и логинов. Когда пользователь пытается войти в какую-либо систему и при попытка ввода данных вылезет ошибка ввода логина или пароля, хотя данные были введены верно, и в этот момент они были направлены компьютерному злоумышленнику, пользователь думает, что ошибся в вводе данных и при повторной попытке у него получается авторизоваться и ничего подозрительного пользователь не замечает.

5. Особую проблему, конечно, представляют собой эксплойты неизвестных уязвимостей, обнаруженных и использованных преступниками, — так называемые уязвимости нулевого дня. Может пройти много времени, прежде чем производители узнают о наличии проблемы и устранят ее.

Так, Орджоникидзевский районный суд г. Екатеринбурга Свердловской области рассмотрев материалы уголовного дела в отношении Александровского А. Г. Кощеева П. В., которые путем неправомерного доступа

к компьютерной информации, совершили копирование сведений, составляющих коммерческую тайну без согласия их владельца лицом. Так, А. А. Г. согласно своим должностным обязанностям имел доступ системе управления которая включала в себя абонентов компании (их персональные данные). А именно у А. А. Г. В распоряжение имелся логин и пароль к системе взаимоотношения с клиентами. При назначении на административную должность по продажам до А. А. Г. была доведена информация о том, что его работа будет затрагивать коммерческую тайну компании, а именно сведения об абонентах. Летом 2016 года, к А. А. Г. обратилось неустановленное лицо с просьбой передачи сведений об абонентах компании за денежное вознаграждение. А. А. Г., из корыстной заинтересованности согласился передать сведения компании, с целью получения материальной выгоды в размере 30 000 рублей. Далее А. А. Г., не имея достаточных знаний по работе с программным обеспечением, попросил своего знакомого К. П. В. скопировать персональные данные абонентов компании за денежное вознаграждение в размере 5 000 рублей, К. П. В., осознавая, что любые действия с персональными данными абонентов компании незаконны, из корыстных побуждений, согласился выполнить просьбу А. А. Г. о копировании персональных данных абонентов компании, тем самым вступил в преступный сговор с А. А. Г.<sup>1</sup>.

В связи со спецификой рассматриваемого вида преступлений, целесообразно отметить, что при их совершении изменения в обстановке практически не имеют место быть. На сегодняшний день одним из проблемных вопросов данной категории преступления является определение места совершения преступления. К примеру совершения неправомерного доступа к компьютерной информации, может включать в себя несколько мест происшествия:

1) Рабочее место – место обработки информации, ставшее местом преступного посягательства.

---

<sup>1</sup> Приговор Орджоникидзеvский районный суд г. Екатеринбурга Свердловской области № 1-405/2017 от 25 июля 2017 года. URL: <https://sud-praktika.ru/precedent/366904.html> (дата обращения: 15.01.2022).

2) Место хранения компьютерной информации – сервер.

3) Место использование технических средств (персонального компьютера, смартфона и т.д.) для неправомерного доступа к компьютерной информации.

4) Место подготовки к совершению преступления (разработка компьютерных программ для совершения деяния).

Местом происшествия может выступать как одно помещение с компьютером, так и ряд помещений с различными компьютерным устройствами которые взаимодействуют между собой дистанционно.

Таким образом, обстановка совершения преступления тесно взаимодействует со следовой картиной, наличие следов позволяет определить место совершения преступления и последующее задержание лица совершившего деяние.

Следовая картина данного направления преступлений достаточно специфична, она выражается в том, что материальные следы (рук, ног и т. п.), хотя и присутствуют, но не главное место в следообразовании компьютерных преступлений. Наиболее значимые следы компьютерных преступлений присутствуют на электронных носителях (компьютерно-технические следы). Под виртуальными следами понимают следы совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей. Любые действия с компьютерными или иными программируемыми устройствами (мобильными телефонами, смартфонами, планшетами и т.д.) получают свое отображение в памяти. Например данные действия можно обнаружить:

1. В журналах администрирования, журналах безопасности отображаются такие действия, как включение, выключение, различные операции с содержимым памяти компьютера.

2. В реестре компьютера (reg-файлах) отражаются действия с программами (установка, удаление, изменение и т.д.).

3. В log-файлах отображаются сведения о работе в сети Интернет, локальных и иных сетях.

4. В свойствах файлов отображаются последние операции с ними (например, даты создания, последних изменений).

Также к ним относятся: специальные программы (например, для преодоления защиты), алгоритмы ложных условий, подобранные пароли, коды, идентификационные шрифты и др.

Таким образом, виртуальные следы могут служить доказательством того, что с компьютером – его памятью, либо иным устройством осуществлялось несанкционированное взаимодействие, создания, использования и распространения вредоносных компьютерных программ, совершения или подготовки совершения преступления лицом или группой лиц.

Следующим элементом криминалистической характеристики является личность преступника.

Возраст правонарушителей колеблется в широких границах – от 15 до 45 лет, причем на момент совершения преступления у трети возраст не превышал 20 лет. Свыше 80 % преступников в компьютерной сфере – мужчины, абсолютное большинство которых имело высшее и среднее специальное образование. Как показывает практика большинство лиц, совершивших компьютерные преступления, это:

- пользователи ЭВМ, имеющие определенную подготовку и доступ к компьютерной сети;
- операторы, системные программисты, лица, производящие техническое обслуживание и ремонт компьютерных сетей или систем;
- административно-управленческий персонал (руководители высшего и среднего звена, бухгалтеры, экономисты и др.).

Личности «компьютерного» преступника целесообразно разделить на три обособленные группы.

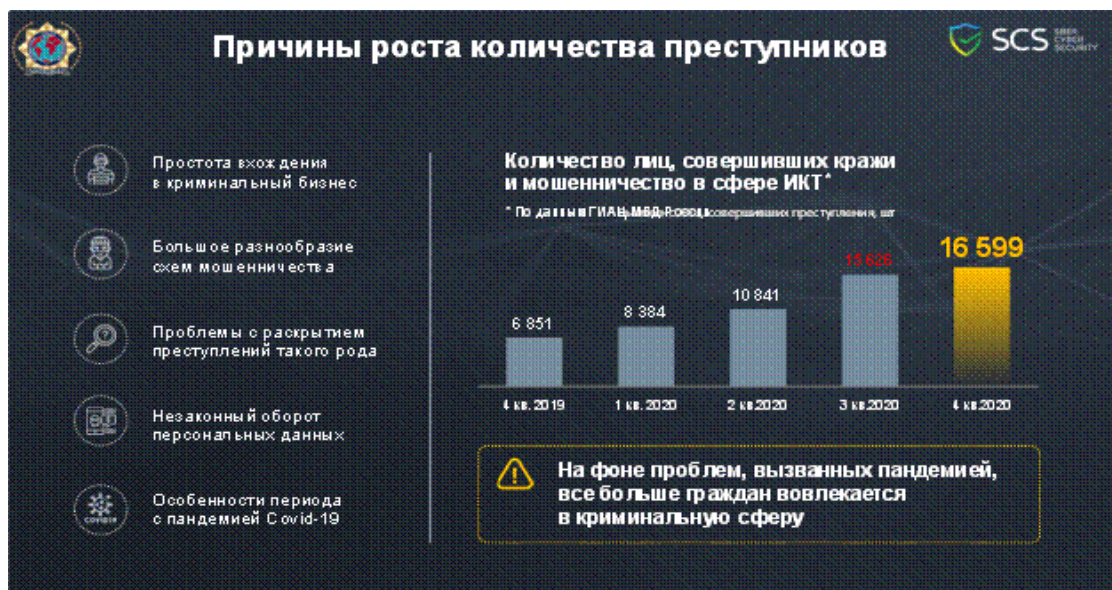
К первой группе относятся лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной

техники и программирования с элементами своеобразного фанатизма и изобретательности. Эти субъекты воспринимают средства компьютерной техники как своеобразный вызов их творческим и профессиональным знаниям, умениям и навыкам.

Вторая группа, включает в себя лиц, которые страдают новым видом психических заболеваний – информационными или компьютерными фобиями. Совершаемые ими преступления, в основном связаны с преступными действиями, направленными на физическое уничтожение либо повреждение средств компьютерной техники (далее – СКТ) без наличия преступного умысла, с частичной или полной потерей контроля над своими действиями.

В третью группу входят «профессионалы» выделяющаяся среди других явными корыстными целями. Как раз она несет основную угрозу миру. Качественные и количественные показатели их преступной деятельности занимают высокий уровень.

Также стоит отметить, что в связи с появлением пандемией коронавирусной инфекцией в 2019 году стремительно выросло число лиц, которые лишились работы и с целью заработка стали искать работу в информационно-коммуникационной сети интернет, но у многих возникли идеи заниматься заработком нарушая законодательство, об этом свидетельствуют показатели предоставленные ПАО Сбербанк:

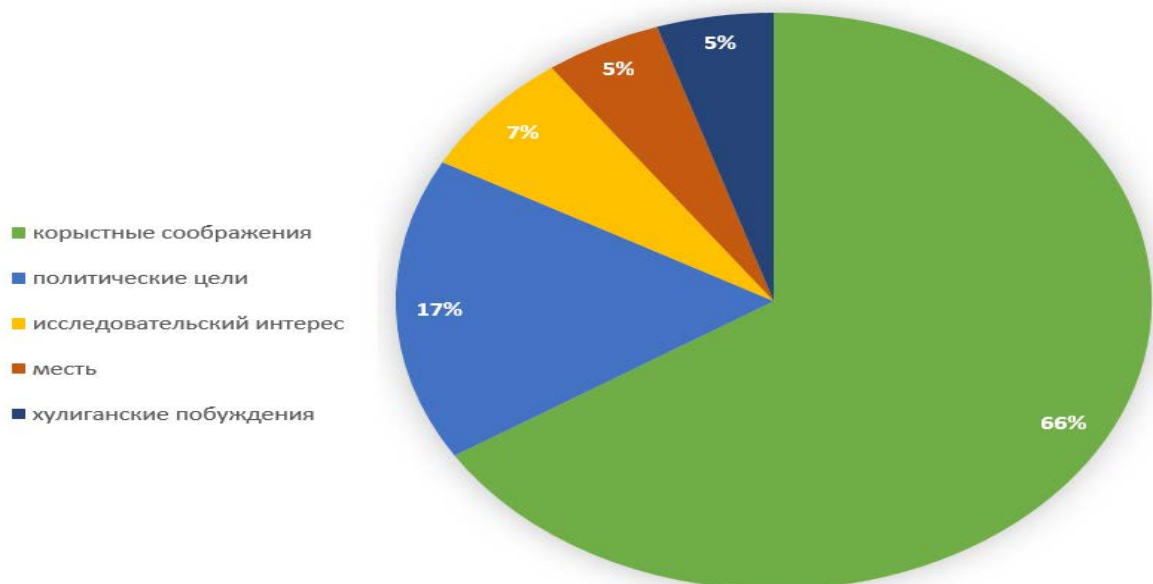


«рис. 1.1»

Немаловажно будет отметить мотивы указанной категории преступлений. Мотивами совершения преступлений в сфере компьютерной информации являются:

- корыстные соображения (совершаются в основном преступниками третьей группы);
- политические цели (шпионаж, преступления, направленные на подрыв финансовой и денежно-кредитной политики правительства, на дезорганизацию валютной системы страны, на подрыв рыночных отношений - совершаются исключительно преступниками третьей группы);
- исследовательский интерес (совершаются в основном преступниками первой группы);
- хулиганское побуждение (преступники первой и второй группы);
- месть (совершаются в основном преступниками второй группы).

Процентную составляющую мотивов совершения преступления можно рассмотреть на диаграмме:



«рис. 1.2»

Существенную роль в структуре криминалистической характеристики компьютерных преступлений играют также обобщенные сведения о потерпевшей стороне.

На практике потерпевшими от компьютерных преступлений обычно выступают юридические лица. Это объясняется тем, что на данный момент в России в процесс компьютеризации втянуты различные учреждения, организации и предприятия всех форм собственности. Зачастую атака осуществляется на операционные системы компьютеров, которые использует юридические лица, а также кража конфиденциальной информации, которая хранится на персональных компьютерах, с целью дальнейшего выкупа.

Стоит отметить также, что юридические лица не хотят предоставлять в органы предварительного следствия информацию о кибератаках на их устройства в связи с тем, что проверка факта совершения преступления занимает большое количество времени, которое может нанести дальнейшей работе организации в стандартном режиме. Кроме этого пострадавшая сторона не всегда спешит сообщить в правоохранительные структуры о факте совершения компьютерного преступления опасаясь подрыва своей репутации, лица занимающиеся обеспечением компьютерной безопасности компании понимают, что могут поставить под вопрос их профессиональную квалификацию, в связи с чем прослеживается латентность данной категории преступлений.

Вторую группу потерпевших составляют лица, которые пользуются услугами, предоставляемыми юридическими лицами, и попадают под действие кибератак, обрушивающихся на компанию-источник услуги.

Третья группа потерпевших страдает от «компьютерных пиратов». «Компьютерные пираты» – осуществляют кражу лицензированной компьютерной продукции путем её копирования, тиражирования и перепродажи. Кроме краж лицензированной компьютерной продукции, также распространены преступления, связанные с нейтрализацией защиты программ, которые позволяют произвести использование программного продукта без покупки официальной лицензии.

В целях грамотного осуществления расследования необходимо привлечь потерпевшего как источника первоначальной информации о

криминальном событии. Характеризуя потерпевшего, следует отметить, что данное лицо обладает лучшей мотивацией для реализации наступательных действий<sup>1</sup>.

В заключении рассматриваемой главы стоит отметить, что преступления в сфере информационных технологий имеют достаточной «молодой» возраст. Их активное совершение, и, как следствие – расследование, началось в XX в. Это повлекло за собой разработку и формулировку специальных знаний, раскрытие базовых элементов криминалистической характеристики.

---

<sup>1</sup> Низаева С. Р. Личность потерпевшего как элемент криминалистической характеристики мошенничества в сфере оборота жилой недвижимости // Правовое государство : теория и практика. 2017. № 3 (49) С. 141–143.



## **ГЛАВА II. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

### **§ 1. Особенности использования специальных знаний при осуществлении следственных действий в ходе расследования преступлений в сфере компьютерной информации**

В литературе нет единого подхода к проблеме привлечения специалистов к участию в следственных действиях. Так, Е. Я. Лопушна рекомендует приглашать специалистов к участию в следственных действиях в тех случаях, когда имеется необходимость в использовании специальных знаний и без таких знаний следователь или суд не в состоянии выяснить те или иные вопросы<sup>1</sup>.

По мнению В.Н. Махова, привлечение специалиста полезно и для выполнения работы, которую следователь мог проделать сам, но медленнее и менее качественно, чем специалист<sup>2</sup>.

Под необходимостью использования специальных знаний и навыков специалиста при этом признаются предусмотренные законом случаи обязательного вызова специалиста для участия в следственных действиях либо случаи, когда следователь и суд убеждаются в невозможности их проведения без участия специалистов. Практическая целесообразность применения специальных знаний и навыков специалистов, по мнению А.В. Мусиенко, не зависит от субъективных возможностей следователя, а состоит в оптимальном использовании специальных знаний при расследовании преступлений исходя из интересов научной организации труда<sup>3</sup>.

При расследовании преступлений в сфере компьютерной информации,

---

<sup>1</sup> Лопушна Е. Я. Участие специалиста-криминалиста в следственных действиях: Автореф. дисс. ... канд. юрид.наук. Алма-Ата, 1971. С. 7.

<sup>2</sup> Махов В. Н. Участие специалиста в следственных действиях: Автореф. дисс. ... канд. юрид. наук. М., 1971. С. 10.

<sup>3</sup> Мусиенко А. В. Указ. соч. С. 97.

следует учитывать, что указанный вид преступных деяний вызывает многочисленные трудности.

Одной из важнейших проблем, которые возникают при расследовании преступлений данной категории – это определение места совершения преступления, например, неправомерный доступ к компьютерной информации (ст.272 УК РФ), поскольку местом совершения подобного деяния, как правило, может являться:

- рабочее место преступника, место хранения или резервирования информации;
- место подготовки программ взлома;
- место самого использования информации, которую получили неправомерно.

Немаловажным будет отметить тот факт, что на сегодняшний момент можно выделить новое место совершения – это «информационное пространство», которое характеризуется различными учеными и практиками, как совокупность информационных структур, которые составляют государственные и межгосударственные компьютерные сети, телекоммуникационные системы и сети общего пользования, иные трансграничные каналы передачи информации.

Указанная проблема демонстрирует тот факт, что следователю будет довольно сложно производить такое следственное действие, как осмотр места происшествия, то есть осуществлять сбор и фиксацию доказательственной информации.

Отметим, что для качественного, эффективного и результативного проведения данного следственного действия, лицу, его осуществляющему необходимы соответствующие специальные знания в информационного – телекоммуникационной области и познаний особенностей расследования киберпреступлений.

При осмотре места происшествия в состав следственно-оперативной группы в зависимости от конкретной следственной ситуации помимо

следователя должны входить: специалист-криминалист, знающий особенности работы со следами по преступлениям данной категории; специалист по ЭВМ; сотрудник ФСТЭК России, Центра защиты информации (при наличии на месте происшествия конфиденциальной компьютерной информации) и др.

Планирование первоначального и неотложного следственного действия, как осмотр места происшествия, необходимо обратить внимание на несколько важных моментов, так как специфика данных преступлений заключается в работе с компьютерной техникой, и следователю рекомендуется для оптимизации времени, грамотно построить линию поведения всех участников осмотра.

Целью осмотра места происшествия является установление конкретного средства вычислительной техники и компьютерной информации, которая может выступать в качестве предмета либо орудия совершения преступления и нести в себе следы преступной деятельности<sup>1</sup>.

При проведении любой манипуляции с компьютером обеспечить обязательное участие специалиста, поскольку малейшие неверные действия могут повлечь безвозвратную потерю доказательственной информации. Наиболее распространённые следственные действия, где рекомендуется привлечение специалиста, - это следственный осмотр, обыск, выемка. С момента получения исходной информации и до направления материалов дела прокурору необходимо взаимодействовать с оперативными работниками. В частности, по указанной категории уголовных дел очень важно оперативное сопровождение. При проведении оперативно-розыскных мероприятий оперативному работнику необходимо вести целенаправленный поиск источников получения доказательств совершенного преступления, проводить работу по выявлению ранее неизвестных свидетелей, осуществлять проверку лиц, которую могут быть причастными к расследуемому событию. Также рекомендуется привлечь потерпевшего как источник первоначальной

---

<sup>1</sup> Сысенко А. Р. Особенности осмотра места происшествия при расследовании компьютерных преступлений // Закон и право. 2020. № 12. С. 216–218.

информации о криминальном событии. Характеризуя потерпевшего, следует отметить, что данное лицо обладает лучшей мотивацией для реализации наступательных действий. Кроме того, потерпевшие и их сотрудники имеют более высокую в области информационных технологий.

В начале осмотра с помощью специалиста можно установить функциональное назначение ЭВМ; определить включено оно или нет; проверить его работоспособность и наличие в его памяти компьютерной информации. Рекомендуется обратить особое внимание на иную систему, которая соединяет компьютеры друг с другом, определяющую наличие соединения компьютера в локальную вычислительную сеть. При наличии данного соединения необходимо найти сервер, в котором размещена часть информации и от которой зависит работа всех элементов сети. Для предотвращения модификации или уничтожения информации с удаленных рабочих мест, которые могут находиться на некотором расстоянии от осматриваемого объекта, рекомендуется определить наличие кабелей и проводов, ведущих в другие помещения от самой электронно-вычислительной техник. После обратить внимания на материальные следы, которые могут находится на системном блоке, комплектующих деталях и проводных соединениях.

В ходе осмотра места происшествия данной категории преступлений следственно-оперативной группе необходимо помимо установления всех обстоятельств совершенного преступления (работы с потерпевшей стороной и свидетелями, установления лиц которые имели доступ к компьютерной технике). Также стоит обратить большее внимание на следовую картину, правильно зафиксировать и изъять следы.

При обнаружении следов на месте происшествия, кроме традиционных к примеру, трасологических, которые нужно зафиксировать в первую очередь (так как возможно злоумышленник был неосторожен и оставил следы рук, ног и т.д.) необходимо обратить внимание на компьютерные следы, где будет проводится работа непосредственно с электронно-вычислительной техникой

(персональный компьютер, системный блок, монитор, переносные носители информации: флэш-накопители, жесткие диски и т.п.). При осмотре монитора необходимо зафиксировать информацию на нем с применением правил криминалистического фотографирования или составления чертежа. В ходе детального осмотра выявить программы, запущенные на компьютерном устройстве. Далее необходимо зафиксировать наличие подключения внешних кабелей к компьютерным средствам, для того чтобы в последующем правильно восстановить их соединения.

Детальному осмотру будет подлежать компьютерная техника, которая может находиться как во включенном, так и в выключенном состоянии, так из нее можно будет извлечь содержащуюся в ней информацию о самом преступлении, какие программы использовало преступное лицо для осуществления преступного умысла. Также сведения об операционной системе, установленном программном обеспечении можно определить по ветке системного реестра компьютера.

Таким образом, поиск информационных следов (цифровых артефактов) в технических средствах можно осуществлять посредством использования встроенных в операционную систему элементов и средств<sup>1</sup>.

В ходе подготовки к производству осмотра, в том числе и беседы с представителями предприятия, учреждения, организации или лицами которые имеют отношения к совершенному преступлению необходимо получить первичную информацию о системах организации процесса функционирования компьютерно-технических средств, а также установить те, которые могли быть использованы в результате совершения преступлений.

В рамках проведения оперативно-разыскного мероприятия, как опрос, необходимо выяснить обстоятельства, касающиеся наличия и разновидностей операционных систем, установленных на каждом персональном компьютере;

---

<sup>1</sup> Харисова З. И., Файзулова Р. Р., Дюсьмекеева Д. С. Современные угрозы информационной безопасности в условиях глобализации информационного пространства В сборнике Всероссийской научно-практической конференции : Актуальные проблемы кибербезопасности в сети Интернет: сборник научных трудов конференции. 2020. С. 163–165.

вариации программного обеспечения, программ защиты и шифрования абонента. Кроме того, устанавливаются места хранения данных, резервных копий, а также наличие паролей супервизора и администраторов системы<sup>1</sup>.

Отметим, что осмотр места происшествия необходимо осуществлять незамедлительно с момента поступления сообщения о преступлении. В большинстве случаев при совершении преступлений данной категории существует проблема, где после него проходит значительное время, в процессе которого злоумышленниками осуществляются неправомерные действия по сокрытию следов, отключению персональных компьютеров или стиранию с них информации, а также осуществление продолжения преступной деятельности.

Непосредственно, приступая к производству осмотра места происшествия, в ходе которого предстоит работа с персональным компьютером, нельзя упускать тот момент, где могут быть установлены специализированные защитные программы, которые без совершения определенных операций начинают уничтожать информацию, которая в дальнейшем будет нести в себе доказательственное значение. В связи с этим, необходимо выяснить обозначения пароля к данному техническому средству или отдельным программам.

Необходимо учитывать, что в соответствии с действующим законодательством изъятию подлежит только та информация, которая имеет отношение к расследуемому виду преступления, следовательно должен определить ее содержание, а также скопировать имеющиеся отношение к расследуемому событию документы.

Исходя из различных мнений ученых-криминалистов, отметим, что для успешного и быстрого выявления, а также объективного и всестороннего расследования преступлений в сфере информационных технологий непременно необходимы новые апробированные в науке и правоприменительной практике. Несмотря на необходимость прохождения сотрудниками дополнительных

---

<sup>1</sup> Кузнецова А. А. Методика расследования налоговых преступлений: учеб. пособие / под общ. ред. проф. М., 2007. С. 110.

курсов в сфере информационных технологий, не стоит так же забывать, что привлечение грамотных специалистов или экспертов также положительно повлияет на расследовании преступлений, предохраняя следователя от совершения неверных и не квалифицированных действий, направленных на уничтожение к примеру важных доказательств.

Анализируя литературу, можно отметить, что помощь специалиста в расследования данного вида преступлений заключается:

- в обнаружении, фиксации и изъятии следов с помощью средств криминалистической техники;
- в описании следов в протоколе, составлению планов и схем их расположения;
- в консультациях по вопросам изучения следов и их отборе для исследования;

Так же существует большая угроза по поводу того, насколько грамотный специалист привлекается к помощи расследования преступления, следователь не должен подвергаться сомнению в профессиональных знаниях. На практике допускают большое количество ошибок, из-за привлечения некомпетентного специалиста, не владеющего специальными навыками и знаниями работы с компьютерной техникой, например, возникали случаи, когда привлекали квалифицированного пользователя ПК, но не владевшего навыками обращения с большими ЭВМ на должном уровне, что вызывало проблемы при проведении следственного действия. В связи с этим важно привлекать специалистов с необходимым профилем знаний. Нередко он должен разбираться в специфических вопросах (особенностях эксплуатации сетевого оборудования, процедурах шифрования информации и т.п.). К тому же следователи отмечают, наиболее целесообразно и эффективно привлекать специалистов которые в последующем будут выступать в роли экспертов при проведении компьютерно-технической экспертизы.

Как мы знаем, что немало важным условием проведения обыска и выемки является то, что искомые объекты, которые могут быть доказательствами

находятся в месте где мы хотим провести следственные действия. Сам поиск доказательств в необычных условиях, так сказать в технологической среде, по сути сохраняет признаки традиционного обыска, правда форма проведения следственного действия специфична. В связи с этим есть необходимость осуществления определенных действий, для расследования таких преступлений, это:

- определение конфигурации вычислительной системы, топологии внутренних компьютерных сетей, используемой схемы подключения к глобальным сетям Интернет, осмотр кабельных линий связи в целях выявления, не санкционированных владельцем физических подключений, а также определение технических параметров устройств;

- выявление вредоносного программного обеспечения, которое нанесло вред ЭВМ и способствовавшего совершению преступления;

- изучение системы обеспечения защиты информации на объекте, порядка доступа в локальную сеть и выхода из нее в глобальные сети Интернет, требований к обработке конфиденциальной информации<sup>1</sup>.

Что касается понятых, то здесь также необходимо обращать внимания на то, что эти привлекаемые лица к участию в следственном действии имеют примитивные познания о процессе работы компьютерной техники, так как это необходимо чтобы в дальнейшем исключить факты того, что следователем в ходе следственных действий были сфальсифицированы доказательства, например стерты какие-либо файлы с персонального компьютера, либо наоборот установлено на него какое-либо программное обеспечение которое способствовало осуществлению преступного умысла.

Частой ошибкой на практике является неправильная упаковка и в последующем транспортировка компьютерно-технических средств, которые изымаются в ходе следственных действий. Здесь следователю стоит учитывать некоторые моменты в ходе осуществления данных действий:

---

<sup>1</sup> Осипенко А. Л. Сетевая компьютерная преступность. Теория и практика борьбы. Монография, Омская академия МВД России 2009. С. 255.



- изымать компьютерную технику в выключенном состоянии, с отсоединёнными от нее периферийными устройствами.

- при отсоединении от компьютерного устройств различных проводов схематично отобразить порядок их соединений протоколе, а также во избежание ошибок подписать каждый порт который был задействован и для чего именно;

- важный момент имеет факт подключения компьютерно-технического устройства к каналу связи, определение вида подключение (проводное или беспроводное), а также провайдера связи.

- при изъятии системных блоков их обязательно опечатывают, с целью исключить возможности снятия с них информации, повреждения, разукomплектования (вытаскивание жестких дисков), что может привести к утрате вещественного доказательства. Опечатывать системных блок необходимо с двух сторон где имеются порты, выходящие из материнской платы и блока питания ПК, также захватывать боковые стороны корпуса с целью недопущения открытия крышек корпуса и попадание к комплектующем деталям (процессор, оперативная память, видеокарта, HDD и SSD диски). Не стоит забывать, что на опечатанном листе бумаге нужно проставить подписи участвующих лиц в следственном действии. На практике существуют разные способы упаковки, всё зависит от самого корпуса системного блока, его формы и из чего он изготовлен, довольно часто в последнее время встречаются системные блоки со стеклянными вставками, и понятно, что при неаккуратной транспортировке оно может разбиться. В связи с этим необходимо упаковать системный блок в коробку и закрепить его внутри, например, пенопластом для исключения его перемещения внутри коробки.

- при транспортировке исключить действие на изъятое устройство различных металлоискателей и иной аппаратуры с электромагнитным излучением, приборов с мощными источниками магнитного поля, что может нанести вред работе компьютерной технике в последующем, например, при осуществление экспертизы.

– перемещение изъятого оборудования должно производиться с учетом всех вышеперечисленных требований, при этом важно исключить физическое воздействие на оборудование, влияние электромагнитных лучей и полей, атмосферных факторов, а также высоких и низких температур, влекущих повреждение аппаратуры<sup>1</sup>.

Тактика допроса свидетелей. При подготовке к допросу возможных свидетелей необходимо тщательно подготовиться, в частности продумать круг вопросов, интересующих по расследуемому преступному событию.

Круг интересующих следствие вопросов будет зависеть от статуса конкретного допрашиваемого лица на предприятии.

В связи с этим, рекомендуем обратить внимание на освещение вопросов, касающихся его интереса к компьютерным сведениям, программному обеспечению; не наблюдал ли свидетель посторонних лиц на предприятии, не привлекался ли работник не компетентный в своей отрасли знаний; не наблюдались ли неполадки в работе системы, хищений электронных носителей информации, а также оборудования; круг сотрудников, посещавших предприятие вне рабочее время, интересовались ли работой не касающейся их напрямую; были ли случаи включения средств защиты ЭВМ; наличие проверок систем на наличие вирусов, и их результаты; даты обновления программного обеспечения; где и как приобретаются телекоммуникационные технические устройства и где осуществляется их ремонт; способы поступлений, передачи и обработки по каналам связи компьютерных сведений предприятия; каким образом осуществляется защита компьютерной сети и др.

Таким образом, при расследовании преступлений в сфере информационно-коммуникационных технологий необходимо учитывать следующие требования:

Первое это следователю необходимо ограничить доступ к устройством ввода со стороны третьих лиц. Во-вторых, должны быть приняты меры к тому,

---

<sup>1</sup> Менжега М. М. Методика расследования создания и использования вредоносных программ для ЭВМ / М. : Юрлитинформ, 2010. С. 103-104.

чтобы не изменялись условия электроснабжения ЭВМ. И в-третьих, при обнаружении незнакомых средств, способных оказать влияние на искомые данные, в последующем – доказательства, необходимость принятия решение о дополнительном привлечении специалистов в области информационных технологий.

## **§ 2. Судебные экспертизы, назначаемые при расследовании преступлений в сфере компьютерной информации**

Хорошо организованные преступные группы и сообщества для достижения корыстных целей активно и высокопрофессионально применяют в своей деятельности новые методы, подходы, специальные программно-аппаратные средства, системы удаленного доступа и криптографического шифрования, высокотехнологичную технику и интеллектуальные комплексы принятия решений<sup>1</sup>.

При расследовании преступлений в сфере компьютерной информации принципиальное значение имеет производство судебных экспертиз, поскольку в дальнейшем результаты ее производства будет иметь большое доказательственное значение в суде.

Рассматривая разновидности судебных экспертиз, назначаемых в ходе расследования преступлений указанной категории отметим, что наряду с традиционными исследованиями, такими как: дактилоскопическими (по следам пальцев рук), почерковедческими (по рукописям, использованным при подготовке к преступлению), назначаются и специфические судебные экспертизы.

Так, к разновидностям специфических экспертиз относится судебная компьютерно-техническая экспертиза, которая в свою очередь включает в себя

---

<sup>1</sup> Антонов В. В., Харисова З. И., Мансурова З. Р., Родионова Л. Е., Калимуллин Н. Р., Куликов Г. Г. Системная модель интеллектуальной предметно-ориентированной профайлинг-системы // Онтология проектирования. 2020. Т. 10. № 3. С. 338–350.

четыре подвида.

В качестве первого подвида судебной компьютерно-технической экспертизы отметим аппаратно-компьютерное исследование, заключающееся в производстве анализа технических, а иногда их называют аппаратных средств компьютерного оборудования. Сущность данной экспертизы является установление события, тесно связанного с использованием технических средств. Объектами указанного вида судебной экспертизы, являются: настольные и портативные персональные компьютеры; аппаратные средства, предназначенные для организации сетевой работы – серверы, активное оборудование, рабочие станции, сетевые кабели и пр.; периферийные устройства, предназначенные для работы с персональным компьютером – клавиатуры, манипуляторы, аудиосистемы, внешние накопители информации и пр.; встроенные аппаратные системы, произведенные на базе микропроцессорных контроллеров – транспондеры, круиз-контроллеры, иммобилайзеры (электронное противоугонное устройство, функция которого – препятствовать запуску двигателя и передвижению на автомобиле при попытке угона); интегрированные системы – смартфоны, различные мобильные телефоны, навигаторы и пр.

Немаловажным будет отметить, что возможности аппаратно-компьютерной экспертизы применяют не только при расследовании уголовных дел, но и в гражданско-правовых спорах. Кроме того, данный вид исследования назначается при анализе аппаратного оборудования в целях установления их функционального предназначения, обстоятельства использования указанных аппаратных средств для совершения определенного преступного деяния. Данный анализ будет производиться с использованием специализированного программного обеспечения в который будет включаться анализ памяти, работа с паролями, ключи Shellbags реестра, Интернет-активность, LNK-файлы.

Информация об уязвимости процессов переработки информации в информационных системах (важная при расследовании преступлений, связанных с нарушением информационной безопасности в открытых

компьютерных сетях, хищением (разрушением, модификацией) информации и нарушением информационной безопасности) формируется именно на аналитической стадии. Также посредством применения преимуществ аппаратно-компьютерной экспертизы восстанавливаются сведения, находящиеся на вышедших из строя электронных носителях информации, то есть происходит выявление замаскированных программами данных.

Формулируя вопросы на судебную компьютерно-техническую экспертизу рекомендуем исходить из ситуационного подхода, то есть в зависимости от целей, задач расследования.

Так, данный вид исследования решает вопросы, связанные с определением вида аппаратного средства, его состояния, наличием неисправностей, заводских браков. Кроме того, ставятся вопросы, касающиеся наличия неисправностей при его эксплуатации, повреждения, причин неисправностей. Также посредством проведения судебной компьютерно-технической экспертизы решаются вопросы, связанные с данными, находящимися на электронных носителях и возможности их восстановления.

Вторым подвидом является программно-компьютерная экспертиза, которая в свою очередь назначается для исследования обстоятельств, связанных с противоправным созданием и распространением вредоносных компьютерных программ.

На сегодняшний день, род программно-компьютерной экспертизы включает в себя следующие виды судебных экспертиз:

- экспертиза системного программного обеспечения;
- экспертиза сервисов веб-серверов;
- программно-компьютерная экспертиза системной безопасности;
- программно-компьютерная экспертиза баз и банков данных.

Данное деление базируется на необходимости для экспертов познаний не только в общей теории программирования, но и в ряде отличных друг от друга областей. В первую очередь это касается инструментария и углубленного знания характеристик не только отдельных операционных систем, но и их

частей.

Программно-компьютерная экспертиза включает в себя цель исследования программного обеспечения, которое может служить установлением способов совершения преступления. Также установления индивидуальных особенностей работы программы, как она функционирует, что необходимо для ее работы, ее взаимосвязь с информационным обеспечением.

Этот перечень является далеко неисчерпывающий, так как постепенно возрастает потребность в подробном исследовании программно-компьютерного оснащения.

Вопросы, задаваемые эксперту, базируются на задачах, решаемых в процессе осуществления исследования. В общем случае вопросы выглядят следующим образом:

1. Каковы общие характеристики исследуемого программного обеспечения?
2. Из каких компонентов состоит данное программное обеспечение?
3. Какова классификационная принадлежность исследуемого программного обеспечения?
4. Каковы характеристики файлов, составляющих исследуемое программное обеспечение (дата создания, тип, размер и пр.)?
5. Как называется данное программное средство? Каков его тип? Кто является разработчиком?
6. Какая версия программного обеспечения представлена для проведения экспертизы?
7. Какова функциональная особенность исследуемого программного обеспечения?

Программно-компьютерная экспертизы зачастую занимается исследованием программных продуктов на признаки контрафактности и выявлением автора создаваемых программ.

Так, Калининский районный суд г. Уфы Республики Башкортостан рассмотрев материалы уголовного дела в отношении Раминов Ф. Р., который

при подготовке к совершению преступления изучил правила по использованию вредоносных программ в информационной телекоммуникационной сети «Интернет», для осуществления незаконного копирования информации, обладая достаточными сведениями в области компьютерной информации совершил использование компьютерной программы. Так, находясь по месту своего проживания используя свой ноутбук и занес на него вредоносную компьютерную программу заведомо созданная для неправомерного копирования компьютерных сведений, реализовал незаконное воздействие. При осмотре места происшествия и заключения эксперта, установлено, что на жестком диске ноутбука находилась программа для подготовки сведений и работы, а также обработки компьютерной информации. Кроме того, на компьютере обнаружены признаки запуска программы. Основным ее предназначением является неправомерное влияние на сетевые ресурсы для перенесения сведений баз данных<sup>1</sup>.

Следующий подвид компьютерно-технической экспертизы является информационно-компьютерная. Данный вид исследования изучает цифровую информацию, то есть данные, находящиеся в компьютерной системе. В качестве примера можно привести проектную документацию на разработку и использование компьютерного оборудования и сетей, либо конфиденциальная информация в электронном формате, позволяющая установить тождество при исследовании.

Указанный вид судебной компьютерно-технической экспертизы позволяет завершить расследование, поскольку отвечает на ряд завершающих и ключевых вопросов, связанных с цифровыми документами. Изучая цифровую информацию можно определить механизм появления следов при работе с компьютером, а именно с какими приложениями работал пользователь.

Отметим, судебная информационно-компьютерная экспертиза решает

---

<sup>1</sup> Приговор Калининского районного суда г. Уфы Республики Башкортостан № 1-499/2017 от 14 ноября 2017 года URL: <https://sud-praktika.ru/precedent/456303.html> (дата обращения: 19.01.2022).

широкий круг задач, направленных на определение способа форматирования носителя, обнаружения мест хранения файлов, а также их формат, объем, время создания. Дополнительно, определяется разновидность файлов, способы доступа к информации ЭВМ. Вместе с тем, осуществляются мероприятия по идентификации средств защиты от копирования, модификации, передаче информации.

Информационно-компьютерная экспертиза является сложным исследованием, так как зачастую для анализа одного компьютерного устройства может понадобиться много времени и усердного труда.

Список вопросов напрямую зависит от характера представленных для проведения экспертизы объектов, а также от предмета и цели исследования.

1. Какова степень совпадения действий пользователя и специальных правил эксплуатации данного персонального компьютера (компьютерной системе)?

2. Содержит ли данный носитель информации какие-либо данные?

3. В каком формате содержатся данные на носителе?

4. Файлы какого типа содержатся на представленном для анализа носителе данных?

5. Имеются ли на данном накопителе данных какие-либо средства защиты от копирования или несанкционированного доступа?

И завершающим подвидом обозначим судебную компьютерно-сетевую экспертизу. Она получает свое существование на функциональном предназначении компьютерных средств. Все перечисленные выше задачи могут решаться данным видом исследования, поскольку ее объекты дифференцированы из представленных судебных экспертиз.

Для решения задач компьютерно-сетевой экспертизы, эксперту необходимо иметь определенные познания в сфере сетевых технологий. А именно иметь представления о работе сетевых технологий таких как: Ethernet, Token Ring, FDDI, ATM.

Круг задач, решаемых компьютерно-сетевой экспертизой, заключается в



исследовании программных сетевых средств, персональных компьютеров, имеющих выход во всемирную сеть интернет. А именно характеристик сети, ее конфигурацию, организацию доступа к данным, выявление установленных сетевых компонентов, выявление изменений которые вносились в компьютерную сеть определение следов оставленными внешними программами.

Кроме того, устанавливается механизм модификации содержимого исследуемой сети, их причины. Отметим, что посредством проведения указанного вида исследования устанавливается текущее состояние сетевой системы или сетевого программного или аппаратного средства, наличие физических дефектов аппаратных средств; определяются специфические характеристики сетевой системы, ее конфигурация, тип устройства архитектуры, а также установленных сетевых программно-аппаратных средств.

Компьютерно-сетевая экспертиза предназначена для анализа информационно- сетевого пространства. Практически любые применяемые в сетевых системах технологии на сегодняшний день успешно анализируются и исследуются.

Вопросы, которые могут быть заданы эксперту по осуществлению компьютерно-сетевой экспертизы:

1. Есть ли признаки того, что данное компьютерное средство работает в сети Интернет?
2. Каково содержание установок программы удаленного доступа к сети Интернет и протоколов соединений?
3. Каковы причины изменения свойств исследуемой компьютерной сети?
4. Имеются ли на компьютере, представленном на экспертизу, аппаратные и/или программные средства, предназначенные для работы данного компьютера в какой-либо компьютерной сети?
5. Имеется ли причинная связь между использованием исследуемых программно-аппаратных средств компьютерной сети и результатами их работы? Если имеется, то каков ее характер?

6. Обнаружены ли признаки работы данного персонального компьютера во всемирной сети интернет?

7. Каким образом настроена программа удаленного доступа в сеть? Каковы ее специфические особенности?

8. Каким образом настроены протоколы соединений?

В заключении отметим, что судебная компьютерно-техническая экспертиза очень молода. Назначение данного вида экспертиз требует определенных познаний в компьютерной сфере. Большинство экспертов прибегают к собственным способам и методикам ее проведения, что может отразиться на доказательственной базе.

### **§ 3. Проблемы использования специальных знаний в расследовании преступлений в сфере компьютерной информации**

Глава 28 представлена совокупностью правовых норм, содержащих санкции за совершение преступлений в сфере компьютерной информации, понятие которой сформулировано в примечании к ст. 272 УК РФ как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Очевидно, что применительно к установлению обстоятельств, характеризующих объективную сторону совершенного деяния, подобная формулировка не может расцениваться как исходное понятие.

Специалисты в данной области предлагают понимать компьютерную информацию как фактические данные, обработанные компьютерной системой и (или) передающиеся по телекоммуникационным каналам, а также доступные для восприятия, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного, гражданского или административного дела.

В ст. 5 УПК РФ вопрос о содержании понятия «компьютерная информация» не урегулирован, в связи с этим при расследовании преступлений

компетентные органы исходят из содержания указанного понятия, представленного в примечании к ст. 272 УК РФ. Из данного определения под компьютерной информацией предлагается понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В тоже время, не все следователи, дознаватели, оперативные уполномоченные реализующие противодействие рассматриваемым деяниям, смогут четко разграничить сообщения от данных, понять, что электрический сигнал должен быть представлен в какой-либо форме. Очевидно, что данное определение необходимо уточнить для единственного понимания правоприменителей.

Необходимо сказать, что при составлении описательно-мотивировочной части постановления о привлечении в качестве обвиняемого (ст. 171 УПК РФ) равно как и обвинительного заключения (ст. 220 УПК РФ) обязательно конкретное описание преступления, что не должно допускать возможность расхождений в терминологии, не только в рамках расследования конкретного уголовного дела, но и при формировании однородной следственной и судебной практики.

Изложенное приводит к выводу о необходимости выработки унифицированного подхода к содержанию диспозиций уголовно-правовых норм, регламентирующих преступления в сфере информационных технологий, разработке понятия «компьютерная информация», подлежащего использованию в ходе уголовного судопроизводства.

При квалификации и расследовании преступлений правоприменительная практика вынуждена рассматривать целый ряд терминов, сформулированных в нормативных правовых актах, непосредственно не регулирующих уголовно-процессуальное законодательство.

Так, согласно Федеральному закону от 27 июля 2006 г. № 149 ФЗ (ред. от 30 декабря 2021 г.) «Об информации, информационных технологиях и о защите

информации»<sup>1</sup> под информацией следует понимать сведения (сообщения, данные) независимо от формы их представления, а под информационными технологиями – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Очевидно, что разработка понятий, подлежащих использованию в ходе квалификации и расследования преступлений в обозначенной сфере предполагает необходимость самостоятельного исследования. Вместе с тем, «болевые точки», обусловленные их отсутствием определены достаточно конкретно.

Большая ряд проблем нас встречает правоприменительная практика, которые непосредственно относятся к расследованию преступлений в сфере информационных технологий:

Первое стоит отразить, что получение ответов на запросы отправляемые следственными органами в различные частные кредитные организации, интернет-провайдерам (Ростелеком, Дом.ру и т.п), операторам сотовой связи (МТС, Мегафон, Билайн, Теле2) требуют длительного времени (как минимум двух недель, но может и доходить до пару месяцев).

Также отметим низкое качество ответов, полученных от упомянутых выше организаций, в которых не только не содержится вся запрашиваемая информация, но и зачастую в ней тяжело разобраться без специальных познаний, то есть нет разъяснений в конце предоставляемых документах по каким-либо сокращениям, которые многим следователям не всегда понятны.

При этом необходимо учитывать, что лучший результат при расследование данной категории преступлений приносит своевременный анализ и рассмотрение сведений о об использовании IP-адресов и точек обмена трафиком с целью установления подозреваемого лица, а также движении денежных средств потерпевших, так как в большинстве случаев исходя из

---

<sup>1</sup> Об информации, информационных технологиях и о защите: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г.

практики денежные средства не задерживаются на одном счете, а через дропов переводятся на другие различные счета и электронные кошельки.

На сегодняшний день уже существует практика заключения соглашений о взаимодействии между подразделениями МВД и ПАО Сбербанк предметом которых является взаимодействие по выявлению, пресечению и предупреждению преступлений в отношении клиентов банка, которое позволяет в наиболее короткие сроки получать информацию о движении денежных средств физических лиц, но стоит понимать, что ПАО Сбербанк не единственная организация которая хранением, переводом безналичных денежных средств, и при наиболее грамотной работе преступных лиц изобличить виновное лицо будет затруднительно.

Особенностью, данной категории преступлений является их межрегиональный характер, что требует значительных временных затрат при проведении проверочных мероприятий и выявлении новых эпизодов преступной деятельности.

Показательно, что в большинстве случаев участники преступных групп, выполняющие отдельные функции в своей преступной цепи, необходимые для достижения единой цели могут быть и не знакомы друг с другом, общение зачастую происходит посредством различных мессенджеров (Whatsapp, Telegram, Discord)

Кроме того, доказывание обстоятельств, характеризующих объективную сторону преступления, либо принятие своевременных решений по предотвращению данных деяний, препятствует постоянному усовершенствованию технической базы преступных групп, видоизменение характера противоправных действий как при подготовке, так и при совершении того или иного преступления, разнообразные способы сокрытия следов.

Зачастую используемый мошенниками трафик не блокируется, при выявлении случаев ненадлежащего оказания услуг связи инициатива о приостановлении действия лицензии или ее аннулировании в порядке, предусмотренном законодательством, от операторов сотовой связи не

поступает.

С учетом особенности совершения значительного числа таких преступлений, заключающейся по большей части в исключении непосредственного контакта с потерпевшим в условиях доступности практически любой информации о гражданах, можно отметить постоянный рост числа пострадавших и высокую латентность преступлений.

Необходимо сказать, что при недостаточном государственном регулировании и контроле за так называемой «виртуальной средой», людям предлагаются новые платные услуги и сервисы, которые не проходили лицензирования для их оказания<sup>1</sup>.

---

<sup>1</sup> О лицензировании отдельных видов деятельности: федер. закон Рос. Федерации от 4 мая 2011 г. № 99-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 апреля 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 27 апреля 2011 г.

## ЗАКЛЮЧЕНИЕ

Исходя из вышеизложенного отметим, что на сегодняшний день компьютеризация общества стремительно идет вперед и вместе с этим широко развиваются компьютерные преступления, которые несут вред безопасности государства во все сферы жизнедеятельности общества. Законодательство в данном направлении требует постоянного изменения, в связи с необратимым совершенствованием информационных технологий, необходимо грамотно прорабатывать понятийный аппарат затрагивающий информационную безопасность, учитывать опыт зарубежных стран.

Особенностью компьютерных преступлений является то, что ее криминалистическая характеристика обладает определенной спецификой. Особое внимание необходимо уделять обстановке и способам совершения преступления. Место совершения противоправных деяний часто не совпадает с местом наступления общественно опасных последствий. Информационное пространство быстро развивается вместе с ним и средства совершения преступления, а также объекте преступного посягательства.

Личность подозреваемого характерна тем, что лицо осознает противоправность своих действий и стремится зачастую извлечь для себя выгоду.

Для следовой картина данной категории преступлений характерно использование компьютерно-технических средств как в качестве орудия совершения преступления, так и объекта посягательства, следы могут находиться в разных местах одновременно и имеют широкий спектр, а для фиксации и изъятия возникает надобность привлечения высококвалифицированных специалистов.

Вместе с этим, подозреваемый, совершая преступные деяния, стремится к тому, чтобы преступление не было выявлено и принимает различные приемы и способы сокрытия, что может повлечь при неграмотной работе специалиста и следователя утрате доказательств при работе с электронно-вычислительной

техникой.

Проведение следственных действий, таких как осмотр места происшествия, обыск, допрос подозреваемых, потерпевших свидетелей преступлений, связанных с компьютерной информацией требует больших подготовительных действий и привлечения лиц, обладающих познаниями в области компьютерной информации. Следователь должен внимательно следить за ходом следственных действий, не допускать к компьютерной техники участников следственных действий, с целью предотвращения утраты доказательств. Установить сам или с помощью специалиста имеются ли соединения по различным каналам связи с находящимся на месте обыска или происшествия ЭВМ с другими устройствами, находящимися за пределами обследуемого участка. Также фиксация в протоколах следственных действий о компьютерных устройствах требует внимательности при отражении серийных номеров и другой информации, которая в дальнейшем позволит их идентифицировать.

Назначение и производство судебных компьютерно-технических экспертиз является трудоемким процессом. Экспертиза в компьютерной области затрагивает научные направления: информационные системы и процессы, автоматизация, электроника, электротехника, вычислительная техника, программирование и др. Проблемы могут возникнуть на начальном этапе, правильность выбора экспертного учреждения и виды назначаемой экспертизы, подготовка объектов и материалов дела которые будут направляться в экспертное учреждение. Имеет место быть и проблема постановки вопросов эксперту, это обусловлено тем, что следователю необходимо широко владеть терминологией в сфере компьютерной информации. В связи с этим на практике зачастую прибегают к помощи специалиста в формулировке вопросов.



## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

### **I. Нормативные правовые акты и иные официальные документы**

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с учетом поправок, внесенных Законом Рос. Федерации о поправках к Конституции Рос. Федерации от 21 июля 2014 г. № 11-ФКЗ // Собр. законодательства Рос. Федерации. – 2014. – № 31, ст. 4398.

2. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 53-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г.

3. Уголовно-процессуальный кодекс Российской Федерации федер. закон Рос. Федерации от 18 декабря 2001 г. № 74-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 ноября 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 декабря 2001 г.

3. Об информации, информационных технологиях и о защите: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г.

4. О банках и банковской деятельности: федер. закон Рос. Федерации от 2 декабря 1990 г. № 395-1-ФЗ.

5. О лицензировании отдельных видов деятельности: федер. закон Рос. Федерации от 4 мая 2011 г. № 99-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 апреля 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 27 апреля 2011 г.

### **Учебная, научная литература и иные материалы**

1. Антонов В. В., Харисова З. И., Мансурова З. Р., Родионова Л. Е., Калимуллин Н. Р., Куликов Г. Г. Системная модель интеллектуальной

предметно-ориентированной профайлинг-системы // Онтология проектирования. 2020. Т. 10. № 3. С. 338–350.

2. Бекряшев А. К., Белозеров И. П., Бекряшева Н.С. Теневая экономика и экономическая преступность. Омск: Омский гос. университет, 2000. 459 с.
3. Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации: науч.-практ. пособие. Изд. 2-е, доп. и испр. М.: ЛексЭст, 2004. 254 с.
4. Дулов А. В. Вопросы теории судебной экспертизы. Минск: изд-во Белгосуниверситета им. В. И. Ленина. 1959. 187 с.
5. Зуева С. В. Основы теории электронных доказательств: монография / М.: Юрлитинформ, 2019. 400 с.
6. А.А. Кузнецова Методика расследования налоговых преступлений : учеб. пособие / под общ. ред. проф.. М.: 2007. 147 с.
7. Колычева А. Н. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие. М.: Проспект, 2020. 199 с.
8. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / В. К. Дуюнов и др.; Отв. ред. Л. Л. Кругликов. М.: Волтерс Клувер, 2005. 547 с.
9. Леонтьев Б. К. Хакеры, взломщики и другие информационные убийцы 2-е изд. Москва: Майор, 2001. 190 с.
10. Лопушной Е. Я. Участие специалиста-криминалиста в следственных действиях: Автореф. дисс. ... канд. юрид.наук. Алма-Ата, 1971. 60 с.
11. Махов В. Н. Участие специалиста в следственных действиях: Автореф. дисс. ... канд. юрид. Наук. М., 1971. 32 с.
12. Менжега М. М. Методика расследования создания и использования вредоносных программ для ЭВМ. М.: Юрлитинформ, 2010. 168 с.
13. Мусиенко А. В. Принципы привлечения специалистов к

производству следственных действий // Проблемы предварительного следствия: Сб. науч. Раб. Волгоград, 1978. Вып. 7. С. 96-97.

14. Низаева С. Р. Личность потерпевшего как элемент криминалистической характеристики мошенничества в сфере оборота жилой недвижимости // Правовое государство : теория и практика. 2017. № 3 (49) С. 141–143.

15. Осипенко А. Л. Сетевая компьютерная преступность. Теория и практика борьбы. Монография. Омск: Омская академия МВД России, 2009. 479 с.

16. Расследование преступлений следователями и дознавателями органов внутренних дел: учеб. пособие. М.: Проспект, 2021. 545 с.

17. Россинская Е. Р. Криминалистика : учебник / Е. Р. Россинская. Москва: Норма : ИНФРА-М, 2021. 464 с.

18. Румянцева А. А. Причины роста числа преступлений в интернете, Москва. 2021. URL: <https://ru.rt.com/j3yg> (дата обращения: 16.03.2022).

19. Себякин А. Г. Современные возможности использования специальных знаний в области компьютерной техники при расследовании преступлений, связанных с доведением до самоубийства несовершеннолетних // Вестник Тюменского института повышения квалификации МВД России. – 2018. – № 1 (10). – С. 69–76.

20. Сорокотягин И. Н. Криминалистические проблемы использования специальных познаний в расследовании преступлений : автореф. дис. ... д-ра юрид. наук. Екатеринбург, 1992. 45 с.

21. Состояние преступности в России за 2020-2021 года, Москва. 2022. URL: [мвд.рф/reports/item/28021552/](http://мвд.рф/reports/item/28021552/) (дата обращения: 17.04.2022).

22. Сысенко А. Р. Особенности осмотра места происшествия при расследовании компьютерных преступлений // Закон и право. 2020. № 12. С. 216 – 218.

23. Шиканов В. И. Проблемы использования специальных знаний и научно-технических новшеств в уголовном судопроизводстве : автореф. дис. ...

д-ра юрид. наук. М., 1980. 158 с.

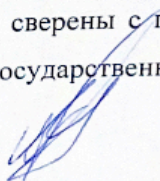
24. Эйсман А. А. Заключение эксперта. Структура и научное обоснование. М., 1967. 152 с.

## II. Эмпирические материалы

1. Приговор Калининского районного суда г. Уфы Республики Башкортостан от 14 ноября 2017 г. по делу № 1-499/2017 [Электронный ресурс]: URL: <https://sud-praktika.ru>.

2. Приговор Орджоникидзевский районный суд г. Екатеринбурга Свердловской области от 25 июля 2017 по делу № 1-405/2017 года [Электронный ресурс]: URL: <https://sud-praktika.ru>.

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну.

  
И.А. Мамаев