МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)
Кафедра «Уголовное право и процесс»
(наименование кафедры)
40.05.02 Правоохранительная деятельность
(код и наименование направления подготовки, специальности)
Оперативно-розыскная деятельность
(направленность (профиль)/специализация)

ДИПЛОМНАЯ РАБОТА

на тему: Методика расследования преступлений в сфере компьютерной информации

Студент Е.Г. Рыжков _____
(И.О. Фамилия) (личная подпись)

Руководитель С.В. Юношев _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий кафедрой «Уголовное право и процесс»
к.ю.н., доцент С.В. Юношев _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____»_____2019 г.

Тольятти 2019

Аннотация

Тема дипломной работы: «Методика расследования преступлений в сфере компьютерной информации».

В результате компьютеризации нашего общества мы столкнулись с одной из главных проблем информационного общества – увеличение удельного веса в общем количестве преступлений именно преступлений в сфере компьютерной информации.

Существует мнение, согласно которому именно преступления в сфере компьютерной информации, совершаемые особенно в Интернете, станут катализатором большей части преступности повсеместно.

Все вышесказанное определяет важность, актуальность, теоретическую и практическую значимость избранной мной темы.

Цель выпускной дипломной работы заключается в том, чтобы изучить особенности методики расследования преступлений в сфере компьютерной информации.

Для достижения поставленной цели необходимо решить следующие задачи:

- анализ криминалистической характеристики субъекта и субъективной стороны преступлений в сфере компьютерной информации;

- изучение предмета посягательства при совершении компьютерных преступлений;

- анализ объекта и объективной стороны преступлений;

- изучение особенности выявления личности преступника;

- анализ обстоятельств, подлежащих установлению и доказыванию;

- рассмотрение особенности производства отдельных следственных действий.

Данная дипломная работа состоит из трех глав, структура обусловлена целью и задачами исследования. Общий объем работы 70 листов.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В результате компьютеризации нашего общества мы столкнулись с одной из главных проблем информационного общества – увеличение удельного веса в общем количестве преступлений именно преступлений в сфере компьютерной информации.

Все учреждения и организации, да и все члены общества почти без исключений применяют в своей деятельности компьютерные сети и системы учета, обработки и управления данными через данные электронные системы, именно от уровня сохранности и защиты этих процессов зависит безопасность государства в целом, а также нормальная жизнедеятельность людей в частности.

Все индивидуальные локальные сети объединены в систему общемировой глобальной сети с помощью существующих на данный момент цифровых телекоммуникационных технологий.

Во всех стратегически важных сферах хозяйства и, самое главное, в сфере обороны страны, используются системы автоматизации управления, контроля (мониторинга), а также прогнозирования, охраны и защиты объектов с помощью устройств, основанных на разнообразных микропроцессорных устройствах (интегральных микросхемах).

Доступность средств ЭВМ и широкая возможность любого гражданина в сфере ЭВМ и электросвязи, а также отсутствие привязки в личности большей части, содержащейся в них компьютерной информации, приводит к повышенной заинтересованности к этой сфере криминальных элементов и структур.

В настоящее время статистические данные говорят о небольшом проценте преступлений, совершенных в сфере компьютерной информации, можно говорить про долю в проценте все зарегистрированных преступлений на территории Российской Федерации, но темпы роста данного количества в

удельном весе дает основания полагать, что данные преступления только начинают набирать свои обороты.

Существует мнение, согласно которому именно преступления в сфере компьютерной информации, совершаемые особенно в Интернете, станут катализатором большей части преступности повсеместно. Именно в сети Интернет компьютерная преступность набирает свои обороты.

Именно развитие компьютерных технологий и просвещения в сфере IT способствуют появлению новых вариантов и способов совершения преступлений против собственности, а также иных преступлений, к примеру, нарушение авторских прав, государственной измены и далее.

Также одной из особенностей и доказательств общественной опасности компьютерных преступлений является свобода совершения преступлений не взирая на государственные границы.

Положение усугубляет плохо разработанная структура теоретической нормативной базы в сфере компьютерных преступлений, данные составы преступлений появились в законодательстве только с момента вступления в силу действующего Уголовного кодекса РФ, то есть с 1 января 1997.

Наличие особенностей технического характера не делают данные виды преступлений проще для расследования и дальнейшего предотвращения. Сотрудники правоохранительных органов не имеют необходимый уровень специальных знаний в сфере IT.

Все вышеназванные моменты приводят нас к выводу о сложности в проведении расследований, а в дальнейшем во время судебного процесса, так как технические сложности, недостаточная компетентность могут привести к нарушению принципов справедливости и законности судопроизводства.

Преступность в сфере компьютерной информации это явление свойственное не только развитым и компьютеризованным на высшем уровне странам, но и странам, в которых слабая компьютеризация и производственные и общественные отношения не имеют глубокого внедрения технологий в сфере IT.

Высокая практическая значимость исследований в сфере преступлений, направленных против защиты компьютерной информации и иных преступлений в данной области, многие аспекты данной области остаются нерешенными, а также вызывают много споров, возможно возникающих по причине различия в терминологии.

Главной проблемой, возникающей при исследовании преступлений в сфере компьютерной информации, является условие наличия определенных знаний в области IT.

Преступления в сфере компьютерной информации требуют внимания и активного изучения криминологами, так как прогресс в сфере ЭВМ неотделим от прогресса в сфере данных преступлений.

Если проанализировать следственную практику, то мы увидим много пробелов и проблем в данной сфере, так как до сих пор имеет место большая разобщенность в действиях следственных органов по обмену и проверке информации по обстоятельствам, подлежащим установлению и проверке.

Можно смело сказать, что возможности экспертно-криминалистических подразделений и помощь специалистов для обнаружения, фиксации, исследования и изъятия специфических вещественных доказательств не используется в полной мере.

Но главной проблемой была и остается слабая профессиональная подготовка специалистов, направленных на расследования данных преступлений.

Отсутствует должное обучение сотрудников правоохранительных органов в сфере информационных технологий, специальных программ ЭВМ, защиты от вредоносных вирусов, современных компьютерных программ, а также баз данных компьютерной информации.

Дополнительно помимо первоначального специального обучения данные специалисты должны обучаться и проходить переподготовку регулярно, так как преступники быстро совершенствуют свои навыки и технические возможности.

Необходимо непрерывное развитие навыков и знаний, чтобы соответствовать профессиональной подготовки компьютерных преступников.

Все вышесказанное определяет важность, актуальность, теоретическую и практическую значимость избранной мной темы.

Цель выпускной дипломной работы заключается в том, чтобы изучить особенности методики расследования преступлений в сфере компьютерной информации.

Для достижения поставленной цели необходимо решить следующие задачи:

- анализ криминалистической характеристики субъекта и субъективной стороны преступлений в сфере компьютерной информации;

- изучение предмета посягательства при совершении компьютерных преступлений, а также изучение различных подходов к определению предмета компьютерных преступлений;

- анализ объекта и объективной стороны преступлений в сфере компьютерной информации;

- изучение особенности выявления личности преступника в сфере компьютерных преступлений;

- анализ обстоятельств, подлежащих установлению и доказыванию в процессе расследования преступлений в сфере компьютерной информации;

- рассмотрение особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации.

Объектом исследования настоящей выпускной квалификационной работы является деятельность правоохранительных органов по расследованию преступлений в сфере компьютерной информации.

Предметом исследования являются криминалистическая характеристика данного состава преступления и производство отдельных следственных действий.

Методика расследования – это система научных положений, технических средств, тактических приемов, методических правил и рекомендаций, применяемых при раскрытии, расследовании и предупреждении преступлений.

Предметом исследования в данной выпускной дипломной работе являются специальная литература, материалы судебно-следственной практики, статистические данные, отечественный и зарубежный опыт в сфере расследования и предупреждения преступлений в сфере компьютерной информации.

Глава 1. Основные элементы криминалистической характеристики субъективной стороны преступлений в сфере компьютерной информации

1.1 Типологические данные о субъектах преступлений.

Существует мнение, что зарождение преступлений в компьютерной сфере неразрывно связано с таким явлением, как «хакеры» (в переводе с английского слова «hacker».

Хакеры можно характеризовать как пользователей электронно-вычислительных машин, систем ЭВМ, сети таких ЭВМ, деятельность которых заключается в несанкционированном доступе к охраняемой законом компьютерной информации[1].

Хакеры обладают высочайшими знаниями и навыками в области компьютерной техники, электронного документооборота (ЭДО), криптографии и т.д. Эти знания постоянно увеличиваются, уточняются, что в большей степени затрудняет работу по расследованию данных преступлений.

Именно хакеров можно назвать, в широком смысле, компьютерным правонарушителем, а в каких-то моментах и компьютерным преступником.

Статистика подтверждает, что большой процент молодых специалистов в области компьютерных технологий оттачивают свои навыки в этом виде деятельности, так она дает свободу действиям и подогревает их интерес именно тем, что данная деятельность запрещена.

Именно вызов, который бросает государство перед хакерами вызывает еще большее желание доказать, что их знаний хватит, что бы нарушить и преодолеть преграды, состоящие из систем защиты государства и отдельных организаций, а также защиты компьютерной информации отдельных граждан.

Так называемые хакеры объединяются в группы, издаются в печатных СМИ, и конечно имеют свои сайты и порталы в глобальной сети Интернет.

---

[1] Коржов В.К. Право и Интернет: теория и практика [Текст] : учебное пособие / В. К. Коржов. – М.: Издательство БЕК, 2006. – 236 с.

Именно сеть Интернет является основной связующей площадкой для всех представителей преступного мира в сфере компьютерных технологий и компьютерной информации, существует много запрещенных сайтов, на которых представители хакерского мира могут не только делиться знаниями, но также вербовать друг друга для выполнения отдельных преступных действий, а также рекламировать свои услуги преступного характера.

Существуют электронные ресурсы, где можно найти исполнителя для своих преступных намерений, что создает благоприятную среду для развития преступлений в данной сфере, так как свободный вариант взаимодействия с представителями преступного мира не может способствовать предупреждению компьютерных преступлений, а только усугубляет и так сложную ситуацию.

Также для обмена опытом между специалистами в этой сфере участвуют в форумах, а также размещают свои объявления для дальнейшего оказания услуг по своему профилю.

Все это способствует вовлечению представителей молодежи в эту противоправную деятельность, а также является так называемой профпереподготовкой и повышением квалификации начинающих и уже опытных правонарушителей в этой сфере.

Именно в этой электронной среде правонарушители, а также будущие правонарушители, делятся между собой методиками, способами и средствами совершения и сокрытия преступлений в сфере IT.

Также нельзя не обратить внимание на взаимодействие российских преступников в сфере компьютерной информации со своими зарубежными коллегами, а также на их обмен опытом.

Объект криминологического исследования в данных преступлениях это, конечно, личность самого преступника, именно данные о его типологии являются неотъемлемой частью криминологической характеристики преступлений.

Изучение криминологами особенностей личности преступников в этой сфере не заходит дальше изучения тех особенных черт, которые нужны

правоохранительным органам для профилактики аналогичных преступлений, а также дальнейшего предупреждения преступлений в этой сфере. Ввиду этого ограниченного изучения, многие важные для определения преступника и его поимки черты остаются за рамками характеристики криминологов, что не способствует раскрытию преступлений.

Самый большой пробел – это оставление без внимания особых навыков преступников, которые говорят нам об определенных способах совершения этих преступлений, которые в свою очередь формируют так называемый почерк преступника. Именно этот почерк и личностные особенности совершения и сокрытия преступлений и содержит большую часть «следов личности», совершившего преступление в сфере IT[2].

Любые вещественные улики, которые могут быть найдены на месте совершения преступления, могут помочь следствию определить многие свойства и характеристики личности предполагаемого преступника, они могут указывать на профессиональный опыт в совершении преступлений, наличие специальных знаний, также пол и возраст, а главное особенности взаимоотношений преступника с потерпевшим.

Именно изучение всех следов и вещественных улик, а далее выявление особенностей личности преступника, которые имеют место в собранной информации о событиях совершения преступления, дают возможность составить портрет преступника, в общих, или даже в частных чертах его личности.

Информацию, имеющую значение для криминалистов, можно классифицировать по нескольким основаниям[3].

Если анализировать всю информацию о личности предполагаемого преступника, то она подразделяется на две разные по содержанию группы:

---

[2] Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. - М.: Норма, 2008. С. 7

[3] Крылов В.В. Информационные компьютерные преступления [Текст] : учебное пособие / В. В. Крылов. – М.: Юрид. Лит., 2005. – 240 с.

1. Первая группа – информация, полученная на этапах проверки места преступления, по следам, найденным на нем, а также информация, полученная от опрашиваемых свидетелях совершенного преступления, если такие имеют место быть. Данная информация является очень важной на первых этапах розыскных действий, так как именно с помощью нее можно надеяться на продуктивный розыск, который приведет к задержанию совершившего компьютерное преступление лица[4].

Очень часто вышеуказанная информация может дать наводку на понимание и определение группы лиц, чьим участником является потенциальный преступник, реже информацию, которая может охарактеризовать конкретного человека как личность и описать его особенные личностные качества.

Информация данной группы имеет огромное значение для сравнительного анализа и подведения статистического вывода, о том, кто же чаще всего становится преступником в сфере компьютерных преступлений. Также можно сделать вывод, что данная информация может послужить материалом для анализа и в дальнейшем основанием для предупреждения данных преступлений.

2. Следующая группа информации – это та, что сотрудники правоохранительных органов получают во врем допросов подозреваемого лица, либо от обвиняемого, в зависимости в каком статусе на момент проведения допроса данное лицо находится согласно нормам уголовно-процессуального права.

Если информация из первой группы может дать нам общее представление о возможном преступнике, то именно информация из второй группы делает типизация и классификация компьютерных преступников реальной и доступной, а также понять возможный способ профилактики данных преступлений в рамках уже конкретного подозреваемого/ обвиняемого.

[4] Гаджиев М. С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): Автореферат дисс. канд. юрид. наук. - Махачкала, 2009. - С. 9

Информация из второй группы делает возможным достижение контакта между подозреваемым/обвиняемым и сотрудником правоохранительных органов, который в свою очередь обеспечивает правдивый допрос и доказывание виновности подозреваемого.

Выше было сказано о возможности типизации (классификации) преступников в сфере компьютерных преступлений, что необходимо для создания так называемых «типовых моделей преступников»[5]. Именно знания отдельных черт преступников и особенностей преступных групп сделать процесс выявления круга лиц доступным и упрощенным. Данный круг лиц ссужает рамки поиска конкретного преступника или даже позволяет установить сразу конкретное лицо, виновное в совершении преступления.

Если анализировать случаи совершения данных преступлений ни отдельным взятым преступником, а группой лиц, то есть преступных сообществом, то предметом изучения становится информация, которая будет описывать именно эту группу. Для групп лиц одним из главных элементов изучения является ее структура, т.е. организация и порядок взаимодействия разных участников данного преступного сообщества. Но даже в данном случае изучаются участники группы как личности, их особенности, а также функционал в данном сообществе, так как преступное сообщество имеет свою иерархию и свои правила взаимодействия между ее участниками[6].

Анализ особенностей группы/сообщества позволяет в большей степени определить курс розыскным мер для определения и дальнейшего установления всех участников преступного сообщества, а также основных преступных эпизодов этой деятельности.

Так называемых «компьютерных преступников» можно поделить, по мнению криминалистов, с точки зрения характеристики личности, на несколько групп.

---

[5] Ермолович В. Ф. Научные основы криминалистической характеристики преступлений. - Минск: ЗАО "Веды», 2009. - С. 273

[6] Информатизация и информационная безопасность правоохранительных органов. М.: Академия управления МВД России, 2005. - С. 94

1. Профессиональные преступники в сфере IT. Именно у представителей этой группы присутствует фанатизм в противоправных деяниях. Именно с помощью совершения данных преступлений лица из числа данной группы чувствуют профессиональную пригодность и чувство личного самоудовлетворения.

Именно этот так называемый «вызов» является фактором, который мотивирует и побуждает человека на действия, которые имеют преступную подоплеку.

Именно представителями этой группы изобретаются и продумываются новые и изощренные способы несанкционированного проникновения в ЭВМ, системы безопасности и т.д.

Действия данных преступников происходят одновременно с одолением средств защиты данных, которые в свою очередь регулярно совершенствуются.

Постоянное совершенствование защиты приводит к постоянному совершенствованию преступников, что является причиной для улучшения алгоритма преступных действий и процессов[7].

Все это приводит к совершенствованию способов совершения и сокрытия преступлений в сфере компьютерной информации.

Главной особенность представителей этой группы преступников является определенного и обоснованного противоправного намерения, то есть все преступления и правонарушения совершаются только с целью доказать свой профессиональный уровень, проявить свои умения и навыки, самоутвердиться в глазах других.

Большое внимание криминалисты уделяют преступникам, которые являются специалистами-профессионалами в сфере компьютерной техники. Данные преступники наделены незаурядными интеллектуальными данными и не лишены азарта.

Любое улучшение безопасности компьютерных систем и защиты данных в сети Интернет расцениваются данными преступниками как вызов именно их

[7] Анин Б. Защита компьютерной информации. - СПб.: БХВ-Санкт-Петербург, 2009.С. 7.

личности, их навыков и знаний, поэтому они ищут все способы, в том числе преступные, чтобы доказать свое превосходство над общей системой. Это является катализатором преступных действий.

Все вышеуказанное приводит к трансформации начинающих неопытных любителей в настоящих профессиональных хакеров.

Обязательно стоит отметить тот факт, что данные преступники не имеют необходимой подготовки к совершаемому преступлению, способ совершения отличается оригинальностью и новизной свершения, а также отсутствуют меры для сокрытия совершаемого преступления[8].

2. Вторая группа преступников - это лица, страдающие новым видом психических заболеваний - информационными болезнями или компьютерными фобиями.

Это плохо изученный аспект данного вопроса, поэтому на нем необходимо остановится подробнее.

Главными причинами в литературе называют систематические нарушения информационного режима индивидуума. Составляющих такого нарушения много, к ним можно отнести и «информационный голод», и «информационный перегруз», также незапланированные срочные и частые переключения с одного процесса на другой в информационной сфере, а также так называемый «информационный шум». Именно анализом этого заболевания, изучением причин появления и способов лечения занимается новая отрасль – информационная медицина[9].

Современный мир диктует свои правила, все наши рабочие места, практически уже без исключения, оборудованы персональными компьютерами (ПК), для автоматизации всех рабочих процессов, для увеличения эффективности каждой манипуляции, в связи с чем многие работники испытывают на себе большое информационное давление и попадают в особо

[8] Панфилова, Е.И. Компьютерные преступления [Текст] : учебное пособие / Е.И. Панфилова. – М. : Феникс, 2007. – 254 с.

[9] Сальников, В.П. Компьютерная преступность [Текст] : учебное пособие / В.П. Сальников. – М. : Приор, 2004. – 192 с.

стрессовые ситуации, что в итоге может послужить причиной для компьютерных фобий, то есть ПК является источником и причиной для профессионального заболевания.

Необходимо указать, что вышеуказанные лица, страдающие данным заболеванием, могут совершать в силу своей неуравновешенной психики или временного затруднения с сознанием компьютерные преступления.

В случае если при проведении следственных действий подтверждается данный факт или есть основания полагать, что лицо страдает данным заболеванием, необходимо в обязательном порядке назначать и проводить судебную психиатрическую экспертизу для дальнейшего определения квалификации деяния конкретного преступника (преступление, совершенное в состоянии аффекта или лицом, страдающим психическим заболеванием и т.д.).

Преступления, которые совершают вышеуказанные лица совершаются в основном при частичной или полной потере контроля над своими действиями.

3. Профессиональные преступники в сфере компьютерной информации, имеющие корыстные цели («профи»). Имеют существенные отличия не только от второй группы, но и от первой так называемой «переходной» группы. Данные отличия лежат в основном в многократно совершенных преступлениях в сфере компьютерной информации, с обязательным условием скрыть совершенное преступление и «замести следы» после своего преступления. Профи обладают высоким уровнем преступных навыков.

Профессиональные компьютерные преступники в основном работают в составе преступных групп, имеющих достаточно высокотехнологическое оснащение специальным оборудованием и техникой. Именно эти группы, в которых есть не только профессиональные преступники программисты, но и юристы и экономисты, и являются главной угрозой безопасности в сфере компьютерной информации.

Именно рост преступлений совершенных преступными группами и показывает статистика в последние годы[10].

Особенностью представителей этой группы преступников является статус наемного сотрудника, причем в большей своей части это представители руководящего состава, обладающего необходимым уровнем доступа к информации, а также средствам ЭВМ. Именно данный статус и особый доступ к защищаемой компьютерной информацией выделяет данных представителей, другими словами, это преступники не имеющие каких либо отклонений, но имеющих реальную возможность на осуществления такого рода преступлений.

В случае рассмотрения специальностей или профессиональной ориентации вышеуказанных представителей мы видим обширный список наемных работников от операторов АЗС до сотрудников банка.

Данные специалисты также имеют свою классификацию, на этот раз данное разделение основано исключительно на категории допуска к ЭВМ, и как следствии к компьютерной информации: внешние и внутренние пользователи.

Необходимо дать определение внешнему пользователю – это лицо, которое для получения информации обращается либо к посреднику, либо к ЭВМ[11].

Также существует классификация, основанная на правовом статусе пользователей, т.е. зарегистрированные на законной основе либо незарегистрированные должным образом.

Статистика, которая может дать описание количественного соотношения между разными видами пользователей, говорит нам, что почти 95 процентов из всех совершенных компьютерных преступлений совершены именно внутренними пользователями, из чего мы видим, что совершение внешними пользователями ничтожно мало.

---

[10] Спирина С.Г. Криминологическая характеристика компьютерной преступности в России. - Краснодар: Российский государственный торгово-экономический университет, 2009. - С. 28.

[11] Гульбин, Ю.А. Преступления в сфере компьютерной информации [Текст] : учебное пособие / Ю.А. Гульбин. – М.: «Статут» 2007. – 321 с.

Вышеназванных преступников подразделяют (условно) на несколько групп, в зависимости от их категории доступа к ЭВМ, а также к компьютерной информации.

1. Совершают преступления с помощью использования специальных программных средств, это могут быть такие специалисты как: программист, специалист по IT, системный администратор, кассир, бухгалтер-расчетчик, оператор АЗС и т.д

2. Совершают преступления с помощью аппаратных средств: оператор средств связи, связист и тд.

3. Совершают преступления с помощью косвенного доступа к к ЭВМ, а также к компьютерной информации, в основном это лица, которые занимаются управленческими или организационными вопросами.

На характеристике преступников из числа внешних пользователей ни стоит останавливаться так подробно, так как это не даст какую-то значимую информацию для дальнейшего анализа порядка и методики расследования преступлений в сфере компьютерных преступлений, а также данная информация не будет столь полезна для дальнейшей работы по предотвращению аналогичных преступлений.

Преступником из числа внешних пользователей может быть любое лицо.

1.2 Сведения об обстановке и типичных мотивах их совершения.

Событие преступления протекает в определенной обстановке, которую принято рассматривать в широком и узком смысле слова.

На основании этого необходимо рассмотреть оба варианта определения данного понятия в уголовном праве и процессе.

Можно сделать вывод, что в широком смысле слова под обстановкой понимается та современность, которая основана на определенном этапе развития общества и влияющая на динамику преступности в которой каждое

конкретное преступление было совершено, данная обстановка всегда, то есть непрерывно меняется и совершенствуется.

Если говорить об этой величине в узком смысле слова понимается определенная группа факторов, позволяющие судить об особенностях влияния этой системы на содержание преступного события[12].

В отличие от широкого смысла слова, данная интерпретация подразумевает уже конкретные условия, влияющие как на субъект, так и на объект преступления, так как они находятся в динамично меняющейся ситуации.

Необходимо указать на большое значение обстановки конкретного преступления, подлежащего расследованию, так как это одно из составляющих криминалистической характеристики любого преступления.

Именно подробно изучив обстановки можно сделать много предположений и выводов относительно всего преступления в целом и его составных частей в частности.

В зависимости от различной ситуации в обществе как потерпевшим так и преступником могут стать различные лица, поэтому так важно на первом этапе расследования преступлений данного типа изучить обстановку конкретно совершенного преступного деяния.

При изучении обстановки конкретного расследуемого преступления можно выявить некоторые черты личности предполагаемого преступника, а также способ совершения данного преступления.

Также анализ особенностей обстановки каждого конкретного преступления позволяет выявить обстоятельства, которые способствовали или вообще сделали возможным совершение данного преступления в сфере компьютерной информации.

Необходимо добавить, что именно данное изучение обстоятельств и обстановки преступления делает розыскные мероприятия более эффективными,

[12] Криминология: Учебник/ Под ред. В. н. Кудрявцева и В. Е. Эминова. - М., Юристъ, 2008. С. 305

приводящими к задержанию преступников, то есть является залогом раскрытия преступлений данного вида.

Говоря о субъективной стороне любого преступления, в том числе и преступления против компьютерной информации, нельзя не упомянуть о так моментах, составляющих субъективной стороны, как вина, мотив и даже цель самого преступного поведения.

Только проанализировав, данные составляющие сотрудники правоохранительных органов, криминологи могут составить для себя целостную картину происходящего в психике отдельно взятого преступника.

Криминалистическая характеристика преступлений субъективной стороны преступлений в сфере компьютерной информации кроме личности преступника подразумевает под собой также понятие мотива и цели преступления.

Не имея цели, лицо не имеет мотива и как следствия желания и необходимости в совершении деликтивного поступка – преступления. Так как именно наличие мотива может побудить индивидуума на совершение преступления.

Необходимо указать классификацию мотивов (целей) преступлений в данной сфере. Для представителей разных групп преступников, о которых выше уже шла речь, данные мотивы различны, во главе их поступков, а именно преступлений, стоят разные цели.

Именно эти различные мотивы (корысть, месть, доказывание своих профессиональных и преступных навыков и т.д) в первую очередь влияют на способ совершения конкретно взятого преступления, а главное на выбор объекта как потерпевшего[13].

Нельзя не отметить, что именно мотив преступника главным образом также определяет, не только способ совершения, но и те средства с помощью

[13] Крылов В.В. Информационные компьютерные преступления [Текст] : учебное пособие / В. В. Крылов. – М.: Юрид. Лит., 2005. – 240 с.

которых совершается преступное деяние, а также конкретные действия конкретного преступника, которые характеризуют его.

Мотив не является обязательной частью состава преступления, но имеет важнейшую роль в расследовании всех преступлений, в том числе преступлений в сфере компьютерной информации и требует установление цели конкретного преступника.

Именно после получения сведений о мотивах или после выявления предположительного мотива преступления правоохранительные органы могут выдвигать версии о предполагаемом преступнике. Данные версии позволяют в свою очередь проводить целенаправленные поиски возможного преступника.

Если анализировать возможные мотивы для совершения рассматриваемых преступлений, то можно распознать следующие: совершение с корыстной целью, преследующие политические цели, месть, хулиганские соображения, а также преследующие только профессиональный (исследовательский) интерес.

Если проанализировать данные мотивы, то можно сделать вывод, что преступления, имеющие политическую подоплеку или имеющие своей целью материальное обогащение выделяются среди других аналогичных компьютерных преступлений особой изощренностью в совершении, а также в сокрытии данного преступления.

Непрофессиональные преступники (любители, не хакеры) очень часто преступают закон не специально, то есть, не ставя перед собой цель, нарушить его, потому что рассматривают компьютер как предмет для игры и анализа своих способностей.

Для них это способ познания предмета исследования, проверки своих знаний и сил в этой профессиональной сфере. Это преступники являются в большей части изобретателями и первопроходцами в новых способах совершения и сокрытия преступлений в сфере компьютерной информации. Именно их способы и новые идеи в дальнейшем используются другими, часто профессиональными, преступниками.

Если говорить о преступниках, которые относятся к группе «страдающих информационными заболеваниями», то их цель свершения преступлений специфическая – уничтожение средств ЭВМ, полное либо частичное, затрагивающее именно материальную оболочку, то есть носитель компьютерной информации, являющееся для них неким условным раздражителем для психики.

В большинстве случаев, данные преступления совершаются преступниками в состоянии аффекта либо невменяемости.

Понятие «обстановка совершения компьютерного преступления» содержит в себе все факторы среды (производственные, социальные, материальные), в которой данное преступление совершается.

Любой из вышеназванных факторов может влиять на способ и условия совершения преступления, определять уровень доступа к компьютерной информации, возможности как таковой совершить данное преступление.

Нестандартные (уникальные для каждого случая) условия деятельности потерпевшего, которым может быть и юридические, и физические лица, подразделяются в криминалистике на два типа:

- объективные:

вид и род занятия, форма собственности потерпевшего, положение в правовом поле, степень доступности информации, система учета и отчетности, обеспечение материальными и кадровыми ресурсами и тд.;

- субъективные:

отступление от порядка обработки информации, эксплуатации программ и самих ЭВМ, нарушение в сфере учета и хранения информации, отсутствие средств защиты для нее, наличие ручных этапов обработки документов наравне с автоматизированными, отсутствие контроля со стороны ответственных лиц потерпевшего, либо самого потерпевшего, а также психологически неправильные межличностные взаимоотношения должностных лиц с подчиненными и другими работниками и т. д.

Вышеперечисленные моменты в значительной мере влияют на обстановку совершения конкретных преступлений связанных с нарушением сохранности компьютерной информации, например, на выбор потерпевшего лица (жертвы преступления компьютерного преступника), способов выполнения, на привлечение соучастников или помощников в отдельных моментах в процессе подготовки или сокрытия преступного деяния, способов заметания следов, а также на условие совершения действий противоправного характера в отношении чего-то кроме компьютерной информации (к примеру, хищение денежных средств).

Именно они определяют наличие возможности и возможные варианты совершения любого преступления в сфере компьютерной информации в каждом конкретном случае, поэтому так важно в процессе расследования преступления анализировать и изучать все аспекты обстановки совершения противоправного действия направленного против безопасности и сохранности компьютерной информации и машинных носителей для данного вида информации.

Глава 2. Криминалистическая характеристика объективной стороны преступлений в сфере компьютерной информации.

2.1 Предмет и объект посягательства при совершении компьютерных преступлений.

Уголовно-правовая квалификация преступления состоит в установлении совпадения типичных обстоятельств конкретного общественно-опасного, противоправного деяния признакам определенного в УК РФ состава преступления[14].

Одной из главных составляющих состава преступления – объект и предмет преступного посягательства в конкретном преступлении.

Далее только можно переходить к изучению и анализу признаком преступного деяния, то есть объективной стороны преступления.

Данный порядок дает основания для уверенности в установлении тождества между совершенным преступным деянием и составом преступления, указанном в нормах УК РФ, также отделить преступления от иных смежных преступлений, с похожими составами.

Для дальнейшего изучения объективной стороны преступления необходимо проанализировать признаки неправомерного доступа к компьютерной информации по отдельным элементам его состава.

Неправомерный доступ к охраняемой законом компьютерной информации в 9 разделе УК РФ (особенная часть), так как родовым признаком данного преступления является совокупность общественных отношений, составляющих содержание общественной безопасности и общественного порядка.

Видовой объект преступного посягательства – критерий, по которому компьютерные преступления могут быть собраны в одной главе УК РФ -

[14] Куринов Б.А. Научные основы квалификации преступлений. М.: МГУ, 2004. С.55.

совокупность общественных отношений в части правомерного и безопасного использования компьютерной информации и информационных ресурсов.

Согласно анализа состава преступления объектом данного вида преступления будет, если дословно трактовать норму закона, общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети.

Факультативный, то есть не обязательный, дополнительный объект при неправомерном доступе к ЭВМ, как следствие к компьютерной информации может иметь место в данной квалификации в зависимости от того вреда который нанесло само преступление.

Факт наличия факультативного объекта повышает степень общественной опасности данного преступления, что необходимо учитывать при назначении наказания виновному лицу[15].

Объект преступления, является обязательным элементом любого преступления, при его отсутствие при анализе преступления необходимо констатировать, что отсутствует и состав преступления, и лицо, не причинившее вреда и создавшее угрозы причинения этого вреда, не будет привлечено к уголовной ответственности.

Предмет преступления заключенного в неправомерном доступе к компьютерной информации является показателем при отделении компьютерных преступлений от всех остальных преступлений, указанных в особенной части УК РФ.

Существует мнение ученых, что предметом в данном случае будет являться именно ПК, как носитель информации, путеводитель в информационную систему[16].

Но если считать данную позицию верной, то мы умышленно увеличиваем границы уголовной ответственности за указанное преступление, что не справедливо.

---

[15] Кадников Н.Г. Квалификация преступлений (теория и практика). М.: БЧ интернешнл Лтд., 2009. С. 18.

[16] Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. - М.: Новый юрист, 2008

Приверженники данной теории считают, что именно доступ к ПК, незаконное его использование можно квалифицировать как компьютерное преступлений, данный подход к определению, того, что же является предметом является слишком примитивным и, как считают большинство ученых правоведов, ошибочным.

Так как сам персональный компьютер будет считаться предметом иных преступлений, а именно преступлений против собственности.

Поэтому можно сделать верный вывод, что предметом в указанном преступлении будет именно компьютерная информация, базы данных или информационные ресурсы, которые содержатся в материальном носители, которым и является ПК[17].

Виновное лицо, совершающее данное преступление, посягает именно на вышеуказанные ресурсы, ставит под удар безопасность и защиту такой информации, а также нормальной работы с персональным компьютером или сети ЭВМ.

Если предметом противоправного общественно опасного посягательства является именно ЭВМ, то перед нами иная группа преступлений, определенная в УК РФ, как преступления против собственности.

Это логично, так как ЭВМ как техника, в отличии от информации овеществлена и материальна, имеет цены, а главное является именно вещью, причем чужой для преступника, что характерно для преступлений определенных 21 главой Особенной части УК РФ[18].

Похитить чужие средства можно и без карты, например, с помощью чужого «мобильного банка» или системы интернет-платежей, обманув владельца. Это кража, но если при этом виновный незаконно не влиял на

[17] Селиванов Н. А. Проблемы борьбы с компьютерной преступностью // Законность. - 1993. - № 8; Вехов В. Б. Компьютерные преступления: Учебное пособие / Под ред. В. П. Тихомирова, А. В. Хорошилова. - М.: Финансы и статистика, 1996

[18] Новое уголовное право России. Особенная часть: Учеб. пособие. М.: Зерцало, ТЕИС, 2006. С. 273

программное обеспечение серверов, компьютеров или сами сети. Это разъясняет п. 21 Постановления № 48[19].

Эти разъяснения не учел суд первой инстанции, который квалифицировал действия А. Ербягина п. «г» ч. 3 ст. 158 УК («Кража с банковского счета, а равно в отношении электронных денежных средств»). Ербягин использовал «мобильный банк», чтобы переводить себе деньги с чужого счета. Сколько именно, из судебных актов вымарано, указано только, что «ущерб значительный». По п. «г» ч. 3 ст. 158 УК Ербягин получил два года лишения свободы. Но Красноярский краевой суд счел наказание слишком суровым и объяснил это в определении № 22-993/2019[20].

Апелляция решила, что осужденный совершил «простую» кражу в крупном размере, п. «в» ч. 2 ст. 158 УК. По ней санкции заметно меньше, чем по п. «г» ч. 3 этой же статьи. Дело в том, что Ербягин пользовался «мобильным банком», но не вмешивался в работу программ, серверов и информационно-телекоммуникационных сетей. Краевой суд убрал этот квалифицирующий признак из приговора и с учетом других смягчающих обстоятельств назначил подсудимому год исправительных работ с удержанием 10% зарплаты.

Компьютерное вмешательство имело место в другом уголовном деле, где судили продавца салона связи «Мегафон» Петра Зволя. С помощью переоформления счетов абонентов он вывел порядка 500 000 руб., принадлежавших «Мегафону». Махинации он проводил в компьютерной базе лицевых счетов. Поэтому районный суд определил преступление как «мошенничество в сфере компьютерной информации» (ч. 1 ст. 159.6 УК). При этом первая инстанция отказалась дополнительно квалифицировать действия Зволя по ч. 3 ст. 272 УК («Неправомерный доступ к компьютерной информации с использованием служебного положения»). Районный суд объяснил свое решение тем, что Зволь использовал доступ к базе данных для реализации

[19] Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. N 48 г. Москва "О судебной практике по делам о мошенничестве, присвоении и растрате" / Компания «Консультант Плюс». - Дата обращения 10.05.2019

[20] Определение Красноярского краевого суда по делу № 22-993/2019 / Компания «Консультант Плюс». - Дата обращения 10.05.2019

преступного намерения завладеть деньгами «Мегафона». То есть эти действия и так входили в состав мошенничества.

Первую инстанцию поправил Самарский областной суд со ссылкой на п. 20 Постановления Пленума № 48. Там содержатся правила квалификации мошеннических действий, которые сопряжены с «неправомерным доступом к компьютерной информации или использованием вредоносных компьютерных программ». Это не только ст. 159 УК «Мошенничество», но и одна из трех специальных статей в зависимости от обстоятельств преступления: ст. 272 («Неправомерный доступ к служебной информации»), 273 («Создание, использование и распространение вредоносных компьютерных программ») или 274 УК («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»). Апелляция сочла, что здесь требуется дополнительная квалификация. Все-таки продавец «Мегафона» неправомерно занимался модификацией охраняемой законом информации, за что предусмотрена ответственность ст. 272 УК, говорится в определении № 22-6541. В итоге дело направилось на пересмотр.

Может возникнуть проблема при квалификации, если предметом посягательства будет не только компьютерная информация, защищаемая законом, но и сам объект ЭВМ[21].

Необходимо отметить, что «охраняемая законом» информация – определяется как информация, которую берет под свою охрану именно законодательство РФ, то есть это не любая компьютерная информация, а только определенная УК РФ.

Такая информация является априори доступной только определенному, ограниченному законом кругу лиц, имеющая особый правовой статус, определенный нормами действующего законодательства РФ, ее субъектов. Такая защищенная законом информация может касаться, например безопасности государства и общества, а также затрагивать жизнедеятельность

[21] Батурин Ю.М. Проблемы компьютерного права. - М.: Юридическая литература, 2001. - С. 129

отдельных членов общества, данных о вооружении, космосе, также данные касающиеся промышленного и сельскохозяйственного комплекса страны.

Но не всякая информация может подходить под смысл и содержания вполне конкретной норме закона об охраняемой законом компьютерной информации.

Данная информация принадлежит не отдельно взятому гражданину, а государству, как суверенному лицу, касающаяся по своему содержанию военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Нельзя ограничиваться только понятием государственная информация, подлежащей защите, необходимо сказать об информации, содержащую коммерческую тайну.

Это может быть информация, как коммерческая, так и содержащая служебную либо банковскую тайну[22].

Данный вид информации находится под защитой государства, а именно ее правовой статус определен нормами ГК РФ и УК РФ.

Особой информацией, находящейся под защитой, является то, что считается объектом авторского права, в данном случае гарантом выступают нормы Конституции РФ, а именно нормы ст. 44.

Если говорить об ответственности за нарушение правового статуса данной информации, то стоит отметить, что предусмотрена нормами УК РФ, а именно ст.272.

Если вышеуказанные виды компьютерной информации априори, по своему содержанию и назначению должны быть защищены законом, то вот вопрос о защите частной информации отдельно взятого гражданина в рамках УК РФ требует подробного анализа.

[22] Викторов М. Законность в кредитно-банковской сфере // Законность. - 2007. № 11. С. 23

Для рассмотрения данного вопроса требуется обратиться к главному закону страны – Конституции РФ.

Согласно данного закона, основы всех законодательных актов государства, каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст.23 Конституции РФ).

Именно данный закон дает с одной стороны свободу выбора в пользовании информации о своей личности (персональной информации), а с другой стороны ограничивает это же право, тем самым защищая права иных лиц.

Проанализировав нормы закона, мы делаем вывод, что нормы защиты прав личности на информацию, защищенную законом, предусмотрены именно ст. 24 Конституции, которая обеспечивает не допущение сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Но норма закона будет работать только в случае наличии иной нормы, которая будет устанавливать соответствующее наказание за нарушение материальной нормы.

Мы уже установили, что правовой статус личной персональной информации гражданина устанавливается нормами Конституции РФ, поэтому необходимо перейти к нормам закона, предусматривающим соответствующее наказание за нарушение данной нормы.

Именно УК РФ предусматривает наказание за нарушение таких норм как тайна переписки или неприкосновенности частной жизни.

Уголовное законодательство защищает информацию любого плана, содержащую сведения о личной тайне отдельно взятого человека, причем законом запрещены любые манипуляции в отношении данного объекта, как сбор, так и распространение, в том числе и семейных тайн человека.

К примеру, УК РФ предусмотрено наказание за разглашение тайны усыновления или удочерения (ст.155), так как данная информация является личной тайной отдельно взятой семьи.

Законом запрещено разглашение данной информации любому лицу, даже тому, кто подлежал усыновлению или удочерению.

Стоит отметить, что органы ЗАГСа не имеют право разглашать данную информацию, в виде выдачи дубликата свидетельства об усыновлении, даже усыновленному лицу. Данный документ доступен только родителям указанного лица.

Из вышесказанного можно сделать вывод, что запрашивание государственными и муниципальными органами такой информации также запрещено, так как нарушает именно семейную, приватную (частную) информацию, касающиеся отдельно взятой ячейки общества.

Семейная (личная) информация, имеющая статус конфиденциальности это и семейное положение, состояние здоровья, информация о денежном состоянии, счетах и вкладах в банках и т.д[23].

Сведения, относящиеся к личной приватной жизни человека, его вероисповедание, мировоззрение также относятся к охраняемой информации, так как считаются составляющей частной жизни человека, то есть является личной тайной, но стоит уточнить, что не все сведения считаются «охраняемой законом информацией».

Этот вопрос решается судом с учетом всех обстоятельств конкретного дела и, прежде всего, с учетом оценки степени тяжести наступивших вредных последствий для потерпевшего.

Объясняя правовой статус личной информации, стоит обратиться к федеральному закону, который регулирует расследования всех преступлений.

Федеральный закон «Об оперативно-розыскной деятельности», принятый в 1995 г., гарантирует сохранение тайны имени лиц, внедренных в

[23] Научно-практический комментарий к Уголовному кодексу Российской Федерации. В 2 т. Т. 1. Нижний Новгород: Номос, 2010. С. 343.

организованные преступные группы, штатных негласных сотрудников органов, осуществляющих оперативно-розыскную деятельность, а также лиц, оказывающих или оказавших содействие этим органам на конфиденциальной основе.

Из содержания норм данного федерального закона мы видим, что сведения указанные выше являются охраняемой законом информацией, за распространение которой грозит уголовное наказание.

Из всего вышеизложенного мы можем сделать вывод, что предмет преступления, согласно содержанию ст. 272 УК РФ:

нематериальные ценности, в частности, компьютерная информация, охраняемая законом, такие как конфиденциальные сведения о персональных данных, сведения, составляющие служебную, коммерческую, банковскую или государственную тайну, информация, являющаяся объектом авторского права.

Неправомерный доступ к компьютерной информации общего пользования, то есть неохраняемой законом информации, адресованной неограниченно широкому кругу лиц, не образует признаков преступления, ответственность за совершение которого предусмотрена ст.272 УК.

Преступления, хотя и связанные с компьютерной информацией, но не предполагающие в качестве основного непосредственного объекта общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети, не образуют признаков анализируемого деяния.

Изолированный же от объекта анализ предмета не позволяет уяснить то отношение, которому наносится ущерб, что, в свою очередь, может порождать ошибки при квалификации преступлений и, следовательно, ведет к противопоставлению основополагающих принципов уголовного права: законности и справедливости.

2.2 Способы совершения и сокрытия преступлений в сфере компьютерной информации.

Объективная сторона преступления, предусмотренного ч. l ст. 272 УК РФ, выражается в неправомерном доступе к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Как говорилось ранее для привлечения к ответственности необходимо наличие всего состава преступления, согласно нормы УК РФ[24].

На основании этого для привлечения виновного лица необходим факт именно неправомерного действия. Причем можно смело заявлять, что в данном случае это именно активное действие, а не бездействие, как это может быть в иных формах УК РФ.

Статья 272 УК РФ это именно осознанное действие преступника, выраженное в доступе к защищенной законом информацией или информационным ресурсам.

Вышеизложенное подтверждает, что обязательным составляющим элементом объективной стороны данного вида преступлений является неправомерность доступа к защищенной законом информации.

На правовую оценку преступления не влияет способ совершения преступления, то есть вариант доступа к защищенной законом информации не имеет значение. Но таких вариантов большое количество, и на одном возможном способе совершения этого преступления, прямо влияющим на квалификацию содеянного виновным, хотелось бы остановиться чуть подробнее.

[24] Панфилова, Е.И. Компьютерные преступления [Текст] : учебное пособие / Е. И. Панфилова. – М. : Феникс, 2007. – 254 с.

Речь идет о неправомерном доступе к компьютерной информации, совершенным с применением насилия над личностью либо угрозой его применения.

Данный вариант возможен, если преступник не владеет специальными профессиональными знаниями в сфере IT или ЭВМ, тогда данное лицо может принудить владельца информации или законного представителя потерпевшего, который обладает остаточными навыками и знаниями совершить преступление самому в отношении вышеуказанной информации.

Проблема в том, что диспозиция данного состава преступления не охватывает своим содержанием указанный способ его совершения. На основании этого квалификация преступления только лишь по ст. 272 УК РФ будет некорректной, так как посягательство в данном случае не только на общественные отношения связанные с компьютерной информацией, но и затрагивает безопасность жизни и здоровья личности и человека. В вышеуказанном примере суду необходимо будет проводить квалификацию содеянного преступления в сфере компьютерной информации по совокупности с преступлением против личности[25].

Стоит отметить, что спорным моментом в данном случае будет статус действия лица в отношении, которого были предприняты меры воздействия.

Рассмотрим несколько вариантов, один из которых, если виновное лицо вынудило третье лицо (потерпевшего либо законного представителя потерпевшего) осуществить незаконные действия и последний находился в состоянии крайней необходимости (ст.39 УК РФ), то виновник несет ответственность предусмотренную УК РФ единолично.

В противном случае ответственность наступает по правилам о соучастии в преступлении, хотя, конечно, квалификация по совокупности преступлений здесь также не исключается.

[25] Пархомов В. А, Старичков М. В. О «троянском коне», хакере и уголовной статье // Правосудие в Восточной Сибири. - 2003. - № 2-3. - С. 105

То есть чтобы квалифицировать действия третьего лица необходимо понимать нормы УК РФ о соучастии, в рассматриваемом варианте ответственность как соучастника будет лишь в одном случае, когда лицо не находилось в состоянии крайней необходимости, установленной нормами уголовного законодательства.

В данном случае лицо в отношении, которого были направлены угрозы только легкого вреда либо были угрозы побоев, будет квалифицироваться судом как соучастник, так как степень угрозы его здоровья не соответствует последствиям неправомерных действий.

Поэтому по ст. 272 и ст.119 УК РФ необходимо квалифицировать действия лица, под страхом убийства заставившего оператора ЭВМ совершить акт неправомерного доступа к компьютерной информации.

УК РФ не подразумевает наличие отдельно выделенных квалифицированных составов с учётом статуса компьютерной информации и ЭВМ. Необходимо уточнить, что неправомерный доступ к компьютерной информации не всегда бывает самостоятельным преступлением и являться самоцелью преступника, нередко данное деяние является только способом и орудием для свершения иного преступного деяния. Часто встречаемый случай, когда помощью дополнительных хакерских программ преступник или преступная группа получают экономическую выгоду, то есть в данном случае доступ к информации и ЭВМ были только средством для достижения результата в преступлении против собственности.

Из вышесказанного делаем вывод, что данный преступный поступок необходимо будет судом квалифицировать по совокупности данных преступлений, предусмотренных разными главами УК РФ[26].

Можно сделать вывод, что в данном случае персональный компьютер, то есть электронно-вычислительная техника, является своеобразным орудием свершения преступлений, причём не только против защищённой компьютерной информации, но и как говорилось ранее против собственности. Именно это

[26] Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 9.

особое орудие свершениями ставит сотрудников правоохранительных органов в тяжелое положение при определении таких обстоятельств преступления, например, как место и время свершения преступления.

Необходимо отметить, что место совершения и место наступления общественно опасных последствий в большинстве случаев не совпадает, так как прогресс в знаниях хакеров и возможностях компьютерной техники не стоит на месте. Что делает возможным несовпадение данных мест до уровня стран, то есть преступник совершает преступление с помощью персонального компьютера в одной стране, а последствия и потерпевшие лица находятся территориально в другой части нашего мира.

Необходимо остановиться на данных понятиях - место и время свершения - отдельно.

Время совершения преступления закреплено действующим законодательством и не ставит под вопрос своё содержание. Временем совершения любого преступления является строго время действия либо бездействия преступника (ст. 9 УК РФ), то есть для законодателя не важно время наступления последствий данных действий или бездействий.

Указанная правовая установка не может быть применена ко второй составляющей - месту совершения. Определение места совершения компьютерных преступлений на сегодняшний день является спорным моментом в правовом поле нашего государства и российского уголовного законодательства в частности.

Существует две точки зрения по данному вопросу, одно из которых на наш взгляд подкреплено нормами уголовного законодательства, что место является та территория, то государство в котором преступление было закончено. Закрепление содержания норм ст. 8 УК РФ подтверждает те случаи когда уголовная ответственность может быть применима, только в случае если деяние содержит все признаки состава преступления согласно норм УК РФ. Состав преступления рассматриваемых преступлений может считаться полным только при наличии вредных последствий, так как данный раздел

подразумевает только материальные составы по смыслу уголовного законодательства.

Иная точка зрения полностью отличается от вышеуказанной, ее последователи утверждают, что ответственность должна наступать в месте совершения преступного действия, не зависимо от места наступления последствий от данного действия. Но стоит отметить, что такой подход не будет верным в некоторых случаях, рассмотрим подробнее.

Если преступление совершалось территориально в нескольких государствах, то ответственность согласно норм уголовного права должна наступить в месте окончания преступления, как следствия наступления общественно-опасных последствий. То есть не зависимо от места нахождения участников преступления ответственность будет наступать по законодательству того государства в котором было окончено преступное деяние.

Стоить отметить, что законодательство не всех стран подразумевает наличие рассматриваемого состава преступления и если преступники пытаются воспользоваться данными пробелами, то им не стоит забывать, что если преступное деяние было направлено на интересы представителей страны, которая имеет вышеуказанные составы то ответственность будет применена того государства в котором было окончено преступление, то есть были нарушены права и наступили последствия.

Обязательное наличие согласно действующему уголовному законодательству последствий деяния преступника было отмечено выше, стоит перейти к следующему обязательному признаку объективной сторону преступления против компьютерной информации - причинной связи между действием и последствиями данного действия.

Для начала необходимо проанализировать и классифицировать способы и виды преступных деяний в отношении компьютерной информации: копирование, уничтожение, изменение и т.д.

Начнём данный анализ с незаконного копирования информации, которая находится под зашитой закона, данное действие можно охарактеризовать как

перемещение информации с одного электронного носителя на другой, например на USB накопитель.

Уничтожение и блокирование защищаемой информации это незаконные действия заключённые в первом случае в том что информация перестаёт существовать совсем, а во втором становится недоступной в силу закрытия данного допуска с помощью технических средств.

Также существует понятие незаконного модифицирования защищаемой законом информации. Данная модификация подразумевает такое изменение исходной информации которое не меняет ее сущности.

Есть некоторые условия, которые не позволяют квалифицировать действие как незаконное копирование, это те случаи когда информацию охраняемую законом не переносили с одного носителя на другой, а только ознакомились с ней. Данные действия могли быть совершены, к примеру, во время приготовления к другому преступлению, то есть данное знакомство с информацией были или подготовкой или способом получить данные или средства для совершения иного преступного деяния.

Можно сделать вывод, вредными последствиями являются:

1. Нарушение работы компьютерной техники (персональный компьютер, система ЭВМ, сеть ЭВМ и т.д.);

2. Вывод ЭВМ путём модификации или иного нарушения компьютерной информации;

3. Нарушение целой сети персональных компьютеров путём незаконной модификации файлов операционной системы ЭВМ. Именно наступление хоть одного из данных вредных последствий и является основанием для утверждения об окончании преступления против компьютерной информации. На данный вид преступлений распространяются нормы уголовного законодательства о покушении (ст. 30 УК РФ), данное условие применяется для случаев, когда незаконное действие в отношении информации было совершено,

но было пресечено третьей стороной до наступления вышеуказанных последствий[27].

Если говорить про такую составляющую как приготовление к совершению преступления против компьютерной информации, то стоить отметить что в силу небольшой тяжести согласно ч. 2 ст. 15 УК РФ, данная стадия не инкриминируется и не несёт за собой уголовное наказание.

Вернёмся к вопросу, который мы поставили перед собой в рамках данного дипломного исследования, к вопросу причинно-следственной связи между действием (так как преступное деяние в данном случае не может быть выражено в бездействии) преступника и негативными последствиями данного проступка[28].

Данный состав преступления не отличается от иных тем, что суд и до него следственные органы обязаны доказать наличие причинно-следственной связи между поступком и последствиями в виде копирования, уничтожения, модификации и т.д.

Данное условие обязательно так как данная составляющая обязательна для объективной сторону данного состава преступления и поэтому решение суда не может быть основано на догадках или предположениях, а должно иметь законное основание, доказанное в рамках правового поля.

Теория уголовного права нашего государства даёт нам определение причинно-следственной связи, благодаря которому определить ее наличие либо отсутствие становится реальным.

Причинно-следственная связь в уголовном праве РФ - это такое явление, при котором причина обоснованно порождает следствие. В нашем случае неправомерный доступ к защищаемой законом информации приводит к уже перечисленным негативным последствиям: копирование, уничтожение, блокировка и иное, установленное ст. 272 УК РФ.

---

[27] Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. Б.П. Смагоринского. – М., 1996. – С. 74-92.

[28] Уголовное право. Общая часть: Учебник / Под ред. н.и. Ветрова, Ю.И. Ляпунова, М.: НОВЫЙ Юрист, КноРус, 2007. С. 217.

Данные негативные последствия, являющиеся последствием незаконного деяния, могут иметь место и без указанного неправомерного доступа, в данном случае ответственность по указанной норме права не может наступить, так как будет отсутствовать само неправомерное действие, то есть будет отсутствовать состав преступления предусмотренного самой материальной нормой права. Нарушение данной константы, установленной нормой уголовного законодательства недоступно и недопустимо в правовом обществе с развитой судебной системой.

После анализа всех составляющих состава преступления, необходимо охарактеризовать способы совершения, данная классификация основана на методе воздействия на ЭВМ, и как следствие компьютерную информацию.

Можно выделить непосредственный доступ к компьютерной информации или ее носителю, а также дистанционный, то есть удаленный доступ.

Отдельным способом является фальсификация данных для замены доступа и дальнейшего управления информацией или ее носителями.

Способ, который делает возможным уничтожение и блокировки информации - создание вредоносных программ либо незаконное внесение изменение в информацию или, а структуру ее носителя. Также выделяют метод незаконного распространения носителей защищаемой законом компьютерной информации.

Также нужно понимать, что данные методы могут быть скомбинированы и быть комплексными, все это зависит от цели преступления.

Разберём вышеуказанные методы подробнее.

Начнём с прямого - доступа к машинному носителю компьютерной информации, то есть непосредственно к информации.

Данный метод непосредственно сопряжён с иными преступлениями, так как возможен только при прямой контакте к компьютерной техники и машинным носителем информации, то есть машинный носитель должен быть временно, или бессрочно изъят у правообладателя, например, путём кражи или грабеже.

Исходя из данной специфике, вероятнее всего, следами данного преступления будут являться следы взлома, повреждения или уничтожения охранной сигнализации и так далее.

Дистанционный (телекоммуникационный) доступ к компьютерной информации, а именно к ее машинному носителю, возможен через промежуточные средства связи и иные персональные компьютеры, без непосредственного материального воздействия на первичный машинный носитель защищаемой законом компьютерной информации.

В данном случае для достижения доступа будут использоваться специальные компьютерные программы, вирусы, специальные компьютеризированный средства подбора пароля или код-доступа, ну и как говорилось ранее обязательное наличие дополнительного транзитного носителя компьютерной информации, например, персонального компьютера.

Следами данного метода будут являться, к примеру, информация, полученная с помощью регистрирующих и пеленгующих средств связи, если используются вирусы, то с помощью программ-антивирусов и так далее. Следующий способ очень распространён в сфере экономических преступлений с целью получения денежные средства путём доступа к банковским счетам и иным способам - фальсификация данных и управляющих команд.

Следами данного метода являются несовпадение первичных данных и модифицированных преступниками данных, то есть нужен сравнительный анализ для их обнаружения.

Следующая группа основана на незаконном внесении изменений в программы для ЭВМ, которые являются носителями компьютерной информации, а также на создании вредоносных программ, с помощью которых может быть достигнуто копирование, уничтожение, блокировка или модификация информации, которая находилась под защитой закона (состав преступления предусмотренный ст. 273 УК РФ).

В данном случае следами преступления будут являться: сбой или нарушение работы ЭВМ или сети ЭВМ, изменение или модификация, а также

блокировка информации, которая находилась на машинном носители, появление иной ранее не представленной информации на носители и так далее.

Пятая группа выражается в форме распространения, продажи, проката, аренды, а также создания условий для распространения программ для ЭВМ или носителей информации, являющихся контрафактными, содержащими запрещённую уголовным правом информацию или нарушающими авторские права.

Комплексные методы, как уже говорилось, состоят из нескольких методов, причём один из них будет являться основным, то есть доминирующий метод, более подходящий и второстепенный необходимый для выполнения отдельных целей и задач в рамках компьютерного преступления[29].

Выбор методов будет зависеть от специальных знаний и профессиональных умений преступника, а также от цели и мотива преступления.

На основании этого можно сделать вывод, что подробный анализ метода совершения противоправного деяния необходим в процессе расследования данного типа преступлений, так как выбранные методы могут приоткрыть завесу многих обстоятельств преступления.

[29] Максимов, В.Ю. Компьютерные преступления (вирусный аспект) [Текст] : учебное пособие / В.Ю. Максимов. – М.: АО «Центр ЮрИнфор», 2006. – 210 с.

Глава 3. Особенности и методы расследования преступлений в сфере компьютерной информации.

3.1 Обстоятельства, подлежащие установлению и доказыванию.

Если говорить о неправомерном доступе к компьютерной информации, то стоить заметить, что данный вид преступлений имеет большую новизну вопроса, но набирает серьезные обороты в настоящее время.

Именно развитие компьютерных технологий и просвещения в сфере IT способствуют появлению новых вариантов и способов совершения преступлений против собственности, а также иных преступлений, к примеру, нарушение авторских прав, государственной измены и далее.

Также одной из особенностей и доказательств общественной опасности компьютерных преступлений является свобода совершения преступлений не взирая на государственные границы.

Положение усугубляет плохо разработанная структура теоретической нормативной базы в сфере компьютерных преступлений, данные составы преступлений появились в законодательстве только с момента вступления в силу действующего Уголовного кодекса РФ, то есть с 1 января 1997.

Необходимо отметить, что именно действующий Уголовный кодекс РФ встал на защиту частных прав граждан на защиту информации, так как до 01.01.1997 под защитой закона находилась лишь государственная тайна.

Наличие особенностей технического характера не делают данные виды преступлений проще для расследования и дальнейшего предотвращения.

Сотрудники правоохранительных органов не имеют необходимый уровень специальных знаний в сфере IT.

Все вышеназванные моменты приводят нас к выводу о сложности в проведении расследований, а в дальнейшем во время судебного процесса, так как технические сложности, недостаточная компетентность могут привести к нарушению принципов справедливости и законности судопроизводства.

В предыдущим двух главах дипломного исследования мы проанализировали субъективную и объективную сторону преступлений в сфере компьютерной информации, выделили все условия наступления уголовной ответственности и все составляющие состава преступлений, предусмотренных уголовным законодательством.

Именно для доказывания наличия всех элементов состава преступления необходимо установить при расследовании многие обстоятельства.

Первое и на наш взгляд самое важное обстоятельство - наличия факта совершения преступления. Так как если негативные последствия являются следствием не преступного действия, а, к примеру, следствием поломки или внешнего техногенного воздействия, то состав преступления не имеет места в данном случае.

То есть первое, что необходимо установить - совершалось ли незаконное действие в отношении компьютерной информации.

Далее, есть факт совершения установлен и доказан, необходимо обратиться к определению того, какая информация подвергалась преступному воздействию.

Главное обстоятельство это содержание и назначение информации, в отношении которой было совершено преступное деяние. Как уже упоминалось ранее не вся информация защищается законом, поэтому нужно определить к какой категории относится информация в каждом конкретном случае: общедоступная или все же охраняемая законом, с указанием ее категории и ссылкой на соответствующий федеральный закон во втором случае.

Правоохранительными органами устанавливается в какой форме была представлена информация, индивидуальные признаки данной информации (форма, количественные и качественные характеристики), а также устанавливаются признаки, персонализирующие машинный носитель информации, в отношении которой совершён преступный поступок.

Также необходимо проверить и установить статус и содержание информации, которая содержится на указанном машинном носителе вместе с предметом конкретного преступления против компьютерной информации.

Время и место совершения компьютерного преступления, также устанавливается в соответствии с нормами уголовного права, о чем говорилось в предыдущей главе дипломного исследования.

Для каждого отдельно взятого преступления необходимо определить способ совершения, в рамках чего подлежит анализу способ доступа к предмету, способ обхода зашиты предмета, метод воздействия, который был объектом исследования ранее.

По причине наличия возможности совершения преступления необходимо изучить режим работы с информации в отношении которой произошло нарушение, порядок и способы ее защиты, а та же установить причину нарушения безопасности, благодаря которой преступное деяние смогло быть осуществлено.

Дополнительно устанавливают с помощью чего было совершено преступление, определяют код, шифр и так далее.

Для дальнейшего расследования важно понять и установить факт наличия утечки конфиденциальной информации, к примеру, от сотрудников или иных сведущих лиц. Так как необходимо установить или опровергнуть факт участия должностных лиц потерпевшей стороны в преступлении, по причине наличия у них соответствующих допусков и необходимых знаний.

Чем отличается мошенничество с использованием служебных полномочий, разъясняет п. 29 Постановления Пленума № 51[30].

В частности, его может совершить лицо, которое использует во вред свои «служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные функции».

30 Постановление Пленума Верховного Суда РФ от 19.12.2017 N 51 "О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)" / Компания «Консультант Плюс». - Дата обращения 10.05.2019

Для правильной квалификации преступления их необходимо четко определить, напомнил Оренбургский облсуд в уголовном деле Игоря Перепелкина. По итогам такого пересмотра подсудимому удалось добиться смягчения наказания.

Районный суд приговорил его к 2,5 годам в колонии общего режима и штрафам в общей сумме на 750 000 руб. Перепелкина признали виновным в уклонении от уплаты налогов (ч. 1 ст. 199 УК) и покушении на мошенничество в особо крупном размере с использованием своего служебного положения (ч. 3 ст. 30, ч. 4 ст. 159 УК).

Как установило следствие, фактический руководитель ООО оформлял фиктивные поставки и пытался возместить из бюджета более 3 млн руб. НДС.

Первая инстанция решила, что Перепелкин совершил мошенничество с использованием служебного положения, потому что он распорядился учредить эту фирму и фактически управлял ею (бизнес был оформлен на родственницу лишь номинально).

Иного мнения оказался Оренбургский областной суд. Он применил более формальный подход. По документам осужденный в компании никто и никаких полномочий не имеет. «Суд не указал в приговоре, какими служебными полномочиями был наделен Перепелкин и какие он использовал при совершении преступления», – излагается в определении № 22-680/2019. Придя к таким выводам, апелляция уменьшила штраф на 250 000 рублей[31].

Отдельно стоит остановиться на определение размера материального ущерба. В ее размер входит не только стоимость самой охраняемой информации, которая послужила предметом преступления, но стоимость системы, средств направленных на защиты, стоимость самого машинного носителя предмета преступления, а главное установленный размер ущерба выраженного в недополученной прибыли, по причине невозможности использовать данную информацию.

[31] Определение Ульяновского районного суда по делу № 22-680/2019 [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019

Размер и вид ущерба, в случае если он не материальный, также подлежит установлению, в том числе кому причинен и кем и как может быть возмещен.

Далее сотрудникам правоохранительных органов необходимо установить или опровергнуть наличие квалифицирующих признаков преступления, предусмотренных уголовным законодательством.

- совершено группой лиц по предварительному сговору или организованной группой;
- совершено лицом с использованием своего служебного положения;
- совершено лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети;
- преступные деяния повлекли по неосторожности тяжкие последствия (утрату особо ценной информации; вывод из строя ЭВМ, системы ЭВМ или их сети, обеспечивающих функционирование основных технологических процессов (систем) режимных объектов информатизации; повлекшие несчастные случаи с людьми, аварии и катастрофы).

Далее подлежит установлению и доказыванию следующие данные - данные о субъекте или субъектах преступления, они содержат много критерий, это анкетные данные, содержащие ни только данные об имени, но и все остальные аспекты жизни личности, например, звание и семейное положение.

Затем подлежит анализу сведения о совершенных ранее преступлениям, если это конечно применимо.

После этого подлежит установлению физические и физиологические данные: рост, отличительные признаки внешности, отпечатки, группа крови и так далее, описание внешности, касательно стиля в одежде и отличительных деталей.

Отдельно стоит обратить внимание на психолого-психические признаки субъекта, то есть на уровень знаний, навыков, самооценки, также наличие определённых наклонностей или, к примеру, фобий.

После этого проводится установление наличия соучастников, круга лиц, с которыми можно обсудить необходимые моменты, касательно субъекта преступления.

Если в расследуемом случае имеет место не субъект, а группа лиц, то стоит установить следующие обстоятельства, касательно признаков организационной преступной группы: момент организации и срок существования, для определения устойчивости функционирования, организация с целью получения экономической выгоды, распределение ролей в данной ОПГ.

Дополнительно в данном случае устанавливается, какой порядок управления в ОПГ, существует ли определенные способы мотивации и наказания в группе для всех участников, наличие общих денежных, транспортных и иные материальных средств, также их вооруженность и техническая оснащенность.

Необходимым обстоятельством в любом расследовании является установление наличия или отсутствия коррупционных связей с правоохранительными и иными силовыми структурами, наличие покровителей, в том числе властных и обладающих определенным статусом в нужных кругах.

Установление элементов объективной стороны, а именно цели и мотивов совершения преступления также является обязательным на момент проведения расследования.

Далее устанавливаются все необходимые сведения, касательно потерпевшего в результате совершения преступником запрещенных уголовным законодательством действий, в зависимости от его правового статуса: физическое или юридическое лицо.

Юридическое лицо: название; адрес; форма собственности; вид хозяйственной деятельности; сведения о руководителе (-ях) и главном бухгалтере; данные о лице, ответственном за получение, хранение, обработку, передачу, уничтожение или защиту компьютерной информации, подвергшейся преступному воздействию, либо ее машинных носителей.

Физическое лицо: анкетные; учетные; физические; физиологические; психолого-психические; оформление внешности; круг связей лица.

Необходимо установить и доказать виновность лица, совершившего преступное деяние, предусмотренное определенным составом преступления УК РФ.

В случаях, когда лицо, совершившее преступление в сфере компьютерной информации, неизвестно, дополнительно необходимо установить: сведения о преступлениях данной категории, совершенных ранее аналогичным способом, о лицах, «проходивших» по этим преступлениям, факты о всех случаях нарушения должностных инструкций и т.д.

Необходимо выявить и установить наличие либо отсутствие недовольных сотрудников в организации, которая является потерпевшей. И в случае наличия таковых, определить местонахождение представляющего интерес лица в момент совершения преступления.

Выявление вышеуказанных обстоятельств происходит в результате проведения следственных действий, оперативно-розыскных и иных мероприятий, о планировании и организации, проведения которых пойдет речь в следующем параграфе данной главы настоящей выпускной дипломной работы.

3.2 Особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации.

В случае возбуждения любого уголовного дела следующим этапом будет являться стадия предварительного расследования. Именно во время данной стадии сотрудники правоохранительных органов, следователи и дознаватели, устанавливают все необходимые обстоятельства совершённого преступления, которые были подробно изучены нами в предыдущем параграфе данного исследования.

Целью расследования является раскрытие всех подробностей совершенного преступления, установление всех фактов и привлечение виновным лиц к уголовной ответственности.

Именно на этой стадии формируется все уголовное дело, которое дальнейшем передаётся в суд.

Ещё одной задачей расследования является установление всех причин и условий совершенного преступления для дальнейшей профилактики аналогичных преступлений.

Как уже упоминалось, предварительное расследование может проводиться силами, как следователя, так и дознавателя, если это будет относиться к компетенции данных органов.

Согласно нормам процессуального права, по решению суда или прокурора даже дела, относящиеся к компетенции дознавателя, могу быть переданы в следственные органы.

Как мы понимаем для достижения целей органы дознания и следствия наделены определенными полномочиями и имеют право осуществлять так называемые следственные действия - уголовно-процессуальные действия направленные на сбор и проверку доказательств.

Целью таких действий является установление и доказывание, обстоятельств конкретного преступления, для достижения данной цели выполняются следующие задачи: проверяются имеющиеся доказательства и находятся новые.

Следственные действия способствуют розыску, выявление новых преступлений и иное.

Главной особенностью следственных действий является четкое следование нормам права на всех этапах данных действий, будь то подготовках к ним или само действие, но и фиксация результатов.

Именно данное строгое соблюдение норма права даёт основание пользоваться результатами следственных действий, в противном случае они не могут быть использованы в дальнейшем.

В действующем законодательстве предусмотрены следующие виды следственных действий: осмотр, освидетельствование, следственный эксперимент, обыск, выемка, наложение ареста на почтово-телеграфные

отправления, контроль и запись переговоров, допрос, очная ставка, предъявление для опознания, проверка показаний на месте, производство экспертизы.

Разберем подробнее некоторые из них, начнем с процедуры допроса.

Следственное действие подразумевающее под собой получение сведений от потерпевшего и свидетелей, если они есть - это допрос, регламентированный нормами УПК РФ.

По общему правило производится по месту проведения предварительного следствия, но в случае особых условий и оснований для переноса, может проводиться по месту жительству допрашиваемого либо по месту лечения.

Необходимо отметить, что на допрос лицо приглашается повесткой, вручённой лично под расписку либо в помощью средств связи.

В случае если лицо, которое требуется допросить ещё не достигло 16-летнего возраста, то данная повестка выдаётся законным представителям.

Данное следственное действие ограничено временными критериями, общая продолжительность в день не может быть более 8 часов, причём данный срок должен быть разделён часом для отдыха после первых 4 часов процедуры.

Для правомерного допроса следователю или дознавателя необходимо предъявить свои документы и разъяснить права и обязанности, установленные законом для тех, кого допрашивают.

Согласно норм уголовного законодательства Российской Федерации допрос должен быть законным, без применения давления и силы, а также не должен содержать наводящих вопросов.

Допрос обвиняемого надо начинать с вопроса - признает ли он себя виновным.

Затем обвиняемому предлагается дать показания по существу обвинения.

На первых этапах расследования такого вида преступлений большое значение имеет осмотр и обыск, в случае необходимости то выемка.

Если говорить про изъятие каких-либо предметов, то тут очень важно зафиксировать его местонахождение в отношении с другими предметами на

месте осмотра, для получения более полной картины происходящего.

Очень часто на практики возникают проблемы связанные с изъятиями электронной техники, так как преступники страхуют себя и создают все условия для нейтрализации доказательств, необходимых следствию, путем написания специальных программ и кодов для уничтожения, к примеру, информации на машинных носителях. Очень часто это сопровождается запросом определено настроенного пароля для доступа к полученной во время обыска информации.

Но помимо изъятия технических средств и носителей информации следственные органы собирают стандартные вещественные доказательства, а главное отпечатки пальцев на всем месте осмотра.

В зависимости от целей осмотра и изъятия электронной техники могут использоваться различные приемы исследования.

Основной род судебных экспертиз по делам этой категории - судебные компьютерно-технические, в рамках которых выделяют четыре вида:

а) судебная аппаратно-компьютерная экспертиза, заключающаяся в проведении исследования:

б) судебная программно-компьютерная экспертиза, назначаемая для исследования программного обеспечения;

в) судебная информационно-компьютерная экспертиза, имеющая цель поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или порожденной программами для организации информационных процессов в компьютерной системе.

г) судебная компьютерно-сетевая экспертиза, основывающаяся прежде всего на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию.

Возможно применение иных экспертиз для расследования преступлений против компьютерной информации.

Одним из следственных действий является следственный эксперимент, который применяется для проведения проверки теории на практике, то есть опытным путем.

Инициатором данного действия могут быть многие участники уголовного процесса по делу.

Целью данного следственного действия является проверка предположений, возникающих в процессе следствия, а также получение дополнительной информации, к примеру, об умениях и навыках подозреваемого, что необходимо для законного установления вины данного участника уголовного процесса[32].

Существует ряд обязательных условий для проведения данного следственного действия, это наличие условий, не унижающих честь и достоинство участников следственного эксперимента, наличие понятых, а также в случае необходимости обвиняемый или подозреваемый, защитники этих лиц, а также потерпевший и свидетель.

Как уже указывалось ранее, все следственные действия требуют соблюдения норм УПК РФ, на основании этого ход следственного эксперимента фиксируется в протоколе, в котором отражаются все условия проведения.

При проведении следственного эксперимента выясняется возможность наступления вредных последствий при нарушении определенных правил.

Он проводится с использованием копий исследуемой информации и по возможности на той же ЭВМ или ПК: при работе на которой или котором нарушены правила.

Согласно ст. 47 УПК РФ обвиняемый появляется в процессе расследования с момента предъявления ему постановления о привлечении в качестве обвиняемого.

[32] Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.М. Лебедева. М.: Издательская группа ИНФРА-М - НОРМА, 2010. С. 640.

До предъявления обвинения при расследовании уголовного дела может фигурировать подозреваемый.

Им согласно ст. 46 УПК РФ является лицо, в отношении которого возбуждено уголовное дело, которое задержано в соответствии со статьями 91 и 92 УПК РФ; либо к которому применена мера пресечения до предъявления обвинения в соответствии со статьей 100 УПК РФ; либо которое уведомлено о подозрении в совершении преступления в порядке, установленном ст. 223.1 УПК РФ.

При допросе подозреваемого в совершении преступлений против компьютерной информации необходимо установить наличие специальных навыков в обращении с ПК и ЭВМ, а также установить, откуда данные навыки появились у данного лица.

Далее устанавливается должность и место работы, а также необходимость работать с ПК согласно должностной инструкции, в случае положительного ответа, необходимо получить информацию о наличие/отсутствии допусков к определенным программам, а также узнать какие операции с компьютерной информацией выполняет на рабочем месте.

Также важно установить имеет ли подозреваемый доступ к сети Интернет, закреплены ли за ним по месту работы коды и пароли для работы в компьютерной сети и иную связанную информацию.

Можно сделать поспешный вывод, что установить подозреваемого проще, если способ проникновения и доступа к предмету преступления был достаточно сложным и требующим специальных знаний, проще, так как существует узкий круг специалистов, обладающих соответствующими способностями, весьма ограничен.

Но данный вывод неверный, так как именно профессиональные хакеры, обладающие специальными знаниями могут подставить третье лицо, для заведения следствия в тупик.

В таких случаях хакер выбирает лицо, которое имеет необходимые доступы для совершения преступления и трудоустроенное в организации,

которая является потерпевшим лицом.

Для получения необходимой информации о лицах имеющих допуск к определенным программам, кодам и допускам, а также определения лиц пользующихся персональными компьютерами и имеющих доступ к сети Интернет, необходимо установить круг лиц, отвечающих за надлежащий режим доступа к компьютерной системе или сети, а также ее защиту.

Доказать виновность и выяснить мотивы лиц, осуществивших несанкционированный доступ к компьютерной информации, можно лишь по результатам всего расследования.

Решающими здесь будут показания свидетелей, подозреваемых, обвиняемых, потерпевших, заключения судебных экспертиз, главным образом информационно-технологических и информационно-технических, а также результаты обысков.

В ходе расследования правоохранительные органы получают необходимую информацию для установления мотивов, наличия вины, способов совершения преступления, а также условий для его совершения, которые этому поспособствовали.

На этапе установления обвиняемого, во время его допроса необходимо выявить и установить все этапы преступлении, от подготовки к нему, в случае если мы имеем вредоносную программу, то необходимо выяснить алгоритм ее действия и элемент информации, на которую он влияет.

Именно в таких случаях, то есть при наличии вредоносной программы, установление вреда и размера ущерба затруднено моментальным размножением данного вируса в огромной количестве на всей компьютерной сети потерпевшего.

Но не только вирусные атаки несут огромный ущерб потерпевшему, но и нарушение правил эксплуатации, так как именно они в конечном итоге полностью парализуют деятельность всего учреждения в целом.

Расследование преступления основанного на нарушении правил эксплуатации ЭВМ строится на подробном анализе и изучении всех

нормативных документов и правил организации- потерпевшей, для получения общего представления всей структуры а также изучение отдельных инструкций для выявления частных особенностей именно данной организации.

В данном случае, как и в случае с вредоносными вирусами, необходимо привлечение специалистов, специализирующих на таких моментах, но не имеющих личной заинтересованности в следствии.

Служебное расследование, в рамках которое было выявлено нарушение правил эксплуатации, может быть источников ответов на многие вопросы следствия, поэтому подлежит тщательного изучению на первых этапах расследования, именно по этим данным можно выстроить алгоритм следственных действий уже имея на руках ответы на многие вопросы.

При расследовании данной категории дел очень важно установить, где расположена станция, эксплуатация которой велась с грубыми отступлениями от требований информационной безопасности.

Ответ на данный вопрос можно получить в процессе информационно-технической экспертизы в рамках расследования, если поставить данный вопрос специалистам, ответственным за данное следственное действие.

Как уже говорилось ранее, для установления времени нарушения данных правил требуется определение наступления вредных последствий от данного преступного деяния.

Время действия и время последствий может, как совпадать, так и иметь между собой большой временной промежуток.

На вопрос о нарушении правил могут ответить специалисты, изучающие все протоколы и серверы, но также это можно установить путем проведения допросов, например свидетелей, если они участвуют в эксплуатации ЭВМ.

Время, как и место, может быть определено в процессе проведения информационно-технической экспертизы.

Если разбирать определение времени наступления именно вредных последствий от совершенного преступления, то следствию может помочь, как уже говорилось ранее служебное расследование, материалы которого являются

основой всего расследования, допрос всех участников уголовного процесса и, конечно же, осмотр места происшествия.

Необходимо указать, что способ нарушения правил эксплуатации ЭВМ может быть выражен в выполнении несанкционированных операций (активный) и в невыполнении обязательных для исполнения операций и действий (пассивный).

Следствие может получить ответ о способе нарушения правил в процессе допросов участников уголовного процесса, при обязательном участие специалистов, в результате экспертизы, а главное в процессе проведения следственного эксперимента.

Участники допроса объясняют последовательность и регламент выполнения работ с ЭВМ, результат следственного эксперимента уточняет последствия и вероятность наступления вредных последствий при нарушении регламента.

Как говорилось ранее, для чистоты эксперимента используется та компьютерная техника (ЭВМ, персональный компьютер или машинный носитель информации), с помощью которой было нарушено правило эксплуатации.

Перед следствием стоит задача установить лицо, допустившее нарушение правил эксплуатации ЭВМ, предусмотренное ст. 274 УК РФ, так как не любое лицо имеющее доступ к данной ЭВМ имеет доступ к необходимой компьютерной информации в силу своей должности и допуска.

Именно среди лиц, имеющих необходимый доступ и допуск к компьютерной информации и стоит устанавливать нарушителей правил.

В отношении каждого из них устанавливается, не только анкетные данные и информация о должности и должностных правах и обязанностях, но и информация касательно его профессионального уровня, также уровня образования и, к примеру, стажу работы и списка должностей, занимаемых ранее.

Но главной информацией является уровень допуска к охраняемой информации, наличие обязанностей по защите компьютерной информации, участие в разработках программных систем, доступ к базам данных и иное.

Вся информация касательно подозреваемого может быть получена из личных дел сотрудников, из информации, полученной в процессе допросов всех участников уголовного процесса, изучения всех ЭВМ и машинных носителях компьютерной информации, при изучении протоколов безопасности и иных данных полученных в процессе расследования.

Нужно напомнить, что наличие вины у подозреваемого может быть установлено только после проведения всех необходимых следственных действий, проводимых для установления наличия всех элементов состава преступления, предусмотренного уголовным кодексом.

Также стоит акцентировать внимание, что именно материалы служебного расследования организации, которая является потерпевшей, может пролить свет на многие обстоятельства уголовного дела, которые требуют установления и доказывания в уголовном процессе и являются по своей сути основополагающим звеном в расследовании преступлений в сфере компьютерных технологий, таких как незаконный доступ к компьютерной информации, создание, использование и распространение вредоносных программ, а также нарушений правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС.

ЗАКЛЮЧЕНИЕ

Компьютеры, и как следствие компьютерная информация, стали постоянными спутниками любого человека в XXI веке, трудно представить работу организации без использования ЭВМ.

Каждое рабочее место в офисах оборудовано персональными компьютерами, оргтехникой, мобильными телефонами и планшетами, весь бухгалтерский и управленческий, в том числе и складской учет организации и индивидуальные предприниматели давно ведут с помощь специальных программ и ЭВМ, что с одной стороны делает работу прощу и более автоматизированной, а с другой стороны создает увеличенную уязвимость той информации, которая храниться на вышеуказанных машинных носителях.

Именно прогресс и усложнение системы работы персональных компьютеров становятся стимулом для профессионального роста и увеличения специальных знаний у любого представителя современного общества, а если говорить про профессионалах в данном вопросе, то их развитие в свою очередь тоже является своеобразным катализатором улучшений в сфере информационных технологий.

Данная компьютеризация общества задает свой тон в сфере компьютерных преступлений.

Если проанализируем статистику преступлений и отдельно преступлений в сфере компьютерной информации, то мы сможем сделать вывод о высоком уровне актуальности данного вопроса.

Именно данная актуальность сподвигла на выбор темы для данного дипломного исследования.

Для достижения цели исследования, которая заключалась в изучение особенностей расследования преступлений в сфере компьютерной информации, были поставлены задачи, которые на наш взгляд были выполнены полностью. Разберём подробнее.

Задачи, поставленные для достижения цели выпускной дипломной работы, выполнены, проанализированы и изучены все аспекты вопроса, касающегося особенностей методики расследования преступлений против компьютерной информации.

В процессе написания данной выпускной дипломной работы были выполнены следующие задачи:

- анализ криминалистической характеристики субъекта и субъективной стороны преступлений в сфере компьютерной информации;

- изучение предмета посягательства при совершении компьютерных преступлений, а также изучение различных подходов к определению предмета компьютерных преступлений;

- анализ объекта и объективной стороны преступлений в сфере компьютерной информации;

- изучение особенности выявления личности преступника в сфере компьютерных преступлений;

- анализ обстоятельств, подлежащих установлению и доказыванию в процессе расследования преступлений в сфере компьютерной информации;

- рассмотрение особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации.

Первое что нужно было проанализировать для достижения это элементы криминологической характеристики компьютерных преступлений, для этого две первые главы были посвящены составляющим субъективной и объективной стороны преступлений, предусмотренных уголовным законодательством в сфере компьютерной информации.

В первую очередь в первой главе был изучен объект криминологического исследования в данных преступлениях - личность самого преступника.

Самый большой пробел, который возможен в расследовании – это оставление без внимания особых навыков преступников, которые говорят нам об определенных способах совершения этих преступлений, которые в свою очередь формируют так называемый почерк преступника.

Именно этот почерк и личностные особенности совершения и сокрытия преступлений и содержит большую часть «следов личности», совершившего преступление в сфере IT.

Событие преступления протекает в определенной обстановке, именно это и составляет один из элементов криминологической характеристики субъективной стороны данных преступлений.

Также в рамках дипломного исследования был проведен анализ особенностей обстановки каждого конкретного преступления, который позволяет выявить обстоятельства, которые способствовали или вообще сделали возможным совершение данного преступления в сфере компьютерной информации.

Были сделаны выводы, что именно данное изучение обстоятельств и обстановки преступления делает розыскные мероприятия более эффективными, приводящими к задержанию преступников, то есть является залогом раскрытия преступлений данного вида.

Говоря о субъективной стороне любого преступления в рамках данного дипломного исследования, было упомянуто о таких моментах, составляющих субъективной стороны, как вина, мотив и даже цель самого преступного поведения.

Нельзя не отметить, что именно мотив преступника главным образом также определяет, не только способ совершения, но и те средства, с помощью которых совершается преступное деяние, а также конкретные действия конкретного преступника, которые характеризуют его.

Мотив не является обязательной частью состава преступления, но имеет важнейшую роль в расследовании всех преступлений, в том числе преступлений в сфере компьютерной информации и требует установление цели конкретного преступника.

Во второй главе были подняты и изучены вопросы основных элементов объективной стороны компьютерных преступлений.

Одной из главных составляющих состава преступления – объект и предмет преступного посягательства в конкретном преступлении, на основании этого в дипломном исследование были даны понятия данных правовых элементов.

Согласно анализа состава преступления объектом данного вида преступления будет, если дословно трактовать норму закона, общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети.

Факультативный, то есть не обязательный, дополнительный объект при неправомерном доступе к ЭВМ, как следствие к компьютерной информации может иметь место в данной квалификации в зависимости от того вреда который нанесло само преступление.

Предметом будет выступать компьютерная информация, защищаемая законом. Список такой информации был представлен и обоснован на основании нормативно-правой базы российского законодательства.

Как говорилось ранее для привлечения к ответственности необходимо наличие всего состава преступления, согласно нормы УК РФ.

На основании этого для привлечения виновного лица необходим факт именно неправомерного действия.

В рамках дипломного исследования было установлено и доказано, что в данном случае это именно активное действие, а не бездействие, как это может быть в иных формах УК РФ.

Данный состав преступления не отличается от иных тем, что суд и до него следственные органы обязаны доказать наличие причинно-следственной связи между поступком и последствиями в виде копирования, уничтожения, модификации и т.д.

Данное условие обязательно так как данная составляющая обязательна для объективной сторону данного состава преступления и поэтому решение суда не может быть основано на догадках или предположениях, а должно иметь законное основание, доказанное в рамках правового поля.

Причинно-следственная связь была подробно проанализирована в данном исследовании.

Если в первых двух главах дипломного исследования мы проанализировали субъективную и объективную сторону преступлений в сфере компьютерной информации, выделили все условия наступления уголовной ответственности и все составляющие состава преступлений, предусмотренных уголовным законодательством, то заключительная глава раскрывает именно особенности проведения расследования преступлений в сфере компьютерной информации.

Первым делом были определены обстоятельства, которые необходимо установить и далее доказать в процессе расследования, далее были выделены особенности проведения отдельных следственных действий, с помощью которых проходит данное установление и доказывание.

Именно во время расследования вышеуказанных преступлений сотрудники правоохранительных органов, следователи и дознаватели, устанавливают все необходимые обстоятельства совершённого преступления.

Целью расследования является раскрытие всех подробностей совершенного преступления, установление всех фактов и привлечение виновным лиц к уголовной ответственности.

Именно на этой стадии формируется все уголовное дело, которое дальнейшем передаётся в суд.

Ещё одной задачей расследования является установление всех причин и условий совершенного преступления для дальнейшей профилактики аналогичных преступлений.

Можно подвести итог, что компьютерные преступления – это общественно опасные деяния, совершаемые в сфере компьютерной информации, признаваемые преступлениями уголовным законодательством, а именно главой 28 УК РФ, до данного федерального кодекса понятия «компьютерные преступления» не существовало.

Главной проблемой, возникающей при исследовании преступлений в сфере компьютерной информации, является условие наличия определенных знаний в области IT.

Преступления в сфере компьютерной информации требуют внимания и активного изучения криминологами, так как прогресс в сфере ЭВМ неотделим от прогресса в сфере данных преступлений.

Но главенствующей проблемой была и остается слабая подготовка специалистов, направленных на расследования данных преступлений.

Так как помимо первоначального специального обучения данные специалисты должны обучаться и проходить переподготовку регулярно, так как преступники быстро совершенствуют свои навыки и технические возможности.

Необходимо непрерывное развитие навыков и знаний, чтобы соответствовать профессиональной подготовки компьютерных преступников.

Помимо вопроса расследования данных преступлений, перед правовой системой стоит ещё одна задача - предотвратить преступления.

Для достижения данной цели в современной правовой системе России не достаёт нормативно-правовой базы, а также мешает отсутствие открытого подхода к статистике данных преступлений.

Все вышеназванные моменты приводят нас к выводу о сложности в проведении расследований, а в дальнейшем во время судебного процесса, так как технические сложности, недостаточная компетентность могут привести к нарушению принципов справедливости и законности судопроизводства.

После изучения данного вопроса, можно сделать вывод, что законодательство, регламентирующее нормы в области преступлений в сфере компьютерной информации, требуют в будущем внесения корректировок и дополнений для соблюдения всех основополагающих принципов уголовного судопроизводства, а также для положительной тенденции в сфере предотвращения преступлений данного вида.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ И ИСТОЧНИКОВ

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) [Электронный ресурс] / Компания «Консультант Плюс». – Дата обращения 10.05.2019
2. Уголовный кодекс Российской Федерации [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019
3. Уголовно-процессуальный Кодекс Российской Федерации [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019
4. Федеральный закон от 21.07.1993 № 5485-1 «О государственной тайне» [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019
5. Федеральный закон от 23.09.1992 №3526-1 «О правовой охране программ для ЭВМ и баз данных» [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019
6. Федеральный закон от 09.07.1993 № 5351-1«Об авторском праве и смежных правах» [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019
7. Федеральный закон от 20.02.1995 г. «Об информации, информатизации и защите информации» [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019
8. Постановление Пленума Верховного Суда РФ от 19.12.2017 N 51 "О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)" / Компания «Консультант Плюс». - Дата обращения 10.05.2019
9. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. N 48 г. Москва "О судебной практике по делам о мошенничестве, присвоении и растрате" / Компания «Консультант Плюс». - Дата обращения 10.05.2019

10. Определение Красноярского краевого суда по делу № 22-993/2019 / Компания «Консультант Плюс». - Дата обращения 10.05.2019Определение Ульяновского районного суда по делу № 22-680/2019 [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019

11. Анин Б. Защита компьютерной информации. - СПб.: БХВ-Санкт-Петербург, 2009.С. 7.

12. Батурин Ю.М. Проблемы компьютерного права. - М.: Юридическая литература, 2001. - С. 129

13. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. Б.П. Смагоринского. – М., 1996. – С. 74-92.

14. Викторов М. Законность в кредитно-банковской сфере // Законность. - 2007. № 11. С. 23

15. Гаджиев М. С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): Автореферат дисс. канд. юрид. наук. - Махачкала, 2009. - С. 9

16. Гульбин, Ю.А. Преступления в сфере компьютерной информации [Текст] : учебное пособие / Ю.А. Гульбин. – М.: «Статут» 2007. – 321 с.

17. Ермолович В. Ф. Научные основы криминалистической характеристики преступлений. - Минск: ЗАО "Веды», 2009. - С. 273

18. Информатизация и информационная безопасность правоохранительных органов. М.: Академия управления МВД России, 2005. - С. 94

19. Кадников Н.Г. Квалификация преступлений (теория и практика). М.: БЧ интернешнл Лтд., 2009. С. 18.

20. Коржов В.К. Право и Интернет: теория и практика [Текст] : учебное пособие / В. К. Коржов. – М.: Издательство БЕК, 2006. – 236 с.

21. Криминология: Учебник/ Под ред. В. н. Кудрявцева и В. Е. Эминова. - М., Юристъ, 2008. С. 305

22. Куринов Б.А. Научные основы квалификации преступлений. М.: МГУ, 2004. С.55.

23. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. - М.: Новый юрист, 2008

24. Крылов В.В. Информационные компьютерные преступления [Текст] : учебное пособие / В. В. Крылов. – М.: Юрид. Лит., 2005. – 240 с.

25. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 9.

26. Максимов, В.Ю. Компьютерные преступления (вирусный аспект) [Текст] : учебное пособие / В.Ю. Максимов. – М.: АО «Центр ЮрИнфор», 2006. – 210 с.

27. Научно-практический комментарий к Уголовному кодексу Российской Федерации. В 2 т. Т. 1. Нижний Новгород: Номос, 2010. С. 343.

28. Новое уголовное право России. Особенная часть: Учеб. пособие. М.: Зерцало, ТЕИС, 2006. С. 273.

29. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. - М.: Норма, 2008. С. 7

30. Панфилова, Е.И. Компьютерные преступления [Текст] : учебное пособие / Е.И. Панфилова. – М. : Феникс, 2007. – 254 с.

31. Пархомов В. А, Старичков М. В. О «троянском коне», хакере и уголовной статье // Правосудие в Восточной Сибири. - 2003. - № 2-3. - С. 105

32. Сальников, В.П. Компьютерная преступность [Текст] : учебное пособие / В.П. Сальников. – М. : Приор, 2004. – 192 с.

33. Селиванов Н. А. Проблемы борьбы с компьютерной преступностью // Законность. - 1993. - № 8; Вехов В. Б. Компьютерные преступления: Учебное пособие / Под ред. В. П. Тихомирова, А. В. Хорошилова. - М.: Финансы и статистика, 1996

34. Спирина С.Г. Криминологическая характеристика компьютерной преступности в России. - Краснодар: Российский государственный торгово-экономический университет, 2009. - С. 28.

35. Уголовное право. Общая часть: Учебник / Под ред. н.и. Ветрова, Ю.И. Ляпунова, М.: НОВЫЙ Юрист, КноРус, 2007. С. 217.

36. Уголовное право России. Части Общая и Особенная: учебник / В.А. Блинников, А.В. Бриллиантов, О.А. Вагин и др.; под ред. А.В. Бриллиантова. 2-е изд., перераб. и доп. М.: Проспект, 2015. 1184 с.

37. Уголовное право. Общая часть. / Под ред. И. Козаченко. — М.: ИНФРА, 2015. — 460с.