

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Юридический факультет

Кафедра

«Правоохранительная деятельность»

ДИПЛОМНАЯ РАБОТА

на тему

Особенности расследования преступлений в сфере компьютерной
информации

Студент

Соколов 10.06.2017
(подпись, дата)

Соколов Роман Владимирович
(ФИО полностью)

Научный руководитель

[подпись]
(подпись, дата)

Мурзина Л. И.
(фамилия, инициалы)

Нормоконтролер

[подпись] 21.06.17
(подпись, дата)

Битюцкий Е. В.
(фамилия, инициалы)

Рецензент заведующий кафедры уголовно-правовых дисциплин Пензенского филиала
ОЧУ ВО «Академия МНЭПУ»

[подпись]
(подпись, дата)

Климкин Н. С.
(фамилия, инициалы)

Работа допущена к защите (протокол заседания кафедры от 01.06.17 № 13).

Заведующий кафедрой

[подпись]
(подпись)

Свечников Н. И.
(фамилия, инициалы)

Работа защищена с оценкой удовлетв. (протокол ГЭК от 26.06.17 № 106).

Секретарь ГЭК

[подпись]
(подпись)

Шихалеева Т. В.
(фамилия, инициалы)

Пенза 2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

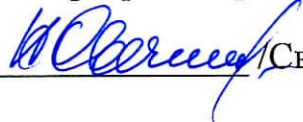
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Специальность: 40.05.02

«Правоохранительная деятельность»

УТВЕРЖДАЮ

Зав. Кафедрой «Правоохранительная
деятельность»  (Свечников Н. И./

ЗАДАНИЕ

по дипломной работе студента

Соколова Романа Владимировича

(фамилия, имя, отчество)

1. Тема работы Особенности расследования преступлений в сфере
компьютерной информации

2. Научный руководитель Мурзина Л. И. 

3. Дата выдачи задания 30.03.2017 г.

4. Срок сдачи студентом законченной работы 10.06.2017

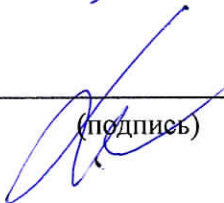
5. Перечень подлежащих разработке вопросов (поэтапно) _____

В работе необходимо рассмотреть понятие и криминалистическую
характеристику преступлений в сфере компьютерной информации,
особенности выдвижения версий и планирование расследования в сфере
компьютерной информации, особенности производства следственных

действий на первоначальном этапе производимых в ходе расследования преступлений в сфере компьютерной информации, особенности следственных действий производимых на последующем этапе расследования преступлений в сфере компьютерной информации.

Этап выполнения дипломной работы	Срок предоставления	Задание выдал (научный руководитель)	Задание принял (студент)
1.Введение	20.03.2017 г.	03.03.2017 г. 	03.03.2017 г. 
2.Понятие и криминалистическая характеристика преступлений в сфере компьютерной информации	20.03.2017 г.	03.03.2017 г. 	03.03.2017 г. 
3.Особенности следственных и иных действий осуществляемых в процессе раскрытия и расследования преступлений в сфере компьютерной информации	20.04.2017 г.	20.03.2017 г. 	20.03.2017 г. 
4.Заключение	10.05.2017 г.	20.05.2017 г. 	20.05.2017 г.

Научный руководитель


(подпись)

/ Л.И.Мурзина /

Оглавление

Введение.....	3
1. Понятие и криминалистическая характеристика преступлений в сфере компьютерной информации.....	6
1.1. Понятие и виды преступлений в сфере компьютерной информации.....	6
1.2. Криминалистические характеристики преступлений в сфере компьютерной информации.....	15
1.3. Предмет доказывания преступлений в сфере компьютерной информации.....	24
2. Особенности следственных и иных действий осуществляемых в процессе раскрытия и расследования преступлений в сфере компьютерной информации.....	33
2.1. Особенности выдвижения версий и планирование расследования, в сфере компьютерной информации.....	33
2.2. Особенности производства следственных действий на первоначальном этапе производимых в ходе расследования преступлений в сфере компьютерной информации.....	44
2.3. Особенности следственных действий производимых на последующем этапе расследования преступлений в сфере компьютерной информации.....	50
Заключение.....	61
Список литературы.....	65

Введение

Актуальность темы исследования обусловлена формированием и развитием в России информационного общества, современная жизнь которого базируется на массовом использовании информационных технологий, средств вычислительной техники и телекоммуникационных инфраструктур. Процесс информатизации общества сопровождается быстрым ростом компьютерной грамотности, особенно среди молодежи. Доступными стали средства компьютерной техники и практически любое программное обеспечение, в том числе вредоносное. Все эти обстоятельства привели к резкому обострению криминальной обстановки в информационной сфере общества. Суть в том, что новые технологии не лишены уязвимых мест, привлекающих внимание преступников. Наибольшую опасность представляют преступления в сфере компьютерной информации. Они, как терроризм, переросли национальные границы и стали международными, транснациональными, что в свою очередь, затрудняет ведение борьбы с ними, а безнаказанность провоцирует к совершению других преступлений и росту криминального «мастерства» в этой области. Преступления в сфере компьютерной информации затрагивают самые различные области жизнедеятельности общества, именно поэтому законодатель совершенно обоснованно отнес их к преступлениям против общественной безопасности и общественного порядка, отметив тем самым их общественную опасность.

По данным Министерства Внутренних Дел Российской Федерации было зарегистрировано в 2011 году 2698 преступлений в сфере компьютерной информации, а в 2012 году их число возросло до 2820 таких преступлений, в 2013 году снизилось и составило 2563 случаев, в 2014 году снова снизилось до 1739, в 2015 году все же возросло до 2382 таких преступлений, в 2016 снизилось до 1748. Но при этом необходимо подчеркнуть, что преступления характеризуются исключительно высоким уровнем латентности в сочетании с низким уровнем раскрываемости.

Эффективное противостояние преступлениям в сфере компьютерной информации, защита прав и законных интересов граждан, а также обеспечение информационной безопасности государства и юридических лиц возможно только на базе постоянно изменяемого комплекса всех мер защиты, включая и формирование криминалистических средств.

Следует отметить, что разработка теоретических основ расследования преступлений в сфере компьютерной информации сложна и имеет много аспектов на стыке права, теории информатики, производства и эксплуатации аппаратных средств компьютерных систем, сетей и иного сопряженного оборудования.

Новизна дипломной работы заключается в том, что рассмотрены новые обстоятельства, условия и факторы преступлений в сфере компьютерной информации; разработан новый подход к формированию типовых версий; разработаны основы криминалистической методики расследования преступлений в сфере компьютерной информации.

Объектом исследования является преступная деятельность, реализуемая в сфере компьютерной информации, а также деятельность по предотвращению и расследованию преступлений, совершаемых в сфере компьютерной информации в их взаимосвязи.

Предметом исследования являются закономерности механизма преступной деятельности, реализуемой в сфере компьютерной информации, закономерности обнаружения, фиксации, исследования, оценки и использования следов данного вида преступной деятельности.

Целью диплома является выявление закономерностей механизма преступной деятельности, реализуемой при совершении преступлений в сфере компьютерной информации и разработка на этой основе соответствующей методики расследования. Цели исследования достигаются решением следующих частных задач:

- определить уголовно-правовые и криминологические предпосылки формирования криминалистической характеристики преступлений в сфере компьютерной информации;
- сформулировать криминалистическую модель компьютерных преступлений;
- разработать методику построения типовых версий;
- дать характеристику каждого этапа криминалистической методики расследования преступлений в сфере компьютерной информации.

Методологическую основу исследования составляют методы системного, исторического и нормативно-правового, логико-семантического анализа; методы исследования эмпирических данных, а также методы моделирования и статистики.

Теоретическую базу исследования составляют научные достижения криминалистики, уголовного процесса, уголовного права и криминологии, заложенные в работах отечественных ученых-правоведов: В.А. Образцова, Н.П. Яблокова и др. Кроме того, в дипломной работе использовались работы ученых, занимающихся исследованием преступлений в сфере компьютерной информации, и специалистов информатики и информационного права: Ю. М. Батурина, В. Б. Вехова, В. В. Воробьева, О. А. Гаврилова, В. М. Глушкова, А.М. Копылова, В. В. Крылова, М. Ю. Максимова, В. Ю. Рогозина и др.

Основные положения, структуры работы:

Работа состоит из введения, двух глав, включающих разделы, заключения, списка использованной литературы.

1. Понятие и криминалистическая характеристика преступлений в сфере компьютерной информации

1.1 Понятие и виды преступлений в сфере компьютерной информации

В настоящее время компьютерные технологии в современном мире доросло до таких высот, когда социальные отношения в компьютерной сфере требуют уголовно-правового управления, так как в равной степени с положительными она создает и массу отрицательных явлений, связанных с преступлениями и средствами ЭВМ в различных сферах жизни государства. Опасность данных деяний увеличивается, когда такие преступления совершаются в отношении работы объектов жизнеобеспечения, систем защиты и атомной энергетики.¹

Впервые, задокументированным в международный реестр, рассматривающий компьютерные преступления, существовал случай в 1979 г., когда на одном предприятии было совершено похищение денежных средств с применением электронно-вычислительных машин. Преступление удостоилось внесения в международный реестр такой категории правонарушений.²

Другое правонарушение случилось в городе Горьком. В 1982 году все отделения связи переводились на централизованную автоматическую обработку принятых и оплаченных денежных переводов на электронной системе «Онега». В тоже время производился и обычный перевод. Существование автоматического и обычного денежных переводов предоставило возможность группе недобропорядочных сотрудников связи совершить хищение. Российские юристы уже давно поднимали вопрос о неопределенности законодательного закрепления правых отношений, происходящих из разных сфер использования средств автоматической обработки информации.

¹ Рослякова О. А. Далинин А. В. Зорина Е. А. Преступления в сфере компьютерной информации : учебное пособие. СПб. : Издательство, 2015. С. 12.

² Крылов В. В. Информационные компьютерные преступления : учебное и практическое пособие. М. : Норма, 2005. С. 85.

Важным моментом к реализации данных пожеланий было получение закона РФ в 1992 г. № 3523-1, этом закон содержал положения о том, что при выпуске под своими именами чужих программ для электронно-вычислительных машин или базы данных, либо противозаконное копирование, или распространение незаконных программ подлежит уголовной ответственности. Но все же глобальных преобразований в УК РСФСР как таковых и не было сделано.

Высоким показателем правовой системы, обуславливающей условия безопасности компьютерной информации, было появление в Уголовном кодексе Российской Федерации в 1996 году ряд статей, предусматривающих уголовное наказание за такие компьютерные преступления. Задействование в Уголовном кодексе главы о преступлениях в сфере компьютерной информации указывает о желании законодателя реализовать правовое регулирование в достаточно новой сфере, уменьшить отрицательные издержки недобросовестного обращения с электронно-вычислительными машинами и должной информацией.³

Федеральным законом от 07.12.2011 г. № 420-ФЗ, были внесены изменения в Уголовный кодекс Российской Федерации, составы преступлений, предусмотренные главой 28 УК, изложены в новой редакции, которые действуют до сегодняшнего дня. Данные преобразования определены некоторыми обстоятельствами. В первую очередь, интенсивное развитие информационно-коммуникационных технологий приводит к значительным переменам понятийного аппарата и уголовный закон должен в полностью отражать сложившиеся явления. Кроме этого, повышение, как количественного признака, так и разнообразие преступлений в сфере компьютерной информации требующей надобность уточнения объективной стороны составов соответствующих преступлений в уголовном законе, а также разграничение уголовной ответственности виновных лиц.

³ Сухарев А. Я. Компьютерные преступления : учебное пособие / А. Сухарев. М. : ПРИОР, 2012. С. 144.

Предметом преступления является компьютерная информация. Очень важно разграничивать информацию как значение обычной жизни так же и как правовую категорию. Такого рода информация, представляется как категория совершенного, она неощутима, не потребляема и не может быть объектом правовых отношений независимо к ее носителю, содержанию, отождествляющими признакам.⁴

Согласно Федеральному закону «Об информации, информатизации и защите информации» информация понимается как сведения о лицах, предметах, фактах, событиях и процессах несмотря от вида их представления.⁵

Введение органом законодательной власти в Уголовный кодекс РФ «компьютерная информация» является новейшим. Раньше в Отечественном законодательстве, регулирующем информационные правовые отношения, определения компьютерной информации не было. Это сделано, прежде всего, для разграничения данного объекта от других преступлений, предусмотренных другими разделами Уголовного кодекса Российской Федерацией.

Глава 28 УК содержит в себе три статьи, ст. 272 УК, ст. 273 УК и ст. 274 УК. Эти статьи охватывают исключительно малую часть общественно опасных действий, получивших символическое название компьютерные преступления. В юриспруденции особенно известные случаи, когда компьютер считается как техническое устройство совершения преступления в сфере информации или как предмет преступления. В первом случае компьютер считается предметом правонарушения против имущества и соответственно его похищение, уничтожение либо дефект оценивается по ст. 158 - 168 УК. Информационная программа не допускается быть предметом этой группы преступлений, так как она не является ни одним из главных признаков предмета преступлений против имущества, она не характеризуется физическим признаком. Связи с этим она ни как не может быть украдена, испорчена или уничтожена в данном смысле.

⁴ Крылов В. В. Информационные компьютерные преступления : учебное и практическое пособие. М. : Норма, 2005. С. 186.

⁵ Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 N 149-ФЗ (ред. от 07.06.2017) // СЗ РФ. 2006. № 31. Ст. 3448.

Ввиду этого выражается специфичность компьютерной информации. Электронно-вычислительная машина как техническое устройство совершения преступления понимается с такими средствами, как орудие преступления или как любое другое техническое устройство. В данном случае его использование присуще второстепенное значение, к пример: для хищений или сокрытия налогов. Такие преступления не являются в качестве независимых преступлений, а квалифицируются по соответствующим статьям Уголовного кодекса.⁶

Глава 28 рассчитана исключительно на те действия, которые покушаются на отношения по использованию, распространению и охране информации и информационных ресурсов. Нанесение неисправности информации реализуется при помощи компьютера как инструмент совершения преступления. Следовательно, таких компьютерных преступлений, как преступлений не стандартизированных в правовом смысле не существует.

Компьютерные преступления можно разделить на две огромные группы преступлений, связанные с внедрением в работу компьютеров и преступления, пускающие в ход компьютеры как вынужденные технические средства.

Базовая группа преступлений, связанная с вмешательством в работу компьютера. Неправомерный доступ к компьютерной информации является наиболее распространенный характер преступлений в сфере компьютерной информации. Кроме того, значится довольно опасным преступлением, которое обретает все более опасные масштабы. В связи с тем, что практически у каждого человека есть компьютер и выход в интернет, информация стала доступной практически всем пользователям персональных компьютеров. Данный характер преступления затрагивает внимание всего международного сообщества, доставляет вред государствам, и конкретным людям.⁷

⁶ Лядский В. В. Преступления в сфере компьютерной информации // Электронный вестник Ростовского социально-экономического института. 2014. № 2. С. 342.

⁷ Андреев Б. В. Расследование преступлений в сфере компьютерной информации : учебное пособие / Б. В. Андреев. М. : МАИК, 2013. С. 227.

Объектом неправомерного доступа к компьютерной информации как преступления значит права на информацию ее обладателя и других лиц, а также сохранность компьютерной информации, безупречная работа электронно-вычислительных машин.

С объективной стороны преступление является в неправомерном доступе к охраняемой законом компьютерной информации, содержащейся на электронном носителе или в ЭВМ повлекшем блокирование, копирование информации, уничтожение, или изменения, нарушение работоспособности ЭВМ, системы компьютерных машин. Под получение допустимости к компьютерной информации предполагается любая форма проникновения к ней с использованием ЭВМ, позволяющая что угодно делать с этой информацией. Безусловным отличием объективной стороны является существование причинной связи между несанкционированным доступом и наступлением предусмотренных статьей 272 УК последствий, поэтому любое совпадение момента сбоя в компьютерной технике, которое случилось с неисправностями или программными ошибками и неправомерного доступа не предусматривает уголовной ответственности.

Субъектом неправомерного доступа может быть только вменяемое физическое лицо, шестнадцатилетнего возраста, так же как и законный пользователь, не имеющий допуска к информации конкретной категории.⁸

Характеризуется статья 272 УК, как умышленная форма вины. Совершая данное преступление, лицо осознает, что незаконно вмешивается в компьютерную систему, догадывается о неизбежность наступления перечисленных в законе последствий, сознательно допускает их наступление или относиться к ним безразлично. Преступление характеризуется наличием прямого умысла или косвенного умысла. Неправомерный доступ к информации заключается не только в основном, но и квалифицированном составе. Квалифицирующими признаками являются совершение преступления группой

⁸ Евдокимов К. Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. 2016. № 1 С. 90.

лиц по предварительному сговору либо совершение его организованной группой, или лица имеющие возможность воспользоваться своим служебным положением, или имеющим доступность к ЭВМ, системе ЭВМ. Понятие совершения преступления в этом случае ничем не будет отличаться от общеустановленного.

Создание, использование и распространение вредоносных компьютерных программ, общественная опасность создания, использования или распространения вредоносных программ осуществляется тем, что вредоносные программы могут в самый неожиданный момент заблокировать работу компьютерной системы, что может привести к неблагоприятным последствиям.

Объектом данного преступления могут быть общественные отношения, которые обеспечивают безопасность информационных систем с точки зрения целостности содержащейся в них компьютерной информации от внешних воздействий. Говоря о целостности, подразумевают защиту данных от разрушения и изменения.

Объективная сторона преступления выражается в создании программ для электронно-вычислительных машин или внесении изменений в уже имеющийся программы, заранее приводящих к несанкционированному блокированию, уничтожению, копированию информации или изменению нарушению работы ЭВМ, системы ЭВМ; использовании таких программ; распространении этих программ или машинных носителей с данными программами.

Наиболее опасной компьютерной программой является, программу-вирус. Программа-вирус разработана специально для заражения компьютерной системы, она способная размножаться, подключаться к другим программам и при запуске может выполнять вредные различные операции: портить файлы и каталоги, исправлять результаты вычислений в отрицательную сторону, засорять или удалять память, создавать помехи при работе, выводить на экран монитора различные сообщения постороннего типа.

Преступление с субъективной стороны совершается как по необдуманности в виде легкомыслия, так и с косвенным умыслом в виде

безразличного отношения связанные другими последствиями. При выявлении прямого умысла в действиях виновного преступление рассматривает квалификации в зависимости от цели, которую виновный поставил перед собой. Лицо осознает, что программа, созданная им, зараженная «вирусом» либо внедряет «вирус» в чужую программу или распространяет и использует его и желает совершить эти действия. В этом случае действия, предусмотренные ст. 273 УК, оказываются лишь приемом для достижения данной цели.

Совершенное действие подлежит квалификации по совокупности совершенных преступлений.

Субъектом данного преступления является только вменяемое физическое лицо, достигшее ко времени совершения преступления 16-летнего возраста.

Закон не требует, чтобы это лицо занимало определенную должность, занималось определенной деятельностью, получило определенное образование.

Особенностью квалифицированного вида данного преступления является то обстоятельство, что в соответствии с законом субъективное отношение виновного лица к тяжким последствиям может характеризоваться только неосторожной формой вины.⁹

В науке уголовного права отмечается, что наиболее спорны в системе рассматриваемых преступлений нормы, содержащиеся в ст. 274 УК. Это связано с тем, что сегодня нет единых правил, определяющих порядок защиты информации, которые служили бы правовой основой для правильной квалификации деяния. Ряд исследователей предлагает принять подзаконный нормативно-правовой акт, который бы содержал правила, определяющие порядок защиты информации. По новой редакции ч. 1 ст. 274 УК категория «существенный вред» заменена на оценочное понятие «крупный ущерб». По мнению А.Н. Ягудина, законодателю следует отказаться от понятия «крупный ущерб», поскольку второе понятие шире первого и доказать причинение крупного ущерба почти нереально.

⁹ Сверчков В. В. Уголовное право. Особенная часть : Краткий курс лекций. М. : Юрайт, 2014. С. 140.

Установление уголовной ответственности за нарушение правил эксплуатации средств и хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей, а также правил доступа к информационно-телекоммуникационным сетям имеет целью предупреждение пользователями невыполнения своих обязанностей, влияющих на сохранность имеющийся и перерабатываемой компьютерной информации.

Непосредственным объектом преступления являются общественные отношения, обеспечивающие правильную, безопасную эксплуатацию ЭВМ, их системы, а так же сети.

Под эксплуатацией компьютерной системы нужно понимать правила, которые могут быть указанные компетентным государственным органом, так и правила технической эксплуатации, либо правила работы с программами, установленные изготовителями электронно-вычислительных машин и различного другого компьютерного оборудования, а так же правила установленные разработчиками программ, сетевыми администраторами, и правила, установленные владельцем компьютерной системы или по его компетенции (например, владелец может запретить использование не прошедших проверку на «вирусы» дискет).

К таким видам нарушения можно отнести несоблюдение общих средств защиты информации, а также нарушение режима эксплуатации ЭВМ. Выделяют два основных средства защиты: копирование информации и ограничение доступа к информации. Нарушение режима эксплуатации ЭВМ образуют, например, несанкционированные изменение, уничтожение или передача информации.

Статья 273 УК состоит в несоблюдении правил режима их работы, предусмотренных инструкциями, исходящими из технических характеристик, правил внутреннего распорядка, а также правил эксплуатации с компьютерной информацией, установленных владельцем информации либо законом или иным нормативным актом. Под охраняемой законом информацией следует понимать

информацию, изъятую из публичного оборота на основании закона, других нормативных актов, а также правил внутреннего распорядка, основанных на упомянутых нормативных документах. По общему правилу такая информация имеет гриф ограниченного пользования. Представляется, что частные фирмы, включая коммерческие банки, вправе устанавливать ограничительные грифы в целях сохранения коммерческой или банковской тайны.

Объективная сторона преступного нарушения правил эксплуатации средств и хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончного оборудования, а также правил доступа к информационно-телекоммуникационным сетям состоит из общественно опасного деяния в форме действия или бездействия, наступивших общественно опасных последствий и причинной связи между ними.

Субъект данного преступления - лицо, достигшее 16-ти лет, имеющее доступ к ЭВМ, системе ЭВМ.

Субъективная сторона характеризуется как умышленной, так и неосторожной виной преступления.¹

Итак, подводя итоги вышесказанному, под компьютерными преступлениями следует понимать установленные уголовным законом общественно опасные действия, в которых компьютерная информация является объектом преступного посягательства. В данном случае в качестве предмета или способа преступления может выступать компьютер, компьютерная информация, компьютерная система.

¹ Сычев Е. А. Алескеров В. И. Колокольчикова О. Н. Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации // ИСОМ. 2014. № 4. С. 353.

1.2. Криминалистические характеристики преступлений преступлений в сфере компьютерной информации

Криминалистическая характеристика преступлений в сфере компьютерной информации представляет собой систему типичных данных о преступлении, которые помогают выдвижению общих и частных версий на первоначальном этапе расследования, чем способствуют его раскрытию. Это сведения о предмете преступного посягательства, способе совершения преступления, следовой картине преступления и некоторых других. Ведущее значение, в структуре криминалистической характеристики преступлений в сфере компьютерной информации принадлежит описанию различных элементов личности преступника. Здесь необходимо отметить связь криминалистической и криминологической характеристики личности преступника.¹

В криминологии под личностью преступника понимается личность человека, который совершил преступление вследствие присущих ему психологических особенностей, антиобщественных взглядов, отрицательного отношения к нравственным ценностям и выбора общественно опасного пути для удовлетворения своих потребностей или не проявления необходимой активности в предотвращении отрицательного результата.

Преобразование криминологических сведений о структуре личностных характеристик через предмет криминалистики может иметь значение, для достижения целей расследования преступления.

Криминалистически значимые данные о личности преступника базируется на двух специфических группах информации. Первая, из которых включает в себя данные о личности неизвестного преступника по оставленным им следам как на месте преступления, в памяти свидетеле и по другим источникам с целью установления направления и приемов его розыска и

¹ Быков В. М. Черкасов В. Н. Преступления в сфере компьютерной информации : криминологические, уголовно-правовые и криминалистические проблемы. М. : Юрлитинформ, 2015. С. 228.

поймки. В большинстве случаев такая информация дает представление об общих свойствах определенной группы лиц, в числе которых может быть преступник, и реже - о неких качествах определенной личности. Такого рода сведения в целях быстрее определения и розыска преступника должны сверяться с криминалистическими данными о том, какие лица чаще всего совершают преступления расследуемого разряда.

Вторая группа включает в себя информацию, полученную с помощью изучения личности задержанного или обвиняемого с целью исчерпывающей криминалистической понимания личности преступника.

Криминалистической литературе неоднократно рассматривалась группирование лиц, совершающих преступления в сфере компьютерной информации. В их числе обычно выделяется группа лиц, именуемые «хакеры». Данные лица характеризуется в криминалистической литературе эксперты своего дела, использующие свои интеллектуальные способности для конструирования способов противоправных посягательств на компьютерную информацию. Иногда их еще называют компьютерными взломщик.¹

В зависимости от вида деятельности хакеры имеют следующие специализации: а) фриеры (используют альтернативные варианты оплаты телефонных услуг для обмана АТС); б) кардеры (оплачивают свои расходы с чужих кредитных карточек); в) сетевые хакеры (взломщики защиты провайдера) и др. К признакам совершения преступлений в сфере компьютерной информации хакерами относятся оригинальность способа и отсутствие тщательной подготовки к преступлению и его сокрытию.²

Термин «хакер» используемый в криминалистике, недостаточно точно характеризует рассматриваемую группу лиц, совершающих компьютерные преступления. Изучая специальную литературу, связанную с вопросами компьютерной безопасности, в ней обратил внимание на разделение всех

¹ Криминалистика : учебник / под ред. Яблокова Н. П. 3-е изд., перераб. и доп. М. : Юрист, 2005. С. 381.

² Подольный Н. А. Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий // Библиотека криминалиста. Научный журнал. М. : Юрлитинформ, 2013. № 5. С. 122.

квалифицированных-компьютерщиков на две группы уже упоминающихся «хакеров», а так же называемых «кракеров».

«Кракер» осуществляет проникновение в компьютерной системы, для цели получения несанкционированного доступа к чужой информации.

Мотивом этого могут быть разные: хулиганские побуждения, шалость, месть, промышленный и иной шпионаж корыстные побуждения.

Следовательно, группа лиц, совершающих преступления в сфере компьютерной информации, более правильно будет использовать термин «кракер».

Все «кракеры» в свою очередь подразделяется на всем известные три группы:

а) «Вандалы» - является самая распространенная группа преступников (благодаря широкому распространению вредоносных программ - вирусов, авторами которых они чаще всего являются). Их цель, составляет во взломе компьютерной системы для ее будущей порчи (уничтожение файлов, влекущего потерю сохраненной информации, удаления жесткого диска компьютера).

б) «Шутники» - наиболее безвредная с точки зрения убытка для компьютерной информации часть «кракеров». Их целью является взлом компьютерной системы и введение в нее разнообразных звуковых, шумовых, эффектов (дрожание, музыка, появление различных надписей, переворачивание изображения, различных картинок). По оценкам экспертов в Интернете - это наиболее распространенная группа «кракеров».

в) «Взломщики» - квалифицированные люди, реализующие взлом компьютерной системы с целью похищений денежных средств, промышленного и коммерческого шпионажа, хищений дорогостоящего программного обеспечения. Эта группа лиц обладает фундаментальными преступными навыками. Преступления, совершаемые ими носят серийный характер. Высоко квалифицированный «кракер» может действовать как для своих интересов, так и для интересов третьих лиц.

За исключение профессиональных взломщиков компьютерных сетей и программ «кракеров», в число лиц, совершающих компьютерные преступления выделяются лица, не обладающие серьезными познаниями в области программирования и компьютерной техники, обладающие лишь некоторые пользовательские навыки работы с компьютером. Как правило, их действия направлены на блокирование, уничтожение, изменение, копирование никак не охраняемой информации (например, если компьютер известен широкому кругу лиц и не имеет пароля доступа).¹

Предметом преступного посягательства при совершении компьютерных преступлений, перечисленных в главе 28 УК РФ, могут являться: средства защиты информации, и компьютерная информация, и так же компьютерные технологии, и программное обеспечение. В случаях, когда они сопутствуются совершением других, сопровождающих им преступлений, с другим предметом преступного посягательства, ответственность наступает по принципу идеальной совокупности.

Действующим уголовным законом введен ряд новых для нашего законодательства терминов, описывающих способы совершения преступлений в сфере компьютерной информации, необходимых для уяснения криминалистической сути преступного поведения данного рода.²

Компьютерная информация - это сведения, знания, а так же подбор команд, разработанных для использования в ЭВМ или регулирование ею, находящиеся в электронно-вычислительных машинах или на других носителях - распознаваемый элемент информационной системы, имеющей владельца, установившего правила использования компьютерной информации. С другой стороны, многие практические работники определяют компьютерную информацию не сами сведения, а форму представления в машиночитаемом виде, или совокупность символов, зафиксированная в памяти компьютера, или на машинном носителе (оптическом, магнитооптическом диске, магнитной

¹ Хаитжанов А. Генералова А. П. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации // НиКа. 2011. № 1. С. 219-221.

² Россинская Е. Р. Криминалистика : учеб. пособие для вузов. М. : ИНФРА-М. 2012. С. 163.

ленте или ином материальном носителе), и что при рассмотрении уголовных дел следует учитывать, что при определенных условиях и физические поля могут быть носителями информации.

Охраняемая законом информация - это информация ограниченного доступа, которая заключена в специальном правовом статусе, установленного соответствующими законами. По своему характеру она предназначена для конкретного круга пользователей, имеющих правовую возможность на ознакомление с ней. Данная информация может затрагивать различные аспекты жизни общества, государства, личности, конфиденциальные сведения о персональных данных, событий и обстоятельств жизни гражданина, сведения о мерах безопасности в отношении отдельных лиц, учетные данные об оружии, сведения, оперативно-розыскная информация составляющие государственную тайну.¹

Как правило, защиты информации устанавливается в отношении сведений, уполномоченными органами, относящихся к государственной тайне, на основании Закона Российской Федерации «О государственной тайне», в отношении документированной конфиденциальной информации - уполномоченным лицом или собственником информационных ресурсов на основании действующего федерального закона в отношении персональных данных - федеральным законом.²

Другой вид информации - это информация всеобщего пользования, для неограниченно широкого круга лиц. По данному характеру информации в всеобщего пользования ограничения доступа быть не может. Соответственно данная информация может находиться или на компьютерном носителе - магнитном диске, являющейся или составной частью электронно-вычислительной машины, или приспособлением ее периферийного устройства, дискете, магнитной ленте, магнитно-оптическом диске, компактные,

¹ Криминалистика : учебное пособие / Адельханян Р. А. Аминов Д. И. Федотов П. В. М. : Юнити-Дана, 2014. С. 138.

² О государственной тайне : Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.03.2015) // СЗ РФ. 1993. № 41. Ст. 4673.

переносные магнитные диски, или в электронно-вычислительной машине, под которой понимается совокупность аппаратно-технических средств и средств программирования, допускающая совершать операции над символьной и образной информацией в постоянном и оперативном запоминающих устройствах, являющихся неотъемлемой частью каждой электронно-вычислительной машины, либо в системе электронно-вычислительной машины. С объективной стороны совершение преступлений в сфере компьютерной информации осуществляется в основном путем активных действий. Исключение из правил составляет объективная сторона нарушения порядка использования электронно-вычислительной машины, системы электронно-вычислительных машин ст. 274 УК, которая может осуществляться и путем бездействия. Незаконные действия, предусмотренные ст. 272 и 274 УК, выражены как противоправные деяния с материальным составом, а действие, рассчитанное ст. 273 УК с формальным составом.¹

Субъективная сторона рассматриваемых правонарушений характеризуется только умышленной формой вины. Вместе с тем квалифицированные виды действий, предусмотренных ст. 273 и 274 УК, реализуется с двумя формами вины. Субъект преступления - вменяемое лицо, достигшее шестнадцатилетнего возраста. Преступления в сфере компьютерной информации представляют собой умышленные общественно опасные действие или бездействие, наносящие вред или создающие угрозу причинения вреда общественным отношениям, регулирующее безопасное производство, распространение или использование информации и информационных ресурсов либо их защиту.²

Уничтожение информации - полная физическая удаление информации или стирание таких ее элементов, которые воздействуют на преобразование существенных распознающих информации признаков. Действия людей в большей степени являются фактором особенно пагубным поражением

¹ Криминалистика. Базовый курс : учебник / под ред. А. Г. Филиппова. М. : Юрайт, 2015. С. 241.

² Сухарев А. Я. Компьютерные преступления : учебное пособие / А. Я. Сухарев. М. : ПРИОР, 2012. С.

информационные системы. Уничтожение информации получается в результате действия лиц, имеющих способность воздействовать на данную информацию. Причинная связь программно-технического характера, связанно со сбоями или недостатками в работе устройств и систем, встречаются достаточно реже, это связано с эксплуатационными ошибками или заблокированными элементами устройств.¹

Результат сильного воздействия на ЭВМ и ее элементы, повлекшие кратковременную или постоянную невозможность осуществлять различные процессы над компьютерной информацией, является блокированием.

Под изменением информации надлежит понимать введение в нее любых несанкционированных владельцем вмешательств, определяющих ее отличие от той, которую внес в систему и которой обладает владелец информационного ресурса.

Копирование информации без ясно выраженного разрешения собственника информационного ресурса неважно, каким способом выполнено копирования также является преступлением. Под нарушение работы ЭВМ следует понимать создание правонарушителем любой нетрадиционной ситуации с ЭВМ или ее устройствами, повлекшей блокирование, уничтожение, изменение либо копирование информации.²

Операции, которые воспроизводятся компьютерной техникой, материализуются, главным образом, над файлами, являющимися носителями информации. Для файлов присущие следующие стандартные свойства: тип информации (текстовая, числовая, графическая, программный код); месторасположение информации (описание места расположения на промежуточном или постоянном носителе); наименование; размер сохраненной информации (количество страниц, абзацев, строк, слов, символов и байт); время составления, время исправлений; атрибуты информации (скрытая, системная только для чтения). При передачи информации, при передаче файлов и в других

¹ Белкин Р. С. Курс криминалистики : в 3-х томах. Т. 3 : Криминалистические средства, приемы и рекомендации. М. : Юрист, 2012. С. 281.

² Балашов Д. Н. Балашов Н. М. Маликов С. В. Криминалистика : учебник. М. : ИНФРАМ, 2005. С. 303.

формах по системам, например электросвязи, они не лишаются своих персональных свойств. Именно поэтому в числе носителей сведений, составляющих государственную тайну, указаны и физические поля, в которых сведения, составляющие государственную тайну, находят свое описание в виде символов, сигналов, образов, процессов или технических решений.¹

Как правило, для совершения преступления в сфере компьютерной информации с использованием телекоммуникационных технологий и средств электросвязи, места совершения общественно правонарушения, не совпадает с местами в действительность наступления общественно опасных последствий. Мест таких может быть многократно. Они могут быть далеко между собой на большом расстоянии, располагаться в транспортных средствах, разных учреждениях, на отдельных участках местности, в том числе в разных странах и на различных континентах. Возможно это по причине неограниченного дальности действия, передвижения и разнообразие современных средств связи, главной частью которых является компьютерная информация. Из за этого, местом совершения преступления рассматриваемой категории разумно всего считать то средство передвижения, то отдельный участок местности или территорию любого учреждения, строение, государства, где были совершены общественно опасные деяния невзирая от места преступных последствий. В действительности невозможно привести точный список способов совершения преступления в сфере компьютерной информации, так как их содержание могут составлять самые различные действия, в виду от изобретательности, преступного умения и профессиональной деятельности преступника. Но, несмотря на разнообразность способов совершения преступления рассматриваемой категории их можно объединить следующим образом:

- эксплуатация либо распространение вредоносных программ для электронно-вычислительных машин или компьютерных носителей с такими родом программами;
- неправомерный доступ к компьютерной информации;

¹ Криминалистика : учебник / Агафонов В. В. М. : Юрайт, 2013. С. 343.

- подтасовка данных и управлением команд;
- нарушения правил эксплуатации средств ЭВМ, электросвязи, охраны компьютерной информации, а также хранения, передачи и обработки конфиденциальной компьютерной информации;
- многоцелевой методы.

Особенно часто применяются последующие способы подготовки, совершения и укрывательство преступления в сфере компьютерной информации:

- похищение компьютерных носителей информации, путем их замены;
- копирование конфиденциальной компьютерной информации;
- создание вредоносных программ для ЭВМ;
- распространение вредоносных программ;
- распространение компьютерных носителей, располагающихся в них вредоносные программы для ЭВМ;
- вписывание изменений уже в существующие программы;
- фальсифицирование входящих или исходящих электронных документов;
- фабрикация копий документов и их носителей;
- перехват компьютерной информации из канала электросвязи;
- использование недостатков программ для ЭВМ;
- деактивированные или обходной путь защиты компьютерной информации от незаконного доступа (путем подбора кода, доступа пароля);
- противозаконный доступ к компьютерным носителям;
- копирование, блокирование, изменение, повреждение компьютерной информации с помощью специально подходящих, разработанных, запрограммированных технических средств неофициального получения информации, уничтожение.

Все действия компьютерного преступника постоянно отличаются изощренностью и сопровождаются искусной замаскированностью. Хотя волнуются о ней больше те правонарушители, чьи устремленности направлены

на обогащение или носят стратегический характер. Остальные же считают средства компьютерной техники как развлечения, как предмет для проведения исследований и поэтому не устанавливают на начальном этапе своих противоправных действий целей. Их больше всего интересует содержательная сторона дела, это поиск более действенного способа посягательства на средства компьютерной техники, как на условного высокоинтеллектуального противника. Собственно эти люди создают в значительном большинстве своем новейшие способы совершения компьютерных преступлений, которыми затем в действительности используются другие правонарушителями.²³

Существенную значимость в структуре криминалистической характеристики компьютерных преступлений играют роль также проанализированные сведения о пострадавшей стороне, которые позволяют в полной мере квалифицировать личность преступника, повод совершения противоправных действий, проанализированных ранее и помогает точнее описать круг лиц, среди которых лучше всего искать преступника, и планировать розыскные мероприятия по нахождению важных доказательств по делу.

1.3 Предмет доказывания преступлений в сфере компьютерной информации

Согласно статье 272 УК РФ ответственность возникает связи с тем условием, если противоправный доступ к компьютерной информации последует за собой хотя бы одно из отрицательных последствий, блокирование, копирование информации, уничтожение, изменение или нарушение работы компьютеров, системы компьютера. Наиболее разумно следующий порядок следования решения основных задач при предмете доказывания данных правонарушений.

²³ Подольный Н. А. Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий // Библиотека криминалиста. Научный журнал. М. : Юрлитинформ, 2013. № 5. С. 116-119.

Установление факта неправомерного доступа к информации в компьютерной системе. Данный факт, как правило, устанавливаются первыми пользователи автоматической информационной системы, оказавшейся жертвой данного правонарушения. Сами факты незаконного доступа к компьютерной информации порой находят в результате ОРД ОВД.²⁴

Определить их можно в результате прокурорской проверки, при проведении инспектирования, следственных действий по данным уголовным делам. Представляется в надлежащих случаях при разбирательстве материалов, относящихся к обработки информации в ЭВМ системе, установление фактов незаконного доступа оперативно-розыскным аппаратом.

При обнаружении факта неправомерного доступа к информации в компьютерной системе нужно обнаружить все места, где по возможности располагаются компьютеры, имеющие неразделимую телекоммуникационную связь.

Установление места противоправного доступа в компьютерную систему, решается достаточно трудно, так как порождает конкретные трудности, потому что данных мест может быть множество. Такая задача решается и рассматривается проще в случае незаконного доступа к одному компьютеру, находящемуся в одном месте. Хотя при этом нужно учитывать, что информация на компьютерных носителях, возможно находится в другом помещении, которое тоже надо определить. Труднее определить то место, где непосредственное применения технологических средств удаленного незаконного доступа. К определению такого места надлежит привлекать специалистов.²⁵

Установление времени незаконного доступа. При помощи программ общего системного назначения в функционирующем компьютере обычно вводится текущее время, которое позволяет по определенной команде выводить

²⁴ Гаврилин Ю. В. Преступления в сфере компьютерной информации : квалификация и доказывание : учебное пособие. М. : Книжный мир, 2013. С. 245.

²⁵ Поляков В. В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АлтГУ. 2013. № 2. С. 114-116.

на экран монитора информацию о днях, недели, выполнения различных видах операции. Если эти данные прописаны, тогда при входе в систему, время на компьютере, какого угодно пользователя и время отдельной операции автономно сохраняется в оперативной памяти компьютера. С надлежащим учетом этого время возможно установить путем следственного осмотра ЭВМ, а так же распечаток. Его разумно производить с участием специалиста, так как малоопытные следователь может по неосторожности ликвидировать информацию, находящуюся в оперативной памяти ЭВМ. Время противозаконного доступа к компьютерной информации, возможно определить также путем допроса свидетелей из числа лиц, которые работали в данной компьютерной системе, выясняя у них, кто и в какое время осуществлял работу на компьютере, если оно не было зафиксировано автономно.

Вина возлагается на пользователя системы, а не на разработчика средств защиты несанкционированного доступа к компьютерной информации, ставшие причиной обнаружение при этом отклонений.

Несанкционированный доступ к ЭВМ системы ЭВМ или их сети, осуществляют, правонарушители с достаточно интеллектуальными способностями и высокой степенью квалификации в области информационных технологий. Поэтому поиск подозреваемых преступников стоит начинать с технического персонала пострадавших компьютерных систем.

Чем сложнее способ проникновения в компьютерную систему или сеть, тем легче выявить подозреваемых, поскольку круг специалистов, обладающих надлежащими способностями, обычно довольно ограничен.

Статья 273 УК «Создание, использование и распространение вредоносных компьютерных программ», представляет следующую последовательность решения основных задач при предмете доказывания таких преступлений.

Вредоносная программа, как правило, выявляется в момент, когда уже четко проявляются последствия ее применения, обнаруживается она также в процессе антивирусной проверки, совершаемые пользователем компьютерной

системы перед началом работы на ЭВМ, особенно часто практикуемой при использовании чужих дисков или других носителей.

Методов создания программ для ЭВМ очень много. Хотя разработывание вредоносных программ воплощается в деятельности обычно одним из двух нижеописанных способов.

Создание вредоносной программы осуществляет деятельность непосредственно на одном из рабочих мест автоматической информационной системы. Это, как правило, вуалируется под правомерную ежедневную работу на том или ином стадии разработчиком вредоносной программы, который в силу своих служебных обязанностей обладает доступом к информационной системе и функционирующей в ней информации, а временами и обладает паролями, скрывая преступных действий разработчик осуществляет путем уничтожения компрометирующих его данных.

Составление такой программы, ведется вне сферы непосредственной деятельности компьютерной системы, для воздействия на которую она предназначена. При этом правонарушителю нужны сведения о работающей в определенной системе информации, способах доступа к ней, методах ее защиты. Для их получения он создает связи с кем-то еще из пользователей системы или внедряет в нее свое доверенное лицо, чаще программиста.

В некоторых случаях вредоносная программа модифицируется путем внесения изменений в существующую программу. Наиболее обширно практикуются следующие способы совершения компьютерных противоправных деяний:

а) «Подмена данных» - наиболее простой и поэтому часто применяемый способ совершения преступления. Действия правонарушителей в этом случае направлены на изменение либо введение новых данных, которые осуществляются, при внесении или удалении информации;

б) «Троянский конь». Данный способ представляется в тайном установлении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы,

приступают делать новые, не предполагавшиеся законным пользователем программы, с одновременным сохранением прежней ее работоспособности.²⁶

В соответствии со ст. 273 Уголовного кодекса Российской Федерации под такой программой понимается «программа для ЭВМ, приводящая к несанкционированному блокированию, уничтожению, изменению или копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. «Троянский конь» - это усовершенствование «люк» с тем лишь отличием, что он «открывается» не только с помощью естественных действий самого правонарушителя, а автоматических - с применением специально подготовленной для этих целей программы без дальнейшего участия самого правонарушителя.

Большинство владельцев компьютерных систем могут обнаружить вредоносные программы при помощи антивирусных программ. Факт использования вредоносной программы может установить, посредственно при осмотре следующих документов, журналов учета доступа к вычислительной технике, регистрации пользователей компьютерной системы, неисправностей и ремонта, выполнение прописанных работ лицензионных соглашений и договоров на применение программными продуктами и их разработку книг паролей приказов и других документов, регулирующие работу учреждения и в частности, использование компьютерной информации. Учитывая, что эти документы могут находиться в электронной форме, на компьютерных носителях. К ознакомлению с ними рекомендуется привлекать специалиста. При проработки таких документов можно получить информацию о легальности того или иного программного обеспечения, системе организации работы учреждения, использования в ней информации, допустимость к информации и вычислительной технике, о круге лиц, находившихся в конкретный момент времени на объекте, где работает компьютерная система, или имевших доступ к компьютеру.

²⁶ Поляков В. В. Лапин С. А. Средства совершения компьютерных преступлений // Доклады ТУСУР. 2014. № 2 С. 162-164.

Важное значение для обнаружения фактов использования и передача вредоносных программ является своевременное производство информационно-технологической экспертизы, которая может установить, какие преобразования внесены в проверяемые программы, характер внесения изменений, какие последствия способны вызвать употребление и распространение вредоносных программ.

При предмете доказывания необходимо иметь в виду, что вредоносную программу может написать человек, располагающий навыками в обращении с компьютером и написании программ. Лучше всего вредоносные программы могут написать профессиональные программисты, но они, как правило, не участвуют в их рассылки.

Использовать и передавать вредоносные программы может любой человек, способный работать на персональном компьютере. Только наибольшую опасность представляют опытные компьютерные взломщики, высококвалифицированные специалисты в сфере компьютерных технологий.

Поиск лиц, причастных к использованию вредоносных программ, нуждается в не малых расходах времени и средств. В удобных случаях найти его можно по следам рук, оставленным на дисководах, клавишах и др. частях компьютера.

Значительный ущерб компьютерной системе может причинить нарушение правил их эксплуатации, что обычно приводит к накладкам в обработке информации, в итоговом счете нестабильности деятельности надлежащего учреждения.

При предмете доказывания по нарушению правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей необходимо, доказать факт нарушения конкретных правил, повлекший блокирование, уничтожение или преобразование охраняемой законом компьютерной информации и нанесение значительные повреждения вред. Кроме того, надлежит определить и привести доказательства, место и время несоблюдения правил эксплуатации

компьютера, характер компьютерной информации подвергшейся уничтожению, блокированию или изменению вследствие нарушения правил эксплуатации компьютерной системы или сети.

При обнаружении факта противоправного нарушения правил эксплуатации компьютера, которое нужно детально исследовать нормативные документы, включающие правила эксплуатации данной компьютерной системы, их характер и назначение, имея в виду, что подобающие правила сосредоточены на защиту информационной безопасности компьютерных систем или сетей. Они могут устанавливать порядок создания, обработки, сбора, хранения, поиска, накопления, распространения и понимания потребителю компьютерной информации, ее защиту.²⁷

Статья 274 УК главным образом предусматривает защищенную законом информацию, то есть информацию ограниченного доступа, которая по положению ее правового режима использования квалифицируется на информацию, относящийся к конфиденциальной, и государственной тайне. Собственно эти два вида информации, двигаются в компьютерных системах, нуждаются в особых средствах защиты.

Порядок обработки, накопления, защиты и обеспечение пользователю информации с ограниченным доступом допускается органами государственной власти или ее владельцем. Такие правила существуют, в государственных архивах, органах государственной исполнительной власти, в информационных системах в которых действует конфиденциальная информация или составляющая государственную тайну.²⁸

Факт нарушения правил эксплуатации компьютера случается известным, прежде всего, обычно пользователям и владельцам компьютерной системы, после выявления отсутствия надлежащей информации или ее значительного

²⁷ Кузьмин А. С. Альбом схем по криминалистической тактике и методике расследования отдельных видов преступлений : учебно-наглядное пособие. / А. С. Кузьмин. Минск. : Юрфак БГУ, 2013. С. 88.

²⁸ О государственной тайне : Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.03.2015) // СЗ РФ. 1993. № 41. Ст. 4673.

изменения, отрицательно отразившегося на деятельности предприятия, организации.

Необходимо разделять место нарушения правил и место наступления вредных последствий. Очень часто они не совмещаются, особенно при нарушении правил эксплуатации компьютерных сетей, которые, выступают в роли соединения ряда персональных компьютеров, находящихся в разных местах, порой на существенных расстояниях между собой.

При предмете доказывания очень важно определить, где находится обычная станция, работа которой проводилась с грубым нарушением правил информационной безопасности. В первую очередь нужно выявить места, где по плану развертывания сети, располагаются рабочие станции, владеющие собственными дисковыми, так как на них больше возможностей для преступных нарушений правил эксплуатации компьютерной сети.

Время наступления опасных последствий указывается по материалам служебного разбирательства, по окончании осмотра места преступления, а также путем допроса свидетелей и осуществлению судебных экспертиз.

Механизм несоблюдение данных правил обусловлено с технологией обработки информации на компьютере. Например, невыполнение требования об обязательном копировании информации для ее сохранения на случай ликвидации первого экземпляра, неправильное включение и выключение компьютера, использование посторонних переносных накопителей без предварительной проверки на наличие в ней компьютерного вируса.

Виновность лица, осуществившегося преступного нарушения правил эксплуатации компьютера, наступает на основании анализа результатов всех проведенных проверок. Надлежащие правила могут быть не соблюдены, как умышленно, также и неосторожно. Касательно последствий, вина может быть только неосторожной. При умышленном правонарушении исследуемых правил, ответственность по совокупности противоправных действий, например:

несоблюдение правил с целью повреждения компьютерной машины - по ст. 274 и 167 УК.²⁹

Факторов, помогающим совершению данного правонарушения, распознаются путем изучения как общего состояния защиты информационной безопасности в конкретной системе, так и факторов, непосредственно предопределивших расследуемое событие.

Предметом доказывания компьютерных преступлений с позиций криминалистики, их типизация и классификация позволяют установить связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

²⁹ Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ (ред. от 07.06.2017) // СЗ РФ. 1996. № 25. Ст. 2954.

2. Особенности следственных и иных действий осуществляемых в процессе раскрытия и расследования преступлений в сфере компьютерной информации

2.1 Особенности выдвижения версий и планирование расследования, в сфере компьютерной информации

При выдвижении версий связанных преступлениями в сфере компьютерной информации нужно иметь ввиду, что данные незаконные действия совершаются обычно группой лиц, хотя преступник может работать и в одиночку. В этом случае он сам является сотрудником либо обладает доступом учреждения, если же действует группа, то вернее всего один из группы правонарушителей является или сотрудником данного учреждения, или обладает свободным доступом к ЭВМ, может работать с компьютером, хорошо знает какая информация и где находится в компьютере. Интерес в большей части представляет информация, содержащая государственную тайну или коммерческую.³⁰

Чаще всего, как правило, информация копируется преступниками на компьютерный носитель, но не исключена возможность передать ее по сетям телекоммуникации либо перехват при помощи специальных технических средств. Украденная информация эксплуатируется в дальнейшем самими преступниками для продажи заинтересованным лицам.

Связи с этими обстоятельствами, следователь может выдвинуть и проверить следующие общие версии:

- правонарушение совершило лицо, осуществляющее деятельность в данном учреждении или лицо, имеющий свободный доступ к компьютеру;
- преступление совершено группой лиц по предварительному сговору или организованной группой с участием работника данного учреждения или лица,

³⁰ Методика расследования компьютерных преступлений : учебное пособие / М. Ш. Махтаев. М. : РосНОУ, 2012. С. 125.

обладающие свободный доступ к компьютеру и профессионально владеющего навыками работы с информацией;

- противоправное действие совершено лицом, либо группой лиц, не связанных с деятельностью учреждения и другие версии.

Данный список представляет собой общие следственные версии и зависит от конкретной ситуации, он может быть расширен.

Принципиальные схемы организации взлома защитных механизмов информационных систем достаточно схожи. Квалифицированный компьютерный взломщик обычно работает только после детальной предварительной подготовки. Преступник снимает квартиру на подставное лицо, подкупает работников учреждения, работников телефонной подстанции, для того, чтобы оградиться на случай поступления запроса от служб безопасности. Подкупают охрану из уже не действующих сотрудников правоохранительных органов.³¹

Признаки неправомерного доступа или подготовки к нему могут служить обстоятельства такие, как возникновения в компьютере неверных данных или не обновление в течение длительного времени в системы кодов, либо других защитных приемов, либо многократные сбои во время работы компьютеров, а так же частые претензии клиентов компьютерной системы.

Идентифицировать место и время прямого применения технических средств дистанционного неправомерного доступа, не содержащихся в данной информационной системе, в действительность получается достаточно трудно. Для определения данных нужно привлечь высококвалифицированных специалистов. Метод несанкционированного доступа можно установлен через выполнение информационно-технической судебной экспертизы. Разумно препоставить эксперту всю констуктивную документацию на изучаемую систему, либо данные о ее подтверждении.

³¹ Кузьмин А. С. Альбом схем по криминалистической тактике и методике расследования отдельных видов преступлений : учебно-наглядное пособие. / А. С. Кузьмин. Минск. : Юрфак БГУ, 2013. С. 78.

Несанкционированный доступ к секретной компьютерной системе, представляет собой технически довольно сложным действием. Осуществить такое под силу только специалистам, обладающие высокой квалификацией.³²

Связи с этим розыск предполагаемых преступников нужно приступать с технического штата пострадавших компьютерных систем. Практика указывает, чем изощренней в техническом плане способ вторжения в компьютерную систему, тем проще определить подозреваемого, так как круг профессионалов имеющих соответствующие способности, весьма ограничен.

При расследовании нарушения правил эксплуатации компьютеров, нужно доказать факт нарушения конкретных правил, повлекший блокирование, уничтожение, или изменение компьютерной информации и доставивший конкретный вред.

Кроме этого, следовательно нужно понимать, что может быть много особенностей, которые нужно учитывать при расследовании отдельных следственных действий.

Если следователь обладает информацией, что на объекте обыска располагаются средства компьютерной техники, раскодировка данных с которых возможно получить подтверждение по делу, он обязан заблаговременно подготовиться к их изъятию. Нужно привлечь во время обыска профессионала по компьютерной технике. По приезду на место обыска нужно в кратчайшие сроки осуществить меры сохранности компьютеров и находящихся на них данных и нужной информации. Для этого необходимо не позволять, никому из лиц, действующих на объекте обыска либо присутствующих по другим поводам, дотрагиваться к компьютерам и не позволять кому бы то ни было из штата, выключать электроснабжение учреждения. После осуществления срочных мер, можно начинать обыск сооружения и изъятие средств компьютерной техники.

Надлежит принять во внимание следующие неблагоприятные факторы:

³² Вехов В. Б. Ковалев С. А. Теоретические и прикладные проблемы применения программного обеспечения специального назначения при расследовании преступлений в сфере компьютерной информации // Вестник ВИ МВД России. 2012. № 1. С. 38-41.

- вероятные попытки со стороны штата испортить компьютеры с целью ликвидации информации и ценных данных;

- вероятное нахождение на компьютерах специализированных средств защиты от неправомерного доступа, которые, не унаследовав в определенное время специальный код, автоматически ликвидирует всю данную информацию;

- неизменное модернизирование компьютерной техники, результат чего возможно существование на объекте программно-технических средств, неизвестных следователю.

В целях, что бы ни допустить пагубных последствий, следователь должен соблюдать следующие указания:

- перед выключением питания правильно закрыть все рабочие программы, а в подозрительных случаях - отключить компьютер;

- при нахождении средств защиты компьютера от незаконного доступа предпринять меры к выявлению ключей доступа;

- правильно выключить питание всех компьютеров, расположенных на объекте;

- не пробовать на месте, изучать информацию, находящуюся в компьютерах;

- в обременительных случаях не просить помощи у персонала, а пригласить специалиста, не увлеченного в итоге дела;

- нужно конфисковать все носители компьютеров, найденные на объекте;

- также изъять все записи, касающиеся работы с компьютером;

- при конфискации средств компьютерной техники нужно гарантировать выполнение условий действующего уголовно-процессуального законодательства. На этот случай надлежит сосредоточить внимание свидетелей на всех совершаемых действиях и их итогах. Кроме того, нужно опечатать компьютеры так, чтобы не допустить право работы с ними. При опечатывании компьютеров надлежит положить один лист бумаги на разъем

электропитания второй - на переднюю панель и закрепить их края. На листах должны расписаться следователь, свидетели (понятые) и представитель штата.³³

К сожалению, практика работы показывает, что данных предложения по большому счету, следователями не используются. В итоге, неправильной конфискации средств компьютерной техники полученная информация часто не может быть доказательством в судебном процессе.

В России большая часть уголовных дел по компьютерным правонарушениям так и остаются нераскрытыми. Не из-за того, что некачественно осуществляет свою деятельность следователь либо российские предприятия скупаются на защите компьютерных сетей. К несчастью, при первоклассном техническом оборудовании и детальной подготовке противоправного компьютерного деяния схватить правонарушителя очень непросто.

Выявлять противоправные действия в сфере компьютерной информации непросто, так как порой правонарушители применяют различные уловки, скрывают свои противозаконные деяния многократными объективными и субъективными факторами. Список безотлагательных следственных действий и оперативных мероприятий, порядок их выполнения будет измеряться определенной следственной ситуацией, в которой устанавливается следствие.³⁴

Следственная ситуация обладает в первую очередь количеством и точностью первоначальной криминалистически ценной информации, находящиеся в распоряжении следователя и оперативного сотрудника.

Причинами и поводами для возбуждения уголовных дел в большинстве случаев является:

- заявления граждан;
- сообщения руководителей компании, организаций, учреждений и должностных лиц;

³³ Головин А. Ю. Проблемы и пути совершенствования методик расследования отдельных видов преступлений // Известия ТулГУ. Экономические и юридические науки. 2014. № 3. С. 3-10.

³⁴ Осипенко А. Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник ВИ МВД России. 2016. № 3. С. 83-88.

- Информация, приобретенная вследствие осуществления оперативно-розыскных мероприятий;
- непосредственное выявление следователем, прокурором или судом признаков правонарушения;
- письма, статьи, заметки, размещенные в СМИ, а также в сети Интернет.

Перед возбуждением уголовного дела производится предварительная проверка сведений, поступивших в правоохранительные органы. Вследствие с этим, следователь может заранее изучить полученные по делу материалами, наряду с оперативным сотрудником избрать в тактическом плане наиболее наилучший момент для возбуждения дела, а также выяснить характер и очередность первоначальных следственных действий, управленческих и иных действий. Успех расследования противоправных действий в сфере компьютерной информации в значительной степени гарантирует:

- скорость и решительность, активность следователя и оперативного сотрудника в первые часы производства по делу;
- сплоченное сотрудничество с разными подразделениями правоохранительных органов;
- присутствие профессионала в области компьютерной обработки информации.

Во время первоначальной проверки материалов при решении вопроса о возбуждении уголовного дела следователь обязан, достичь четкого и полного представление о предмете преступления, месте его расположения и условиях защиты, так же о характере деятельности и структуре объекта, где именно было совершено противоправное деяние, так же об специфики технологии производства, аналогично исследовать определенные условия деятельности объекта, представленный порядок учета и отчетности, информационные и другие тактико-технические особенности практикуемой компьютерной техники, организацию защиты. Нужно отлично разбираться в служебных обязанностях лиц, обладающих прямыми или косвенными отношением к

орудиям производства и компьютерной информации, которые стали предметом преступления.

К стандартным признакам совершения и маскировки противоправных действий в сфере компьютерной информации относятся:

- появление в компьютерах, системе компьютеров или их сети поддельных данных;
- неправомерное исправление структуры файловой системы, программного обеспечения и расположение компьютеров, системы компьютеров;
- нестандартные проявления в работе программного обеспечения;
- многократные сбои в работе оборудования;
- претензии клиентов на оказание неудовлетворительного доступа к компьютерам, системе компьютеров или их сети, либо компьютерной информации;
- сверхурочная работа некоторых работников на компьютерах, в системе компьютеров, несоблюдение указанного графика их работы;
- нерегламентированный доступ к компьютерам, системе компьютеров, либо к компьютерной информации отдельных субъектов;
- несоблюдение правил работы с компьютерной информацией и неразрешенной махинацией с ней;
- излишний интерес индивидуальных клиентов или сотрудников к материалам чужих распечаток и компьютерной информации конкретной категории;
- случаи перезаписи конкретных данных и компьютерной информации без весомых запрашиваемых на то причин;
- пользование на рабочем месте и вынесение с работы персональных компьютерных носителей информации под разными поводами;
- изучение мусорных корзин с технологическими отходами компьютерной обработки информации;

- случаи потери секретной информации или выявление тайных устройств ее получения;
- несоблюдение указанных правил выполнения документов при работе с компьютерами, системой компьютеров, их сетью либо компьютерной информацией;
- формирование копий конкретной категории данных и компьютерной информации, не рассчитанных технологическим процессом;
- противоречивость данных, хранимых в исходных документах, данным машинограмм и другим поздним по времени создания документам;
- сомнительное отношение одного и того же пользователя к данным и компьютерной информации конкретной категории.³⁵

Для того, чтобы досконально понять особенности деятельности потерпевшего, следователю и оперативному работнику нужно изучить надлежащую справочной литературой, исследовать ведомственные нормативные правовые акты. Важную роль играют консультации со специалистами. Для этого могут быть приглашены лица, имеющие обязательные знаниями и опытом для консультаций по делу. Эти высококвалифицированные работники, выполняют свою деятельность в сфере информатизации и охраны информации. Наилучшими сотрудниками считаются, это сотрудники ФСТЭК, так же сотрудники центров защиты информации, либо оперативно-технических подразделений правоохранительных органов, либо подразделений «К» при БСТМ МВД Российской Федерации, или специалисты межрегиональных центров защиты информации, осуществляющие свою деятельность на базе высших учебных технических заведений.

Для преступлений в сфере компьютерной информации характерны три обстоятельства первоначального этапа расследования:

³⁵ Соловьев Л. Н. Вредоносные программы. Расследование и предупреждение преступлений. М. : Собрание, 2014. С. 119.

- данные о причинах зарождения общественно опасных деяний, о способе осуществления данных преступлений и личности преступника отсутствуют.

- имеются данные о мотивах появления преступления, приме его осуществления, но нет сведений о личности преступника.

- известны причины возникновения правонарушения, способы его осуществления и маскировки, личность правонарушителя и иные ситуации.

Следственные действия планируются и исполняются следующими следственными действиями, оперативно-розыскными и иные мероприятия:

а) принятия пояснений заявителя или лиц, на которых указано в первоначальной информации как на вероятных очевидцев;

б) обращение и информирование требуемых высококвалифицированных экспертов для помощи в осмотре места происшествия;

в) осмотр места происшествия;

г) выполнение оперативно-розыскных действий в целях выяснения причин осуществления правонарушения, нахождение лиц, виновных в его совершении, установление рабочего места злоумышленника, выявление следов и иных вещественных доказательств;

д) исследование справочной литературы, ведомственных нормативно правовых актов, инструкций и регламента работы с компьютерной информацией, а также консультации относящихся к делу специалистам;

е) выемку и дальнейший осмотр отсутствующих документов, определяющую производственную процедуру, во время которой по доступным данным осуществлены преступные действия, а кроме этого-орудия, при помощи которых они, вероятно, были сделаны;

ж) допросы подозреваемых или свидетелей, отвечающих за данный часть работы, определенную производственную операцию и защиту секретной информации;

з) обыски на рабочем месте и по месту жительства подозреваемых;

и) установление экспертиз - программно-технической, технической, бухгалтерской, радиотехнической, полимерных материалов и изделий данных материалов.

Последующие действия предопределяются с учетом вспомогательной информации, приобретенной при производстве вышеуказанных действий.

При существовании третьей следственной обстановки нужно:

- исследовать полученные материалы с точки зрения их полноты, выполнения норм уголовно-процессуального законодательства и правильности их предоставления в органы предварительного следствия. При надобности надлежит провести меры к получению отсутствующей процессуальной информации;

- разрешить вопрос о возможности задержания правонарушителя с личным и об обязательных в связи с этим мероприятиях;

- личный обыск задержанного предполагаемого преступника;

- осмотр места происшествия с содействием относящихся к делу предварительно вызванных экспертов;

- допрос задержанного предполагаемого преступника;

- обыски на рабочем месте и по месту жительства задержанного предполагаемого преступника;

- определение связей задержанного и лиц, имеющих отношение к осуществлению преступления;

- допрос очевидцев;

- выемка и осмотр следующих вещественных доказательств и документации;

- допрос лиц, упомянутых в документации, предоставленных в следственные органы, как допустивших нарушения правил, отвечающих за определенную часть работы по фактам указанных нарушений;

- освоение, а при потребности производство выемки нормативно правовых актов и документов, квалифицирующих регламент и координирование работы в данном подразделении с секретной информацией, с

бланками жесткой отчетности, компьютерной информацией, компьютеров, системой компьютеров, их сетью и т. п.;

- допрос свидетелей, участвующих в производственных операциях или подозреваемых в операциях с правонарушителем;

- исследование накопленной информации и определение вопроса о надобности направления судебных экспертиз, контрольной проверки или проведение инвентаризации.

В последовательность данных выше следственных действий, оперативных и управленческих мероприятий, возможно внести поправки в зависимости от изменения случаев.³⁶

Все следственные действия по делам о преступлениях в сфере компьютерной информации воспроизводятся с жестким соблюдением с правилами, указанными настоящим уголовно-процессуальным законодательством, но применительно последующих преимущественных особенностей:

- следственное действие обязано быть своевременно специализировано и до мельчайших деталей рассчитано; в следственной операции обязаны участвовать высококвалифицированные специалисты, отчетливо исполняющие свои задачи, права и обязанности;

- понятые обязаны иметь минимальные требующие специальные знания в сфере обработки компьютерной информации, следователь и специалисты - знаниями в части полной сохранности компьютерной информации, находящейся на изымаемом компьютере; для осмотра, обыска и выемки компьютерной информации, заблаговременно обязаны быть подготовлены нужные материалы.

³⁶ Кузьмин А. С. Альбом схем по криминалистической тактике и методике расследования отдельных видов преступлений : учебно-наглядное пособие. / А. С. Кузьмин. Минск. : Юрфак БГУ, 2013. С. 56.

2.2. Особенности производства следственных действий на первоначальном этапе производимых в ходе расследования преступлений в сфере компьютерной информации

Допрос подозреваемого и потерпевшего - пожалуй, одно из распространенных следственных действий. Он способом получения, и такого вида доказательств, как названных лиц. По допрос имеет определенное с опросом, объяснений и интервью. он существенно от них правовой и всего установленным для него процессуальным порядком.

Важнейшим условием ценности любого лица его правдивость, обеспечивается прежде добровольностью и долгом показания говорить правду только правду. К допросу обвиняемого приступить сразу же после предъявления обвинения и разъяснения его прав. Допрос собственно и является прежде всего способом обеспечения одного из важнейших прав обвиняемого - давать объяснения по предъявленному обвинению в интересах собственной защиты. Он в меньшей мере необходим и следователю, для которого служит способом получения доказательства - показаний обвиняемого и тем самым одним из важных способов проверки правильности сформулированной по делу версии обвинения. Допрос обвиняемого является также одним из средств, с помощью которого его изобличают в совершении преступления.

Допрос обвиняемого надо начинать с вопроса - признает ли он себя виновным. Затем обвиняемому предлагается дать показания по существу обвинения.

Следует,однако,иметь в виду, что дача показаний для обвиняемого - это его право, а не обязанность. Поэтому обвиняемого, в отличие от свидетеля и потерпевшего, нельзя перед допросом, а также в ходе допроса предупреждать

об уголовной или какой-либо иной ответственности за отказ от дачи показаний, равно как и за дачу ложных показаний.

По смыслу ст. 51 Конституции РФ обвиняемый и подозреваемый вообще вправе отказаться от дачи показаний и не отвечать ни на какие вопросы либо отвечать на них сугубо добровольно. Потому при возникновении у суда сомнений относительно добровольности данных этими лицами показаний в ходе предварительного следствия или дознания обязанность доказывания, что показания действительно были даны добровольно, следовало бы возлагать на органы уголовного преследования, получившие такие показания.³⁷

О каждом допросе обвиняемого составляется протокол с соблюдением требований, предусмотренных ст. 141, 142 и 151 УПК. После дачи обвиняемым показаний, в случае его просьбы, ему предоставляется возможность изложить свои показания собственноручно.³⁸

Обычно по уголовным делам рассматриваемой категории при допросе обвиняемого необходимо выяснить обстоятельства подготовки и совершения преступления, алгоритм функционирования вредоносной программы, а также на какую информацию и как она воздействует.

По делам данной категории при допросе подозреваемого требуется установить уровень его профессиональной подготовленности как программиста, опыт его работы по созданию программы конкретного класса на данном языке программирования, знание им алгоритмов работы программ, подвергшихся неправомерному воздействию.

Также необходимо выяснить места его жительства, работы или учебы, профессию, взаимоотношения с сослуживцами, семейное положение, образ жизни, сферу интересов, привычки, наклонности, круг знакомых, навыки в программировании, ремонте и эксплуатации средств вычислительной техники, какими средствами вычислительной техники, машинными носителями,

³⁷ Конституция РФ от 12.12.1993 (ред. от 30.12.2008) // Российская газета. 1993. № 237.

³⁸ Уголовно-процессуальный кодекс РФ от 18.12.2001 № 174-ФЗ (ред. от 12.06.2017) // СЗ РФ. 2001. № 52. Ст. 4921.

аппаратурой и приспособлениями он располагал, где, на какие средства их приобрел и где хранил.

Допрос свидетелей, потерпевших и необходимо со рассказа о всем, что им по делу. свободный рассказ, может задать вопросы.

При расследовании неправомерного к информации допросов и пользователей системы установить, ли в данной компьютерной меры от доступа к определенным файлам. лиц, компьютерную систему, установить, кто запускал программу, было ли это каким-либо способом. Следует также выяснить, кто программированием, или на компьютерных курсах.³⁹

Когда производится расследование создания, и вредоносных для ЭВМ, то при свидетелей из представителей стороны следует выяснить, информация неправомерному воздействию, ее назначение и содержание, как доступ к ЭВМ, ЭВМ или их сети, кодам, и компьютерной информации, как организована противовирусная защита, образом учет компьютерной системы.

При нарушения правил ЭВМ, ЭВМ или их сети, а для установления конкретного эксплуатации ЭВМ, которого к вредным последствиям, целесообразно всех лиц, на ЭВМ и обслуживавших оборудование в период времени. В необходимых к в привлекается специалист.

При осмотре места происшествия в штат следственно-оперативной группы в зависимости от определенной следственной обстановки, кроме следователя, соответственно обязаны входить:

- специалист-криминалист, обладающий особенностями работы с отпечатками преступления определенной группы;
- сотрудник ФСТЭК;
- специалист по сетевым технологиям;
- специалист по системам электросвязи;
- оперативные сотрудники (отдела «К»);

³⁹ Шеметов А. К. О понятии виртуальных следов в криминалистике // Российский следователь. 2014. № 20. С. 52-54.

- участковый оперативник, осуществляющий свою работу на данной территории;
- инспектор отдела вневедомственной охраны;
- специалист для выполнения цветной фотосъемки следственного действия.

При потребности в группу могут быть включены непричастные в деле специалисты, обладающие знаниями спецификой работы осматриваемого объекта.

Осмотр сетевой вычислительной техники чаще всего приводит к надобности их изъятия для последующего экспертного исследования или приобщения к делу в качестве вещественного доказательства.

В протоколе осмотра сетевой вычислительной техники записывают:

- его назначение, конфигурацию, цвет, марку и заводской номер;
- назначение, цвет и другие индивидуальные признаки соединительных и электропитающих проводов; состояние на момент осмотра;
- техническое состояние - целостность корпуса, внешний вид, комплектность, тип используемого машинного носителя информации, наличие расходных материалов;
- тип источника электропитания, его тактико-технические характеристики и техническое состояние;
- наличие заземления сетевой вычислительной техники и его техническое состояние; наличие и техническая возможность подключения к сетевой вычислительной техники периферийного оборудования или самого СВТ к такому оборудованию либо к каналу электросвязи; имеющиеся повреждения, не предусмотренные стандартом конструктивные изменения в архитектуре строения сетевой вычислительной техники, его отдельных деталей, особенно те, которые могли возникнуть в результате преступления, а равно могли спровоцировать возникновение происшествия;
- следы преступной деятельности;

- расположение сетевой вычислительной техники в пространстве, относительно периферийного оборудования и других электротехнических устройств;

- точный порядок соединения сетевой вычислительной техники с другими техническими устройствами;

- категорию обрабатываемой информации;

- наличие или отсутствие индивидуальных средств защиты осматриваемого сетевой вычислительной техники и обрабатываемой на нем информации от несанкционированного доступа и манипулирования.

Если на момент осмотра сетевая вычислительная техника находится в рабочем состоянии, необходимо детально описать:

- расположение его рабочих механизмов и изображение на его видеоконтрольном устройстве;

- основные действия, производимые специалистом при осмотре сетевой вычислительной техники.

Осмотр машинного носителя и компьютерной информации проводят по принципу «от общего к частному». Вначале описывают внешние индивидуальные признаки носителя: его, заводской и индивидуальный номер, название, размер, цвет, вид, тип, марка, на ней, наличие или отсутствие физических повреждений корпуса и следов на нем, наличие наклейки и надписей, положение элемента защиты от стирания компьютерной информации. Затем переходят к осмотру компьютерной информации, содержащейся на машинном носителе информации.⁴⁰

Перед началом ее осмотра необходимо указать в протоколе следственного действия:

- индивидуальные признаки используемого для осмотра средства электронно-вычислительной техники и основные реквизиты его программного обеспечения;

⁴⁰ Соловьев Л. Н. Вредоносные программы. Расследование и предупреждение преступлений. М. : Собрание, 2014. С. 124.

- юридические реквизиты программы, с помощью которой сетевой вычислительной техники и его программное обеспечение в присутствии понятых было тестировано специалистом на предмет отсутствия вредоносных программно-аппаратных средств.

После этого на указанный предмет проверяется и осматриваемая компьютерная информация.

Анализируя содержащуюся на осматриваемом носителе компьютерную информацию, надо установить сведения, имеющие отношение к расследуемому событию. Для оптимизации процесса осмотра большого объема информации можно применять функции автоматизированного поиска по конкретному реквизиту, входящие в состав стандартного программного обеспечения компьютеров. Ход осмотра должен дополнительно фиксироваться на цветной фотопленке. При обнаружении следов преступления необходимо сделать распечатку всей или части компьютерной информации и приложить ее к протоколу следственного действия с указанием в протоколе индивидуальных признаков использованного для этого печатающего устройства.⁴¹

В протоколе осмотра, также необходимо отразить:

- наличие, индивидуальные признаки защиты носителя от несанкционированного использования;
- признаки материальной подделки МНИ и его защиты; внутреннюю спецификацию носителя - серийный номер или метку либо код;
- размер области носителя свободной от записи и занятой под информацию;
- количество и номера сбойных зон, участков, секторов, цилиндров кластеров;
- количество записанных программ, каталогов, файлов;
- наличие скрытых или ранее стертых программ и их реквизиты.

⁴¹ Мусаева У. А. Специфика проведения следственного осмотра по делам о преступлениях в сфере компьютерной информации // Известия ТулГУ. Экономические и юридические науки. 2013. № 4. С. 297-299.

2.3 Особенности следственных действий производимых на последующем этапе расследования преступлений в сфере компьютерной информации

Готовясь к проведению обыска, следователь должен решить, что и где он будет искать. Для этого необходимо тщательно изучить обстоятельства дела и собрать ориентирующую информацию о предмете обыска, месте его проведения и личности обыскиваемого. По делам о преступлениях в сфере компьютерной информации предметом обыска могут быть не только разнообразные сетевая вычислительная техника, машинные носители и содержащаяся на них компьютерная информация, но и документы, средства электросвязи, разработанные и приспособленные специальные технические устройства, бытовые электротехнические устройства и оборудование, материалы и инструменты.

В ходе обыска следует обращать внимание на литературу, методические материалы и рекламные проспекты по компьютерной технике, обработке, защите, передаче и негласному получению компьютерной информации, а также на видеокассеты, распечатки машинной информации и документы о соответствующем образовании. Особое внимание нужно уделять предметам, содержащим коды, пароли доступа, идентификационные номера, названия, электронные адреса пользователей конкретных компьютерных систем и сетей, алгоритмы входа и работы в системах и сетях.⁴²

Необходимо также перлюстрировать записные книжки, справочники и каталоги, в том числе электронные, находящиеся в памяти телефонных аппаратов и других компьютерных устройств.

Ценные доказательства могут быть обнаружены и при личных обысках обвиняемых.

Бесспорно, обыск как независимое процессуальное действие имеет свое определенное место и играет специфическую роль в сфере

⁴² Головин А. Ю. Проблемы и пути совершенствования методик расследования отдельных видов преступлений // Известия ТулГУ. Экономические и юридические науки. 2014. № 3. С. 6-7.

правоприменительной деятельности уполномоченных органов в рамках уголовного судопроизводства. Регулируемые с его участием задачи во многом определены той или иной следственной ситуацией, формирующийся во время предварительного расследования. Незамедлительное и правильное осуществление обыска помогает достижению целей отправления правосудия.

Итог данного следственного действия могут быть заложены, как в основу обвинительного приговора, так и стать поводом для исключения факта необоснованного привлечения лица к уголовной ответственности.⁴³

По делам о преступлениях в сфере неправомерного доступа к компьютерной информации, исследуемое следственное действие, чаще всего, имеет неотложный характер. Основанием для его производства служит наличие веских данных считать, что в каком-нибудь месте или у какого-то лица могут иметься предметы, документы и ценности орудия преступления, которые могут иметь важность для уголовного дела.

Цели обыска: выявление, фиксирование и изъятие перечисленных выше объектов, а также обнаружение разыскиваемых и поимка подозреваемых лиц.

В криминалистике относительно от объекта выделяют разные виды обыска. По делам о преступлениях в сфере неправомерного доступа к компьютерной информации, характерным может быть обыск в жилище и личный обыск обвиняемого, который там проживает. Эти следственные действия обладают определенной спецификой, которая предусмотрена как предметом, так и орудием преступного посягательства компьютерной информацией. Отличительные особенности последней ложатся отпечатком на все этапы осуществления установленного следственного действия.

Предварительная стадия обыска выступает как наиважнейшая роль во всем процессе осуществление плана следственного действия. Доскональная и

⁴³ Андреев Б. В. Расследование преступлений в сфере компьютерной информации : учебное пособие / Б. В. Андреев. М. : МАИК, 2013. С. 227.

серьезная детализация всех нюансов установившейся накануне обыска следственной обстановки во многом устанавливает его эффективность.⁴⁴

Практика указывает, что многое базируется от плотного взаимодействия следователя со специальным органом дознания - Отделом «К» при БСТМ МВД.

С его помощью поставляется соответствующая оперативная информированность следователя об обстоятельствах, связанных с проведением обыска, которая способствует избавиться от ряда тактических недоработок, а также компетентно определить вопрос об участии к его проведению квалифицированных экспертов в области компьютерной техники и понятих, содержащие конкретные навыки в этой сфере.

Выявить местоположение и схему размещения помещения, которое необходимо быть подвергнуто обыску. Определить характер охраны объекта. Выявить пути вероятного отступления подозреваемого.

С помощью специалиста в сфере телекоммуникаций установить дислокацию в данном здании узлов связи, размещение разводки коммуникационных сетей. Проанализировать вероятность наличия на объекте средств радиосвязи, применяемых обвиняемым. Определить их опознавательные характеристики: позывной, рабочую частоту, абонентский номер, логин и пароль доступа для работы.

Определить, какие средства электронно-вычислительной техники располагаются в помещении, в котором планируется провести обыск. При этом в большинстве случаев необходима консультация с подходящим специалистом. Впоследствии приобретенная информация будет применена для установления границ места, подвергнутое обыску, и внесет ясность касательно искомых предметов.

Определить, какие средства защиты информации и сетевой вычислительной технике от несанкционированного доступа располагаются по месту, где планируется провести обыск; выявить источники их питания и проанализировать возможность их обесточивания до начала обыска. Это

⁴⁴ Россинская Е. Р. Криминалистика : учеб. пособие для вузов. М. : ИНФРА-М, 2012. С. 245.

предоставит возможность исключить факты преднамеренного уничтожения необходимых предметов или документов.

Определить тип источников электропитания сетевой вычислительной техники и местонахождения пунктов их обесточивания для устранения вероятных попыток истребления искомой компьютерной информации, хранящейся в оперативной памяти компьютерных устройств.

Пригласить высококвалифицированных специалистов, владеющие достаточными умениями и навыками для предоставления эффективной помощи следователю при разработке и во время производства обыска. Для этих целей особенно подходят многофункциональные специалисты в области цифровых средств электросвязи и компьютерной техники.

Подготовить соответствующие СВТ, специальную аппаратуру и материалы для поиска, фиксации, осмотра и изъятия искомой компьютерной информации, предметов и документов.

Установить время, место и дату осуществления обыска, его длительность, а также меры, направленные на обеспечение его скоротечности и секретности. Особенно удобной обстановкой представляет собой момент отсутствия подозреваемого на месте обыска. Это обстоятельство допускает устранить активное сопротивление с его стороны и обеспечивает возможность следователю моментально выявить и грамотно изъять искомые объекты. При этом нужно отметить, что пребывание на месте обыска сослуживцев или близких родственников подозреваемого, как правило, создает у них конкретное отрицательное отношение к совершенному преступлению. Данный фактор может быть применен для решения тактики выполнения дальнейших следственных действий, например, допросов свидетелей.⁴⁵

Провести инструктаж лиц, привлеченных к содействию в обыске, с установлением четких персональных задач.

⁴⁵ Вехов В. Б. Попова В. В. Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации : научно-практическое пособие. 2-е изд., доп. и испр. М. : ЛексЭст, 2012. С. 45.

Изучить личность обвиняемого. Больше всего нужно обратить внимание на уровень его профессиональных навыков и знаний в области компьютерных технологий.

Пригласить обязательно понятых, владеющих конкретными знаниями в сфере компьютерной информации и телекоммуникаций.

По прибытии на место осуществления обыска специфика действий следователя будет заключаться в следующем:

- установить места вероятного отступления подозреваемого или вынесение документов и предметов, носящих весомую важность для уголовного дела. Принять меры к осуществлению наблюдения за ними;
- в случае оказания активного сопротивления со стороны лиц, присутствующих на объекте обыска, применить меры по нейтрализации сопротивления и незамедлительному попаданию в обыскиваемое жилище;
- устроить охрану места обыска и наблюдение за ним. Охране подлежат: охват обыскиваемых площадей; хранилища компьютерных носителей информации; сетевая вычислительная техника; спецсредства защиты от правомерного доступа; все пульты связи, охраны и электропитания, располагающиеся на объекте обыска; хранилища паролей аварийного и планового доступа к сетевой вычислительной технике, помещения и иным объектам, оказавшимися в зоне обыска.

В современной криминалистической литературе обсуждаются различные точки зрения по поводу последующих действий следователя на месте обыска.

Мы, в свою очередь, полагаем, что после реализации вышеуказанных мероприятий следователь должен перейти к следующей стадии обыска и выполнить следующие действия:

- установить местоположение подозреваемого на объекте обыска. При установлении - применить меры к выдворению его от пультов управления техническими устройствами, разомкнуть от них и образовать охрану;
- выявить и отключить специальные средства защиты информации и сетевой вычислительной техники от несанкционированного доступа, особенно

те, которые автоматически уничтожают компьютерную информацию и при нарушении процедуры доступа к ним, порядка их использования или установленных правил работы с ними; принять меры к установлению пароля санкционированного доступа и ключа шифрования-дешифрования информации;

- установить наличие телекоммуникационной связи между сетевой вычислительной техникой, сетевой вычислительной техникой и каналами электросвязи. При наличии компьютерной сети любого уровня технической организации в первую очередь должна быть осмотрена и подвергнута обыску управляющая компьютером - сервер, который хранит в своей оперативной и постоянной памяти наибольшую часть компьютерной информации, управляет другими сетевыми вычислительными техниками, имеет с ними прямую и обратную связь. В этом случае следует учитывать то обстоятельство, что у сообщников обвиняемого или у него самого имеется реальная возможность уничтожения искомой компьютерной информации дистанционно с помощью сетевой вычислительной техники, находящихся вне периметра обыскиваемой зоны. Применительно к этому положению вызывает недоумение утверждение некоторых авторов о том, что подключением компьютера к телефонной линии невозможно уничтожить или изменить информацию на нем. Эта информация может быть лишь пополнена или куда-либо передана. Расследование неправомерного доступа к компьютерной информации.⁴⁶

Для предупреждения вышеуказанных отрицательных последствий необходимо в зависимости от ситуации и рекомендаций специалиста временно или на длительный срок, частично или полностью отключить сетевую вычислительную технику или локальную вычислительную сеть от технических устройств, находящихся за периметром обыскиваемой зоны.

Отключение может быть произведено как на программном, так и аппаратном уровне. Если сетевая вычислительная техника работает в режиме

⁴⁶ Введенская О. Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. № 4. С. 212-214.

«электронной почты», то предпочтительнее оставить его до конца обыска в работающем состоянии в режиме «приема почты», исключив возможность какой-либо обработки и обратной передачи информации. Эту работу может сделать только квалифицированный специалист. Все выполняемые им действия должны быть зафиксированы с помощью видеозаписи и отражены в протоколе рассматриваемого следственного действия:

- определить сетевую вычислительную технику, находящиеся во включенном состоянии, характер выполняемых ими операций и название программ. Особое внимание необходимо уделить печатающим и видеоотображающим устройствам. Распечатки информации при необходимости должны быть изъяты и приобщены к протоколу следственного действия; изображение на экране монитора – видеограмма изучено и детально описано в протоколе.

Если специалист установит, что на момент обыска на каком-либо сетевом вычислительном оборудовании происходит уничтожение информации либо ее машинного носителя, необходимо срочно всеми возможными способами приостановить этот процесс и начать обследование с данного места.

При обследовании персонального компьютера необходимо:

- а) установить последнюю исполненную программу или операцию, а при возможности - все, начиная с момента включения компьютера;
- б) произвести экспресс-анализ компьютерной информации, содержащейся на жестком диске и в оперативной памяти с целью получения данных, имеющих значение для следствия.⁴⁷

В случае совершения преступления выделенной категории с помощью портативного или малогабаритного сетевого вычислительного механизма, например, коммуникатора или сотового радиотелефона, организовать производство личного обыска подозреваемого или лиц, находящихся в обыскиваемом помещении. Это возможно лишь в тех случаях, когда у

⁴⁷ Белкин Р. С. Курс криминалистики : в 3-х томах. Т. 3 : Криминалистические средства, приемы и рекомендации. М. : Юристъ, 2012. С. 345.

следователя имеются достаточные основания полагать, что лицо скрывает при себе предметы либо документы, которые могут иметь значение для уголовного дела. Личный обыск такого лица производится по правилам, изложенным в ч. 3 ст. 184 УПК РФ.⁴⁸

Детальный этап обыска является очень трудоемким и требует слаженной работы всех участников следственного действия. Необходимо четко организовать поисковые мероприятия, направленные на выявление тайников, в которых могут находиться предметы и документы. Ими могут быть и сами компьютерные устройства - аппаратные и программные модули, входящие в состав компьютеров, системы компьютеров или их сети.

На заключительном этапе обыска составляются: протокол следственного действия и описи к нему; вычерчиваются планы обыскиваемых помещений, схемы расположения сетевой вычислительной техники относительно друг друга, инженерно-технических коммуникаций, а также схема соединения сетевой вычислительной техники между собой и с другими техническими устройствами; проводится дополнительная фотосъемка или видеозапись.

Предметом выемки в подавляющем большинстве случаев совершения преступления в сфере компьютерной информации являются персональные компьютеры, машинные носители информации и всевозможные документы, отражающие и регламентирующие различные операции, технологические процессы, связанные с обработкой, накоплением, созданием, передачей и защитой компьютерной информации, использованием компьютеров, системы компьютера и их сети. Последние находятся по месту работы подозреваемого, в рабочих кабинетах должностных лиц и других служебных помещениях.⁴⁹

Помимо вышеуказанного, могут быть изъяты специальные технические средства для негласного получения, модификации и уничтожения информации, свободные образцы почерка, бланки и фрагменты документов, заготовки машинных носителей информации, исходные тексты программ для ЭВМ,

⁴⁸ Уголовно-процессуальный кодекс РФ от 18.12.2001 № 174-ФЗ (ред. от 12.06.2017) // СЗ РФ. 2001. № 52. Ст. 4921.

⁴⁹ Россинская Е. Р. Криминалистика : учеб. пособие для вузов. М. : ИНФРА-М, 2012. С. 254.

черновики и иные образцы для сравнительного исследования. Перед изъятием магнитных носителей информации они должны быть в обязательном порядке упакованы в алюминиевый материал, предохраняющий его содержимое от внешнего электромагнитного и магнитного воздействия.

Судебная экспертиза - это процессуальное действие, проводимое в целях получения заключения по вопросам, имеющим доказательственное значение по делу. Лицо, обладающее специальными полномочиями и назначенное в соответствии с постановлением следователя для дачи такого заключения, именуется экспертом.

Назначение любого вида экспертизы оформляется постановлением следователя. В нем обязательно должны содержаться, мотивировка необходимости этого следственного действия, сведения об эксперте или экспертном учреждении, вопросы, на которые должен дать эксперт, а также описание материалов, предоставляемых для исследования.

С постановлением обязательно знакомят обвиняемого, которому даны достаточно широкие права, заявить отвод эксперту, просить о назначении эксперта из числа указанных им лиц, представить дополнительные вопросы эксперту для получения по ним заключения, присутствовать с разрешения следователя при производстве экспертизы и давать объяснения эксперту, знакомиться с его заключением до окончания расследования. При отказе в удовлетворении ходатайства обвиняемого должно быть вынесено мотивированное постановление. Если же оно удовлетворяется, то должно быть составлено новое постановление о назначении экспертизы.

По делам данной категории путем производства информационно-технической судебной экспертизы может быть установлен способ несанкционированного доступа. При производстве такой экспертизы рекомендуется использовать компьютерное оборудование той же системы, в которую проник преступник, либо специальные технические и программные средства.

По делам рассматриваемой категории по результатам информационно-технической судебной экспертизы может быть установлено место нарушения правил.

Следственный эксперимент представляет собой познавательный прием, посредством которого путем воспроизведения действий, обстановки или иных обстоятельств определенного события или явления и совершения необходимых опытных действий, в контролируемых и управляемых условиях исследуются эти события или явления. Такой прием с давних пор применяют и при исследовании каких-либо обстоятельств преступного события в ходе расследования, а также судебного разбирательства уголовных дел.

Действующим УПК для производства следственного эксперимента предусмотрены специальные правила. Его вправе производить следователь, а также орган дознания по делам о преступлениях, по которым предварительное следствие не обязательно. Известны случаи, когда интересные и убедительные эксперименты подобного рода проводились и в суде.⁵⁰

Суть самого следственного эксперимента, как сказано в законе, заключается в воспроизведении действий, обстановки или иных обстоятельств определенного события и совершения необходимых опытных действий в целях проверки и уточнения данных, имеющих значение для дела. Посредством такого рода действий обычно проверяют возможность видеть, слышать определенные, значимые для дела обстоятельства в тех или иных условиях, возможность совершения определенных действий и получения определенных результатов при наличии конкретных условий.

При производстве следственного эксперимента в необходимых случаях могут участвовать обвиняемый или подозреваемый, защитники этих лиц, а также потерпевший и свидетель.

Ход и результаты производства следственного эксперимента описываются в протоколе с соблюдением требований статей 141 и 142 УПК.

⁵⁰ Уголовно-процессуальный кодекс РФ от 18.12.2001 № 174-ФЗ (ред. от 12.06.2017) // СЗ РФ. 2001. № 52. Ст. 4921.

Если при производстве следственного эксперимента производились какие-либо измерения или применялись технические средства, то все это должно найти отражение в протоколе.

Следственный эксперимент по делам данной категории производится с целью проверки возможности преодоления средств защиты компьютерной системы одним из предполагаемых способов.

Для установления возможности создания вредоносной программы определенным лицом, сознавшим в этом: проводится следственный эксперимент с использованием соответствующих средств компьютерной техники.

При проведении следственного эксперимента выясняется возможность наступления вредных последствий при нарушении определенных правил. Он проводится с использованием копий исследуемой информации и по возможности на том же компьютере, при работе на которой нарушены правила.⁵¹

⁵¹ Балашов Д. Н. Балашов Н. М. Маликов С. В. Криминалистика : учебник. М. : ИНФРАМ, 2005. С. 133.

Заключение

Данная дипломная работа посвящена рассмотрению особенности расследования преступлений в сфере компьютерной информации.

По итогам рассмотрения преступлений в сфере компьютерной информации сформулировано научно обоснованное заключение по основным направлениям применения статей, содержащихся в гл. 28 УК РФ, а также конкретные предложения по совершенствованию уголовно-правовых норм, предусматривающих ответственность за данные преступления.

Несмотря на научную разработанность данной проблемы, на практике, при квалификации преступлений в сфере компьютерной информации правоприменитель часто сталкивается с затруднениями технико-юридического характера, например, у следователя или судьи возникает проблема при уяснении некоторых понятий, содержащихся в диспозициях ст. 272-274 УК РФ, а именно:

- компьютерная программа;
- несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации;
- средства хранения, обработки или передачи охраняемой компьютерной информации.

Это связано с тем, что указанные технико-юридические термины законодательно нигде не определены.

В связи с этим было предложено дополнить ст. 272-274 УК РФ технико-юридические термины, для того, чтобы в полном объеме квалифицировать данное преступление.

Кроме того, при квалификации деяний, предусмотренных ст. 272-274 УК РФ возникает ряд вопросов, требующих конкретного толкования для правоприменителя Верховным Судом Российской Федерации.

Например, будет ли являться уничтожением компьютерной информации деяние, при котором информация была изначально уничтожена, но спустя

определенное время частично или полностью восстановлена специалистами. Как квалифицировать уничтожение компьютерной информации сильным электромагнитным или высокочастотным излучением, не повлекшим уничтожение самого носителя информации.

Описанные деяния и последствия носят противоправный характер и должны учитываться при квалификации преступлений в сфере компьютерной информации.

При квалификации преступных действий, предусмотренных ст. 273 УК, следует отметить неудачную юридическую конструкцию ч. 1 ст. 273 УК РФ, в диспозиции которой указывается на «создание, распространение или использование компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации». Указание законодателем на создание, использование и распространение вредоносных компьютерных программ во множественном числе по смыслу статьи можно трактовать таким образом, что правоприменитель не вправе привлекать к уголовной ответственности лицо, которое создало, использовало или распространило одну вредоносную компьютерную программу.

В связи с этим было предложено внести изменение в название статьи, для того, что бы правоприменитель имел право привлекать к уголовной ответственности лиц, которые создают, используют и распространяют одну вредоносную программу.

Существенную значимость в структуре криминалистической характеристики компьютерных преступлений играют также проанализированные сведения о пострадавшей стороне, которые позволяют в полной мере квалифицировать личность преступника, повод совершения противоправных действий проанализированных ранее и помогает точнее описать круг лиц, среди которых лучше всего искать преступника, и

планировать розыскные мероприятия по нахождению важных доказательств по делу.

Анализ особенностей формирования следовой картины при совершении преступлений в сфере компьютерной информации привел к необходимости введения понятия «виртуальных следов» определяемых как любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации на материальном носителе, в том числе и на электромагнитном поле.

Предметом доказывания компьютерных преступлений с позиций криминалистики, их типизация и классификация позволяют установить связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

При проведении обыска или выемки электронные носители информации изымаются с участием специалиста. Соответствующее положение вызывает ряд вопросов. В первую очередь, исходя из принципов уголовного судопроизводства, изъятие в ходе производства обыска или выемки электронных носителей без участия специалиста будет считаться нарушением требований УПК РФ, то есть эти доказательства согласно п. 3 ч. 2 ст. 75 УПК РФ, будут признаны недопустимыми. Не вызывает сомнений, что изъятие электронных носителей информации, которые являются частью других электронных устройств, либо подключенных к другому оборудованию, а также копирование информации с изымаемых электронных носителей в интересах третьих лиц должно производиться только специалистом. Но вряд ли существует техническая необходимость привлекать специалиста для изъятия, к примеру, сотового телефона, цифрового фотоаппарата, MP3-плеера, а в соответствии с требованиями УПК РФ в ходе обыска или выемки это обязательно.

В связи с этим мы предлагаем ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ дополнить предложением «Допускается изъятие электронных носителей

информации без участия специалиста, если электронные носители информации изымаются целиком и изъятие производится без копирования содержащейся на них информации».

Таким образом, мы видим, что, не смотря на всю положительность распространения и внедрения в нашу жизнь компьютерных технологий, мы приходим к пониманию опасности использования этих технологий в преступных целях. Существующее законодательство по охране нового вида общественных отношений от преступных посягательств еще не достаточно совершенно. Поэтому дипломная работа представляет собой попытку улучшения уголовного законодательства и уголовно-процессуального законодательства и выработке наиболее оптимальной схемы его применения в области борьбы с компьютерной преступностью. Эта работа, также, служит толчком к дальнейшему исследованию проблем противодействия преступным деяниям в сфере компьютерной информации.

Список литературы

Нормативно-правовые акты

1. Российская Федерация. Конституция (1993) // Российская газета. – 1993. - № 237.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.06.2017) // СЗ РФ. – 1996. - № 25. – Ст. 2954.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 12.06.2017) // СЗ РФ. – 2001. - № 52. – Ст. 4921.
4. Об информации, информационных технологиях и о защите информации Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 07.06.2017) // СЗ РФ. – 2006. - № 31. – Ст. 3448.
5. Об оперативно-розыскной деятельности Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 06.07.2016) // СЗ РФ. – 1995. - № 33. – Ст. 3349.
6. О государственной тайне Закон Российской Федерации от 21.07.1993 № 5485-1 (ред. от 08.03.2015) // СЗ РФ. – 1993. - № 41. – Ст. 4673.
7. О персональных данных Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017) // СЗ РФ. – 2006. - № 31. – Ст. 3451.
8. О коммерческой тайне Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014) // СЗ РФ. – 2004. - № 32. – Ст. 3283.

Учебная литература

9. Андреев, Б. В. Расследование преступлений в сфере компьютерной информации : учебное пособие / Б. В. Андреев. - М. : МАИК, 2013. - 527 с.
10. Балашов, Д. Н. Балашов, Н. М. Маликов, С. В. Криминалистика : учебник. - М. : ИНФРАМ, 2005. - 503 с.
11. Белкин, Р. С. Курс криминалистики : в 3-х томах. Т. 3 : Криминалистические средства, приемы и рекомендации. - М. : Юрист, 2012. - 480 с.

12. Быков, В. М. Черкасов, В. Н. Преступления в сфере компьютерной информации : криминологические, уголовно-правовые и криминалистические проблемы. - М. : Юрлитинформ, 2015. - 328 с.
13. Вехов, В. Б. Попова, В. В. Илюшин, Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации : научно-практическое пособие. - 2-е изд., доп. и испр. - М. : ЛексЭст, 2012. - 160 с.
14. Гаврилин, Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание : учебное пособие. - М. : Книжный мир, 2013. - 245 с.
15. Криминалистика. Базовый курс : учебник / под ред. А. Г. Филиппова. - М. : Юрайт, 2015. - 441 с.
16. Криминалистика : учебник / Агафонов, В. В. - М. : Юрайт, 2013. - 463 с.
17. Криминалистика : учебник / Волохова, О. В. и др. - М. : Проспект, 2013. - 501 с.
18. Криминалистика : учебник / под ред. Яблокова, Н. П. 3-е изд., перераб. и доп. - М. : Юристъ, 2005. - 781 с.
19. Криминалистика : учебное пособие / Адельханян, Р. А. Аминов, Д. И. Федотов, П. В. - М. : Юнити-Дана, 2014. - 238 с.
20. Крылов, В. В. Информационные компьютерные преступления : учебное и практическое пособие. - М. : Норма, 2005. - 285 с.
21. Кузьмин, А. С. Альбом схем по криминалистической тактике и методике расследования отдельных видов преступлений : учебно-наглядное пособие / А. С. Кузьмин. – Минск. : Юрфак БГУ, 2013. - 118 с.
22. Методика расследования компьютерных преступлений : учебное пособие / М. Ш. Махтаев. - М. : РосНОУ, 2012. - 192 с.
23. Родин, А. Ф. Вехов, В. Б. Использование компьютерных технологий в деятельности следователя / Под ред. проф. Б. П. Смагоринского. - Волгоград : ВА МВД России, 2013. - 156 с.

24. Рослякова, О. А. Далинин, А. В. Зорина, Е. А. Преступления в сфере компьютерной информации : учебное пособие. - СПб. : Издательство, 2015. - 180 с.
25. Россинская, Е. Р. Криминалистика : учеб. пособие для вузов. - М. : ИНФРА-М, 2012. - 463 с.
26. Сверчков, В. В. Уголовное право. Особенная часть : Краткий курс лекций. - М. : Юрайт, 2014. - 240 с.
27. Соловьев, Л. Н. Вредоносные программы. Расследование и предупреждение преступлений. – М. : Собрание, 2014. - 224 с.
28. Сухарев, А. Я. Компьютерные преступления : учебное пособие / А. Я. Сухарев. - М. : ПРИОР, 2012. - 384 с.

Научная литература

29. Введенская, О. Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. - 2015. - № 4. - С. 209-216.
30. Вехов, В. Б. Ковалев, С. А. Теоретические и прикладные проблемы применения программного обеспечения специального назначения при расследовании преступлений в сфере компьютерной информации // Вестник ВИ МВД России. - 2012. - № 1. - С. 38-41.
31. Головин, А. Ю. Проблемы и пути совершенствования методик расследования отдельных видов преступлений // Известия ТулГУ. Экономические и юридические науки. - 2014. - № 3-2. - С. 3-10.
32. Евдокимов, К. Н. Актуальные проблемы совершенствования субъекта состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Сибирский юридический вестник. - 2013. - № 3. - С. 69-75.
33. Евдокимов, К. Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. - 2016. - № 1 - С. 86-94.

34. Лядский, В. В. Преступления в сфере компьютерной информации // Электронный вестник Ростовского социально-экономического института. - 2014. - № 2. - С. 332-338.
35. Мусаева, У. А. Специфика проведения следственного осмотра по делам о преступлениях в сфере компьютерной информации // Известия ТулГУ. Экономические и юридические науки. - 2013. - № 4-2. - С. 295-302.
36. Осипенко, А. Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации» : содержание и основы осуществления // Вестник ВИ МВД России. - 2016. - № 3. - С. 83-90
37. Подольный, Н. А. Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий // Библиотека криминалиста. Научный журнал. - М. : Юрлитинформ. - 2013. - №5. - С. 116-127.
38. Поляков, В. В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АлтГУ. - 2013. - № 2. - С. 114-116.
39. Поляков, В. В. Лапин, С. А. Средства совершения компьютерных преступлений // Доклады ТУСУР. - 2014. - № 2 - С.162-166.
40. Потапов, С. А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. - 2016. - № 10. - С. 90-96.
41. Сычев, Е. А. Алескерова, В. И. Колокольчикова, О. Н. Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации // ИСОМ. - 2014. - № 4. - С. 350-355.
42. Хаитжанов, А. Генералова, А. П. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации // НиКа. - 2011. - № 1. - С. 219-221.
43. Шеметов, А. К. О понятии виртуальных следов в криминалистике // Российский следователь. - 2014. - № 20. - С. 52-54.