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

Кафедра уголовного процесса

Расследование преступлений в сфере компьютерной информации

Учебное пособие

Екатеринбург
2019

ББК 67.408.135
Р244

Расследование преступлений в сфере компьютерной информации: ***учебное пособие.*** – Екатеринбург: Уральский юридический институт МВД России, 2019. – 75 с.

ISBN 978-5-88437-662-5

Коллектив авторов:

Федосеева Е. Л., кандидат юридических наук;
Мухачев С. В., кандидат физико-математических наук, доцент;
Харламова А. А., кандидат юридических наук, доцент;
Пашнин А. Н., кандидат юридических наук, доцент;
Ретюнских И. А., кандидат юридических наук, доцент;
Зеленина О. А., кандидат юридических наук, доцент;
Политыко О. Е.;
Расулова Н. С.

Рецензенты: **Н. С. Диденко**, начальник кафедры уголовного процесса Ростовского юридического института МВД России, кандидат юридических наук;
А. В. Никитин, начальник кафедры уголовного процесса Восточно-Сибирского института МВД России, кандидат юридических наук, доцент

В учебном пособии раскрываются особенности расследования преступлений в сфере компьютерной информации: квалификация компьютерных преступлений, особенности производства отдельных следственных действий и т. д. Издание способствует развитию способности применять в профессиональной деятельности теоретические основы раскрытия и расследования преступлений, реализовывать мероприятия по получению юридически значимой информации, работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.

Учебное пособие предназначено для курсантов и слушателей образовательных организаций МВД России, обучающихся по специальности 40.05.01 Правовое обеспечение национальной безопасности.

Обсуждено на заседании кафедры уголовного процесса УрЮИ МВД России (протокол № 9 от 15 мая 2019 г.).

Рекомендовано к использованию в образовательном процессе методическим советом УрЮИ МВД России (протокол № 8 от 17 июня 2019 г.).

ISBN 978-5-88437-662-5 ББК 67.408.135

Введение

В связи с развитием технического прогресса, компьютеризацией общества и повсеместным распространением в обиходе глобальной сети Интернет возникла потребность в использовании компьютерной техники и различного рода электронных устройств обмена и передачи информации. Как в продаже, так и в пользовании физических и юридических лиц, госорганов появилось множество всевозможных «электронных гаджетов», расширение использования которых привело сначала к появлению, а затем и к увеличению числа совершаемых компьютерных преступлений.

Согласно статистическому исследованию, проведенному Бюро специальных технических мероприятий МВД России, число таких преступлений в России увеличилось на 8,6 % и составило более 11 тысяч[1].

Сложность в понимании способа совершения компьютерных преступлений и в их расследовании связана с используемой в данной сфере терминологией, поскольку она имеет технический характер. Большинство понятий определяются и содержатся в отраслевых и специальных нормативных актах. Одним из основных в этом смысле является Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2], который постоянно претерпевает изменения.

Данный нормативный документ вводит и раскрывает понятие компьютерной информации, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Несмотря на то, что до сих пор термин «компьютерное преступление» законодательно не определен и носит «операционный характер», его определение можно встретить в научной литературе.

Так под компьютерным преступлением понимается предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства[3].

Вообще преступления подобного рода в России совершались еще в 20 веке. Так, первое преступление было выявлено в бывшем СССР (в Прибалтике) в 1979 г. и зарегистрировано в международном реестре правонарушений. На сегодняшний день число таких преступлений, совершенных с использовани-

---

[1] См.: Киберпреступность в России. URL: http://www.tadviser.ru/index.php

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (в ред. от 19.07.2018) // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448. URL: http://www.consultant.ru.

[3] См.: *Дуленко В. А., Мамлеев Р. Р., Пестриков В. А.* Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учеб. пособие. URL: https://www.bestreferat.ru/referat-199192.html

ем электронных средств, возрастает, а их способы становятся все более изощренными.

На самом деле, подсчет статданных о маштабах этих преступлений сейчас достаточно затруднителен. Связано это с тем, что статистическая отчетность ГИАЦ МВД России (отчет о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации, – форма 1-ВТ) не отражает объективную картину ввиду фрагментарности содержащейся в ней информации (в форме, например, нет сведений о количестве зарегистрированных преступлений по ст. 159.3, 159.6, 187 УК РФ). Определенную роль в невозможности отражения реального положения дел сыграло также и отсутствие единообразия при квалификации рассматриваемых деяний с учетом их юридико-экономической природы[1].

Между тем анализ поступающих в суды уголовных дел свидетельствует о незначительном их количестве по данным преступлениям. Указанное обстоятельство заставляет задуматься об уровне эффективности выявления таких преступлений и сложности расследования.

Общественная опасность преступлений в сфере компьютерной информации состоит в том, что уничтожение, блокирование, модификация информации, важной для действий, связанных с управляющими датчиками сложных компьютерных систем, способны повлечь гибель людей, причинить вред их здоровью, уничтожить имущество, причинить экономический вред в больших размерах. Учитывая эти обстоятельства, законодатель отнес гл. 28 «Преступления в сфере компьютерной информации» к разд. IX Уголовного кодекса Российской Федерации «Преступления против общественной безопасности и общественного порядка». Поэтому, несмотря на то, что глава 28 УК РФ предусматривает только четыре состава преступлений в сфере компьютерной информации, в соответствии с законодательством России компьютерные преступления классифицируются более широко. К ним можно отнести преступления в сфере оборота компьютерной информации, в сфере информационного оборудования, телекоммуникаций, в области защиты охраняемой законом информации.

В данном пособии анализу подлежат особенности расследования преступлений, предусмотренных только данной главой УК РФ, что и является предметом исследования.

Использование учебного пособия в практической деятельности позволит активизировать и повысить эффективность расследования уголовных дел по преступлениям в сфере компьютерной информации, не допускать ошибок со стороны должностных лиц, осуществляющих расследование.

---

[1] См.: *Хисамова З. И.* Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. … канд. юрид. наук. Краснодар, 2016. С. 5.

Издание может применяться в практической деятельности подразделений органов внутренних дел при расследовании компьютерных преступлений, а также в образовательном процессе обучающимся образовательных организаций МВД России по специальностям 40.05.01 Правовое обеспечение национальной безопасности при изучении учебных дисциплин «Расследование преступлений в сфере компьютерной информации», «Методы и способы получения доказательственной информации с электронных носителей».

Использование пособия в учебном процессе может способствовать формированию профессиональных компетенций, необходимых в конкретных практических ситуациях, возникающих при расследовании уголовных дел и связанных с деятельностью по возбуждению уголовных дел, производству следственных действий, обнаружению, изъятию и фиксации электронных носителей информации по преступлениям указанной категории, а именно:

– способности принимать решения и совершать юридические действия в точном соответствии с законодательством Российской Федерации (ПК-3);

– способности разрабатывать и правильно оформлять юридические и служебные документы (ПК-5);

– способности выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения (ПК-9);

– способности реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений (ПК-11);

– способности правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации (ПК-13);

– способности производить предварительное расследование (в форме предварительного следствия) по уголовным делам о преступлениях, подследственных органам внутренних дел (ПСК-1.1).

Тема 1. Общая характеристика компьютерной информации

§ 1.1. Понятие и сущность компьютерной информации. Специфика представления информации в электронном виде

Понятие «информация» является фундаментальным, первичным в цикле наук, связанных с информационными технологиями. Это обстоятельство обусловливает сложность при формулировке определения информации. Действительно, когда дается определение какого-либо понятия, прибегают к первичным понятиям и через них определяют какое-либо вторичное. А в случае определения понятия «информация» приходится определять первичное понятие. Поэтому в литературе можно найти различные определения информации, в зависимости от сферы использования, субъекта, воспринимающего информацию и т. д.

Приведем некоторые определения, которые можно встретить в литературе. Определение, основанное на информационном взаимодействии человека с окружающим миром, обычно звучит следующим образом.

Информация – это отражение предметного мира, выраженное в форме сигналов и знаков. Это определение дается с точки зрения восприятия человеком окружающего мира. Различные виды информации человек ощущает с помощью органов чувств, и далее в сознании возникает отражение, образ окружающей действительности. Информация закрепляется человеком посредством знаков и передается сигналами.

Другое определение информации. Информация – это сведения, которые уменьшают или снимают неопределенность, существовавшую до их получения.

Именно такое определение закладывается в основу того, чтобы задать количество информации в том или ином сообщении. Такой подход сегодня наиболее распространен, он основан на наличии либо отсутствии содержательного компонента в сообщении.

Количественная мера информации определяется как логарифм от числа возможных состояний в системе, относительно которых снимается неопределенность при получении информации (формула Хартли):

$I = \log_2 N$,

где I – количество информации, N – число возможных состояний, относительно которых снимается неопределенность.

Стандартную единицу измерения информации предложил свое время знаменитый ученый в области информатики К. Шеннон.

Бит – это количество информации, снимающее неопределенность в отношении появления одного из двух равновозможных состояний.

На практике используют более крупные производные единицы: байт, килобайт, Мегабайт, Гигабайт, Терабайт.

В Федеральном законе «Об информации, информационных технологиях и о защите информации»[1] дается такое определение: «Информация – это сведения (сообщения, данные) независимо от формы их представления».

Особенность представления информации в компьютере состоит в том, что и программы, и данные обрабатываются, хранятся и передаются в виде двоичных кодов. Связано это с техническими причинами: реализовать устройство с двумя устойчивыми состояниями (интерпретируемыми как 0 и 1) гораздо проще, чем устройство с десятью устойчивыми состояниями (как требуется при использовании десятичной системы счисления). При кодировании различных видов информации (цифр, текста, графических изображений, звука) разработаны и применяются специальные системы кодирования.

§ 1.2. Правовое понятие и признаки электронного документа

Понятие «электронный документ» прочно вошло в деятельность, связанную с обработкой и использованием материалов, обрабатываемых с использованием компьютера. Наиболее строгое определение этого понятия содержится в Федеральном законе «Об информации, информационных технологиях и о защите информации»: «Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель».

Из приведенного определения понятно, что признаков, позволяющих идентифицировать документ и его содержание, два: реквизиты либо материальный носитель информации.

Основные реквизиты, которые используются в процессе работы с документами: Государственный герб Российской Федерации; эмблема организации или товарный знак (знак обслуживания); наименование организации; наименование вида документа; дата документа; регистрационный номер документа; адресат; резолюция; заголовок к тексту; текст документа; подпись; гриф и визы согласования документа; оттиск печати; отметка об исполнителе; отметка о поступлении документа в организацию; идентификатор электронной копии документа.

Второй признак документированной информации – материальный носитель – представляет собой объект, используемый для записи, хранения и считывания различных видов информации: текстовой, звуковой или графической. В качестве материального носителя применяют бумагу, магнитные диски, флэш-накопители и т. п. Бумажный носитель широко использовался в докомпьютерное время, но продолжает использоваться и сегодня. Наряду с бумагой с появлением компьютеров получили широкое распространение электронные (машиночитаемые) материальные носители.

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ.

Документы, используемые в бумажном виде, имеют такие привычные реквизиты, как подпись, гриф и визы согласования документа, оттиск печати и некоторые другие. Такие реквизиты выполняют либо механически (печать), либо собственноручно (подпись). Некоторые реквизиты в таком документе могут быть созданы и с помощью компьютера.

На электронном материальном носителе записывается документ, созданный с помощью компьютера.

Главное требование при работе с электронным документом – гарантия его подлинности, или, как говорят, аутентичность. Чтобы обеспечить аутентичность, разработаны специальные принципы и процедуры, позволяющие контролировать различные этапы работы с электронным документом. К таким этапам относятся создание, передача, хранение и обработка документов. Реализуемый на различных этапах контроль позволяет гарантировать защищенность электронного документа от несанкционированного изменения, использования и сокрытия. Кроме того, названные принципы и процедуры дают возможность идентифицировать лицо, создавшее электронный документ.

Из вышеизложенного очевидно, что документ с обычными реквизитами, обрабатываемый с помощью компьютера, не является электронным документом. Такой легко может быть изменен, причем изменения не удастся распознать. Кроме того, при работе с электронными документами необходимы надежные средства для идентификации лица, создавшего документ. Названные требования привели к созданию специального средства – электронной подписи.

Электронная подпись является основным реквизитом электронного документа. Понятие электронной подписи и ее виды приведены в федеральном законе «Об электронной подписи»[1]. Электронная подпись – это информация в электронном виде, которая связана с подписываемым документом, сгенерирована по специальному алгоритму и используется для идентификации электронного документа и подписавшего лица.

Средства для работы с электронной подписью проходят сертификацию в установленном порядке.

В последнее десятилетие активно развивается электронный документооборот, который представляет собой электронный обмен документами между автоматизированными системами различных ведомств и компаний в стандартизованной форме. Внедряются специальные программные системы электронного документооборота.

§ 1.3. Понятие аппаратной и программной части компьютера

Программное обеспечение – это совокупность программ, под управлением которых работает вычислительное устройство.

[1] Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ. URL: http://www.consultant.ru/

По выполняемым функциям программное обеспечение можно разделить на две большие категории: системное программное обеспечение и прикладное программное обеспечение.

Системное программное обеспечение – это совокупность программ для обеспечения работы вычислительного устройства и компьютерных сетей.

Прикладное программное обеспечение – это компьютерные программы, разработанные для решения определенных задач пользователя. Например, табличный процессор Microsoft Word, средства для работы в сети Интернет, бухгалтерские программы, компьютерные игры и т. д.

Системное программное обеспечение включает следующие основные компоненты.

1. Операционные системы.

Представляют собой совокупность программ, которые управляют компонентами компьютера, загружают программы пользователя и реализуют их выполнение, организуют взаимодействие пользователя с компьютером. Сегодня используется достаточно много различных операционных систем: Windows, Linux и другие. Они различаются политикой распространения, возможностями, элементами интерфейса.

2. Инструментальные системы. Необходимы для создания новых программ. Например, Pascal, C++.

3. Сервисные системы. Позволяют реализовать некоторые дополнительные (по отношению к операционной системе) функции: работа с архивами, получение расширенной информации о программных и аппаратных ресурсах, антивирусные средства. Следует отметить, что постепенно сервисные функции становятся частью операционных систем.

Аппаратное обеспечение компьютера – это совокупность технических компонентов, входящих в его состав. От того, какие компоненты используются, зависит мощность и функциональные возможности компьютера.

Современные компьютеры имеют магистрально-модульную архитектуру: состоят из модулей (блоков), связанных посредством магистрали. По магистрали, представляющей из себя набор проводников, передаются данные, команды и адреса.

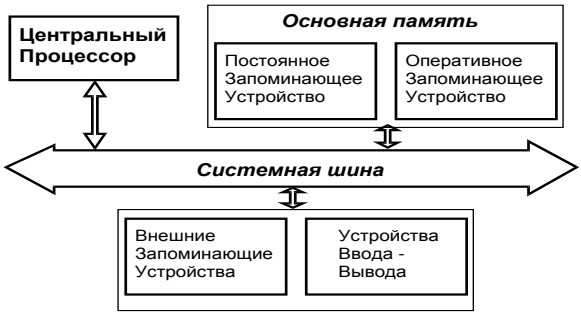


Рис. 1. Обобщенная структурная схема компьютера

Охарактеризуем функциональные блоки, представленные на структурной схеме.

Центральный процессор – это устройство, которое обрабатывает информацию и управляет работой всех компонентов компьютера. Технические характеристики микропроцессора во многом определяют вычислительную мощность компьютера, его быстродействие и функциональные возможности. Основные технические характеристики – тип процессора и тактовая частота. Например, Intel Corei 7, 2 ГГц.

Основная память – устройство, предназначенное для хранения информации, с которой оперирует центральный процессор. Основная память включает интегральные микросхемы оперативных и постоянных запоминающих устройств (ОЗУ и ПЗУ). Основные характеристики основной памяти – информационная емкость и быстродействие. Быстродействие определяется временем доступа к ячейкам памяти. Время доступа – это промежуток времени, в течение которого может быть записано или прочитано содержимое ячейки памяти. Основная память характеризуется высоким быстродействием – запись в ОЗУ информации и чтение ее, а также чтение информации из ПЗУ, происходит за очень короткое время – около 1 нс (одна наносекунда равна одной миллиардной доле секунды). Типичный для персонального компьютера объем ОЗУ составляет несколько Гбайт, ПЗУ – сотни Мбайт.

ОЗУ хранит записанную информацию только при включенном электропитании. Если электропитание отключить, содержимое ОЗУ уничтожается. ПЗУ сохраняет информацию и при выключении электропитания.

К периферийным устройствам относятся внешние запоминающие устройства и устройства ввода-вывода информации.

Долговременное хранение больших объемов информации реализуется во внешних запоминающих устройствах (ВЗУ). В качестве ВЗУ в компьютерах обычно используются накопители на магнитных дисках, накопители на SSD-дисках, флэш-накопители. Объем памяти ВЗУ достигает сегодня нескольких Терабайт. Однако по сравнению с ОЗУ они обладают относительно низким быстродействием (велико время записи-считывания). ВЗУ сохраняют записанную информацию и после выключения компьютера, т. е. используют такие физические принципы, которые не связаны с наличием электропитания.

Устройства ввода-вывода (УВВ) обеспечивают общение пользователя с компьютером и обмен информацией по сетевым каналам. Примеры устройств ввода информации в компьютер: клавиатура, манипулятор «мышь»; устройств вывода информации: монитор, принтер.

Монитор – основное устройство отображения информации. Наиболее распространены жидкокристаллические дисплеи. Они создаются на основе специальных веществ – жидких кристаллов. Это материалы, оптические свойства которых изменятся приложенным электрическим напряжением. Экран такого дисплея состоит из множества жидкокристаллических точек, комбинация которых позволяет сформировать любое изображение.

Дисплеи характеризуются размером экрана по диагонали (17, 19 дюймов), разрешением (1024x800 – количество точек на экране по горизонтали и вертикали) и соответствием эргономическим требованиям, где оговариваются такие характеристики, как величины рассеиваемых электромагнитных полей и электростатических полей, бликов на экране и т. п. Чем выше разрешение, тем выше качество изображения.

Принтер предназначен для вывода текстовой и графической информации на бумажный носитель. По принципу работы сегодня наиболее распространены струйные и лазерные принтеры (в зависимости от принципа создания изображения).

В струйных принтерах микрокапли чернил выстреливаются на бумагу из специальных сопел. Сопла связаны с резервуарами, в которых содержатся специальные чернила различного цвета. Множество сопел, встроенных в печатающем устройстве, перемещается относительно поверхности бумаги. Для печати цветных изображений используется 4, 6 и 8 красок, при смешивании которых на бумаге получается изображение. Используются следующие цвета: голубой, пурпурный, желтый и черный. Для высококачественных фотопринтеров добавляют светло-голубой и светло-пурпурный. Добавочные краски улучшают изображение в светлых тонах, когда точек мало и они не образуют цельной картины. Цвета выбраны с учетом того, что изображение на бумаге рассматривается в отраженном свете.

В лазерном принтере изображение формируется на бумаге с помощью специального барабана. Предварительно барабан электризуется с помощью луча лазера, управляемого компьютером; затем на барабан напыляется специальный порошок, который прилипает к электрически заряженным областям. Лазерные принтеры наиболее распространены и обеспечивают хорошее качество печати.

§ 1.4. Понятие вредоносной программы. Классификация вирусов

Понятие «вредоносная программа» дается в ст. 273 Уголовного кодекса Российской Федерации[1]. Это компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Можно найти различные классификации вредоносных программ. Остановимся на классификации, предложенной «Лабораторией Касперского»[2].

Вирус – это самовоспроизводящийся программный код, который внедряется в установленные на устройство программы без согласия пользователя.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. URL: http://www. consultant.ru/

[2] См.: URL: https://www.kaspersky.ru/blog/klassifikaciya-vredonosnyx-programm/2200/

Наиболее распространены классификации, предлагающие различать компьютерные вирусы по типу заражаемых объектов и по методам заражения и выбора атакуемых объектов.

Способы заражения компьютерным вирусом разнообразны. Например, заражение может произойти при переходе по ссылке, открытии файла в письме электронной почты, при посещении специального сайта. Вирус может выполнять множество различных действий, связанных с причинением вреда операционной системе; информации, хранящейся на компьютере, финансовым и иным интересам пользователя.

Одна из разновидностей вредоносных программ – червь – также создан на основе саморазмножающихся программ. Но он не может заражать существующие файлы. Вместо этого червь локализуется в компьютере в виде отдельного файла и ищет уязвимости в компьютерной сети или системе с целью дальнейшего распространения своих копий. Червь может распространяться через электронную почту, мессенджеры, обмен файлами и т. д. Червь хранится на жестком диске в виде файла. Однако есть модификации, которые сохраняются только в оперативной памяти компьютера с целью обеспечения скрытности.

Троянская программа по способу распространения отличается от вирусов и червей. Она заносится в компьютер под видом легального приложения, однако кроме функций приложения выполняет еще и те, которые заложены злоумышленником. Троянские программы получили свое название в соответствии с известным из древнегреческой мифологии конем, так как под видом какой-либо полезной программы в систему проникает программа вредоносная. Троянские программы не могут самовоспроизводиться. Такие программы выполняют сложные и разнообразные задачи в компьютерной системе. Известна, например, троянская программа, использующая вычислительные мощности компьютера-жертвы для генерации электронной валюты Bitcoin.

Еще одна разновидность вредоносных программ – руткит. Особенность руткита в том, что для сокрытия вредоносного кода и его работы от пользователя и установленного защитного программного обеспечения применяется тесная его интеграции с операционной системой. Более того, некоторые руткиты могут запускаться перед загрузкой операционной системы.

Бэкдор (средство удаленного администрирования), или RAT (remote administration tool), – программа, которая позволяет злоумышленнику управлять компьютером дистанционно. В зависимости от преследуемых целей злоумышленник, например, может установить и запустить на компьютере жертвы любое программное обеспечение; сохранить все нажатия клавиш; загрузить и сохранить любые файлы; включать микрофон или видеокамеру. Таким образом, появляется возможность контролировать компьютер и информацию жертвы.

Следующая разновидность вредоносных программ называется «загрузчик». Это небольшая программа, которая служит для загрузки и установки на

компьютере-жертве полной версии вредоносной программы. После того как загрузчик попадает в систему, он соединяется с удаленным сервером и загружает тело вредоносной программы.

Внедрение вредоносной программы в компьютер-жертву или мобильный телефон реализуется по-разному. Основных способов два[1]:

– социальная инженерия;

– технические приемы внедрения вредоносного кода в заражаемую систему.

Методы социальной инженерии направлены на то, чтобы пользователь своими усилиями обеспечил заражение компьютера. Хитрость состоит в том, чтобы привлечь внимание пользователя к зараженному файлу (или ссылке на зараженный файл). Классический пример – распространявшийся в 2000 г. почтовый червь LoveLetter. Электронное письмо, приходившее на электронный почтовый ящик, называлось «I love you». Пользователи, получившие такое письмо, открывали его, так как хотели узнать, кто прислал им признание. В результате активировалась вредоносная программа. Результат «эпидемии» – почтовые серверы компаний не выдержали нагрузки, т. к. червь рассылал свои копии по всем контактам из адресной книги пораженного компьютера. Другой пример – червь Swen, выдававший себя за сообщение от компании Microsoft и маскировавшийся под обновление, устраняющее ряд уязвимостей в операционной системе Windows.

Для распространения вредоносных программ используются возможности файлообменных P2P-сетей. Червь или троянская программа выкладывается в P2P-сеть под привлекательным названием. В поиске новых программ пользователи P2P-сетей скачивают файлы и запускают их на выполнение.

Технические приемы внедрения используются злоумышленниками для скрытной установки в компьютерную систему вредоносного кода. Цель состоит в том, чтобы не привлекать внимания владельца компьютера-жертвы. Для этого используются различные уязвимости в системе безопасности операционных систем и программного обеспечения. Такие уязвимости связаны с недокументированными возможностями либо ошибками реализации программного обеспечения. Они позволяют вредоносной программе внедриться и проникнуть в компьютер-жертву, которая далее самостоятельно запускается. Современные операционные системы и приложения работают в соответствии со сложными алгоритмами, имеют сложную структуру, выполняют множество различных задач. Поэтому гарантировать отсутствие ошибок или недокументированных возможностей нельзя. Злоумышленники пользуются этими обстоятельствами.

Достаточно часто применяются оба описанных метода в какой-либо комбинации. Например, метод социальной инженерии – для привлечения внимания жертвы, а технические приемы внедрения – для проникновения в систему. Один из ярких примеров такой комбинированной стратегии, почтовый

[1] См.: URL: https://encyclopedia.kaspersky.ru/knowledge/how-malware-penetrates-systems/

червь Mimail, использовался для кражи персональной информации пользователей интернет-кошельков системы e-gold. Распространялся он как вложение в электронное письмо. А для привлечения внимания жертвы в него встраивался специально оформленный текст. При запуске червя из вложенного в письмо архива применялась уязвимость в браузере Internet Explorer.

Контрольные вопросы

1. Дайте определение термина « информация».
2. Какие единицы используются для измерения количества информации?
3. Какие признаки используются для идентификации электронного документа?
4. Какие функциональные блоки входят в структурную схему компьютера и для чего они служат?
5. Назовите виды вредоносных программ.

Тема 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации

Глава 28 УК РФ включает нормы, предусматривающие ответственность за преступления в сфере компьютерной информации. Появление этой главы в УК РФ было обусловлено коренным изменением общественных отношений, формированием в России открытого информационного общества. Общественная опасность указанных преступлений обусловлена тем, что компьютеры и иные современные устройства и информация, которую они аккумулируют и предают, касаются всех сфер жизнедеятельности современного общества. Преступные вмешательства в компьютерную информацию могут поставить под угрозу осуществление банковских операций, социальное обеспечение, оборонную способность, транспортную инфраструктуру и, в конечно итоге, национальную безопасность. Именно поэтому уголовный закон, как и акты других отраслей права, защищает законные процессы сбора, обработки, накопления, хранения, поиска, распространения (передачи) информации.

Нормы, предусматривающие ответственность за преступления в сфере компьютерной информации, можно считать относительно молодыми, так как уголовное законодательство, предшествовавшее УК РФ 1996 г., не включало подобных предписаний. Система преступлений в сфере компьютерной информации сегодня объединяет четыре статьи: ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» и ст. 274^1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Надо сказать, что компьютерной техникой считаются не только традиционные персональные компьютеры и ноутбуки, но и планшеты, смартфоны, кассовые аппараты, банкоматы, терминалы по приему платежей и иные устройства, оперирующие с компьютерной информацией. Законность операций с любой информацией, в том числе и с компьютерной, будет зависеть от наличия согласия и допуска со стороны собственника или оператора, соблюдения требований к обработке и передаче данных и к эксплуатации компьютеров, их систем и сетей.

Родовым объектом преступлений в сфере компьютерной информации, исходя из названия Раздела IX УК РФ, выступает совокупность общественных отношений, направленных на охрану общественной безопасности и общественного порядка. В качестве видового объекта можно определить общественные отношения, возникающие в процессе создания и любых видов воздействия на компьютерную информацию.

Понятие «компьютерная информация» не нашло свое закрепление в специальном нормативном акте и законодательно определено только в примеча-

нии к ст. 272 УК РФ, где под ней предлагается понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Данное определение, по всей видимости, является производным от общего понятия информации, содержащегося в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1].

Как уже было сказано выше, главу 28 УК РФ открывает ***ст. 272 УК РФ «Неправомерный доступ к компьютерной информации».***

Непосредственным объектом данного преступления являются общественные отношения, обеспечивающие безопасность и правомерное использование компьютерной информации. Дополнительным объектом могут выступить отношения, обеспечивающие сохранность соответствующего вида тайны (налоговой, коммерческой, банковской), факультативным – отношения, охраняющие собственность или интересы государственной службы и службы в коммерческих организациях.

Предметом преступления, предусмотренного ст. 272 УК РФ, является охраняемая законом компьютерная информация.

В соответствии с положениями Федерального закона «Об информации, информационных технологиях и о защите информации» информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. В зависимости от категории доступа информация подразделяется на общедоступную и информацию, доступ к которой ограничен федеральными законами[2]. Обладатель информации, если иное не предусмотрено федеральными законами, вправе: разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; использовать информацию, в том числе распространять ее, по своему усмотрению; передавать информацию другим лицам по договору или на ином установленном законом основании; защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами; осуществлять иные действия с информацией или разрешать осуществление таких действий.

По конструкции объективной стороны состав преступления, предусмотренный ч. 1 ст. 272 УК РФ, материальный. Объективная сторона включает следующие обязательные признаки:

1) деяние в виде неправомерного доступа к информации;

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ.

[2] См., например: О государственной тайне: закон РФ от 21.07.1993 № 5485-1. URL: http://www.consultant.ru/; О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1. URL: http://www.consultant.ru/; О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ. URL: http://www.consultant.ru/

2) последствия в виде уничтожения, блокирования, модификации либо копирования информации;

3) наличие причинной связи между совершенным деянием и наступившими последствиями.

Под доступом к компьютерной информации следует понимать возможность получения информации и ее использования[1]. Здесь имеется в виду любая форма проникновения в источник информации с использованием средств (вещественных и интеллектуальных) в виде электрических сигналов, позволяющая манипулировать полученной информацией (копировать, модифицировать, блокировать либо уничтожать ее)[2].

Неправомерным становится доступ, который осуществляется без разрешения ее законного владельца и в нарушение порядка, установленного законодательством. Владелец может установить ограничения доступа посредством правовых, организационных, технических мер или иным способом.

Таким образом, неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты[3].

Что касается общественно опасных последствий, то под уничтожением информации необходимо понимать приведение ее или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Не будет считаться уничтожением информации простое переименование файла, а также автоматическая замена старой версии файлов новой. Перенос информации на другой носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен либо исключен.

Блокирование информации – это результат такого воздействия, последствием которого является постоянное или временное отсутствие возможности осуществлять над компьютерной информацией операции. Блокирование приводит к ограничению или полному прекращению доступа к компьютерному оборудованию и находящимся на нем ресурсам, не связанному с уничтожением компьютерной информацией.

При совершении деяния в виде модификации информации происходит изменение последней либо ее параметров. Если модификация осуществляется

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ.

[2] См.: Комментарий к Уголовному кодексу Российской Федерации (постатей.) / под ред. А. В. Бриллиантова. М.: Проспект, 2017. Т. 2. С. 643.

[3] См.: Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс».

законным владельцем или пользователем информации с целью исправления ошибок, обеспечения функционирования программы, базы данных на какомлибо устройстве либо для налаживания взаимодействия нескольких программ, то такая модификация является легальной и не влечет ответственности.

Копирование информации представляет собой перенесение ее на другое обособленное устройство (носитель) при сохранении неизменной первоначальной версии, а также воспроизведение информации в любой материальной форме путем переписывания от руки, фотографирования, а также считывания (перехвата).

Между деянием и перечисленными последствиями должна присутствовать причинно-следственная связь. Важно установить, что причиной стали целенаправленные действия, а не технические неисправности и ошибки в работе программного обеспечения. Для признания преступления оконченным достаточно наступления хотя бы одного из перечисленных в диспозиции статьи последствий. Наличие совокупности нескольких последствий на квалификацию не влияет.

Так, К., обладая достаточными познаниями в области пользования компьютерной техникой и навыками работы в телекоммуникационной сети «Интернет», путем подбора и ввода ответа на секретный вопрос («Девичья фамилия мамы») осуществила неправомерный доступ к охраняемой конфиденциальной компьютерной информации, для которой установлен специальный режим ее правовой защиты. Своими действиями К. с использованием средств компьютерной техники осуществила не разрешенный собственником доступ, позволяющий использовать полученную информацию, содержащуюся в электронном почтовом ящике, принадлежащем С. После чего К. изменила пароль доступа к указанному электронному почтовому ящику, блокировав компьютерную информация, следствием чего явилась невозможность для законного пользователя осуществить требуемые операции с компьютерной информацией. Затем К. путем удаления электронного почтового ящика уничтожила все находившиеся в нем электронные сообщения и электронные документы, что привело в непригодное для использования состояние указанную информацию[1].

Встречаются случаи неправомерного доступа к компьютерной информации в виде несанкционированной модификации программ, осуществляющих функционирование тех или иных сайтов в Интернете и размещения на их страницах различной информации, в том числе рекламного, оскорбительного или порнографического характера.

По мнению большинства исследователей, субъективная сторона преступления характеризуется умышленной формой вины[2]. Виновный осознает об-

[1] Приговор Дзержинского районного суда г. Оренбурга Оренбургской области от 28.01.2019 по делу № 1-55/2019 // ГАС «Правосудие».

[2] См., например: *Гайфутдинов Р. Р.* Понятие и квалификация преступлений против безопасности компьютерной информации: дис. … канд. юрид. наук. Казань, 2017.

щественную опасность деяния в виде неправомерного доступа предвидит возможность или неизбежность наступления последствий в виде уничтожения, блокирования, модификации либо копирования информации и либо желает наступление, этих последствий, либо не желает, но сознательно допускает их наступления или относится к их наступлению безразлично. Субъект данного преступления общий – физическое вменяемое лицо, достигшее 16-летнего возраста.

Законодатель установил повышенную ответственность, если помимо обозначенных в ч. 1 ст. 272 УК РФ последствий был причинен крупный ущерб (превышает один миллион рублей) или деяние было совершено из корыстной заинтересованности. Последняя означает стремление виновного получить для себя или других лиц выгоду имущественного характера (денег, имущества или прав на его получение и т. п.) либо избавиться от материальных затрат (освобождение от каких-либо имущественных затрат, погашения долга, оплаты услуг, уплаты налогов и т. п.).

В части 3 ст. 272 УК РФ предусмотрена ответственность за совершение анализируемого преступления группой лиц по предварительному сговору, организованной группой либо лицом с использованием своего служебного положения. Для квалификации по указанной части достаточно одного из перечисленных признаков.

Неправомерный доступ будет считаться совершенным группой лиц по предварительному сговору, если в его осуществлении участвовали два или более исполнителей, предварительно договорившихся о совместном совершении преступления. Каждый из исполнителей должен отвечать всем признакам субъекта и выполнить хотя бы часть объективной стороны.

Признак «совершенный организованной группой» может быть вменен только в том случае, если группа имела устойчивый характер. Об устойчивости группы может свидетельствовать длительность ее существования, постоянство состава участников, тщательность подготовки преступлений, использование одних и тех же форм и методов совершения посягательств. В каждом конкретном случае оценивается совокупность обстоятельств, указывающих на устойчивость. Организованная группа может иметь целью и совершение только одного, но требующего тщательной подготовки преступления.

Традиционно признак «с использованием служебного положения» вменяется, если лицо, совершившее преступление, являлось должностным лицом, лицом, выполняющим управленческие функции в коммерческих или иных организациях или государственным либо муниципальным служащим, не отвечающим признакам должностного лица[1]. Однако историческое толкование нормы приводит к выводу, что использующими служебное положение применительно к ст. 272 УК РФ должны признаваться те, кто имел возможность доступа к компьютерной информации в силу выполняемой работы (по трудо-

[1] См., например: О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // СПС «КонсультантПлюс».

вому, гражданско-правовому договору). Следовательно, субъектами квалифицированного состава могут стать программисты, системные администраторы, операторы и т. п.

В части 4 ст. 272 УК РФ предусмотрена ответственность за совершение обозначенных в ч. 1, ч. 2 или ч. 3 деяний, если они повлекли тяжкие последствия или создали угрозу их наступления. «Тяжкие последствия» – признак оценочный, и в каждом конкретном случае его содержание «отдается на откуп» правоприменителю. Тяжкими последствиями можно считать причинение по неосторожности смерти или тяжкого вреда здоровью хотя бы одному человеку; причинение средней тяжести вреда здоровью двум и более лицам; дезорганизацию деятельности органов государственной власти и местного самоуправления, крупные аварии, длительную приостановку или дезорганизацию работы общественного транспорта, какого-либо предприятия, учреждения или организации; длительное отключение потребителей от источников жизнеобеспечения – электроэнергии, газа, тепла, водоснабжения[1]; существенное ухудшение экологической обстановки; самоубийство или покушение на самоубийство потерпевшего[2].

Следующее общественно опасное деяние, включенное в главу 28 УК РФ, – ***создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).***

Непосредственным объектом указанного преступления являются общественные отношения, обеспечивающие безопасность компьютерной информации и средств ее защиты. Предметом преступления выступают компьютерные программы или иная компьютерная информация, предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

Компьютерная программа – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования компьютерного устройства с целью получения определенного результата. Программами, имеющими цель нейтрализации средств защиты или несанкционированного воздействия на информацию, считаются различные виды компьютерных вирусов (черви, троянские кони, кейлоггеры, руткиты и др.). Вредоностность программы определяется возможностью получения с помощью нее доступа к компьютерной информации и совершения действий с последней без согласия законного владельца или пользователя.

---

[1] См., например: Постановление Пленума Верховного Суда РФ от 05.06.2002 № 14 «О судебной практике по делам о нарушении правил пожарной безопасности, уничтожении или повреждении имущества путем поджога либо в результате неосторожного обращения с огнем» // СПС «КонсультантПлюс»; Постановление Пленума Верховного Суда РФ от 16.10.2009 № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» // СПС «КонсультантПлюс».

[2] См., например: Постановление Пленума Верховного Суда РФ от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» // СПС «КонсультантПлюс».

Назначение современных вирусных программ достаточно широкое. Они могут использоваться для хищения денежных средств, рассылки различного рода спама, блокирования доступа к файлам, предоставления виновному удаленного доступа, создания подложного дубликата сайта, внесения изменений в контрольно-кассовые аппараты.

По конструкции объективной стороны состав преступления, предусмотренный ч. 1 ст. 273 УК РФ, является формальным. Преступление считается оконченным с момента совершения одного из перечисленных в диспозиции деяний в виде создания, распространения, использования.

Создание вредоносных программ представляет собой совокупность действий, результатом которых является представление определенного алгоритма на языке программирования, способного несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

Под распространением программ понимается предоставление доступа к ним любому постороннему лицу любым возмездным или безвозмездным законным или незаконным способом, включая продажу, обмен, рассылку.

Использование вредоносной программы представляет собой применение ее с целью уничтожения, блокирования, модификации или копирования компьютерной информации или для нейтрализации средств защиты последней.

Понятия «уничтожение», «блокирование», «модификация», «копирование» были подробно рассмотрены при анализе признаков состава преступлений, предусмотренных ст. 272 УК РФ.

К средствам защиты компьютерной информации относятся технические, криптографические, программные и другие средства, предназначенные для защиты компьютерной информации, а также средства контроля эффективности защиты такой информации (например, антивирусные программы, программы предотвращения несанкционированного копирования информации, средства защиты, встроенные в операционные системы, и т. п.). Под нейтрализацией средств защиты компьютерной информации понимается уничтожение этих средств или ослабление их действия.

Так, судом был осужден Н., который в интересах и по просьбе Ш. на языке программирования Pascal создал алгоритм, т. е. исходные данные для вредоносной программы, названной Н. «sss.pas». Эта программа несанкционированно уничтожала бы дерево каталога после введения ее в любой удаленный персональный компьютер и функционировала бы без уведомления об этом его владельца при включении (загрузке) компьютера, т. е. выполняла бы не санкционированную пользователем модификацию информации, хранящейся на жестком диске[1].

[1] См.: *Дворецкий М., Копырюлин А.* Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ // Уголовное право. 2007. № 4. С. 30.

Другой пример.

Ч. предварительно изучил в информационно-телекоммуникационной сети «Интернет» инструкции по использованию вредоносных компьютерных программ, предназначенных для несанкционированного копирования информации и нейтрализации средств защиты компьютерной информации, а затем, используя свой персональный компьютер, имеющий доступ к сети «Интернет», загрузил с интернет-ресурсов на накопитель на жестких магнитных дисках вредоносные компьютерные программы: «Private Keeper», «MailsBrute», «SQL Map», заведомо предназначенные для несанкционированного копирования компьютерной информации и нейтрализации средств защиты компьютерной информации. Затем Ч. неоднократно использовал указанные вредоносные компьютерные программы для осуществления несанкционированного воздействие на сетевые ресурсы (подбор регистрационных данных (логин и пароль) от учетных записей пользователей на почтовых сервисах сети «Интернет», а также копирование информации из уязвимых баз данных)[1].

Субъективная сторона преступления характеризуется прямым умыслом. Виновный осознает общественную опасность деяний в виде создания, распространения или использования вредоносной компьютерной программы или компьютерной информации и желает их совершать. Признак заведомости означает, что умыслом виновного охватывается способность созданной им программы или информации уничтожать, блокировать, модифицировать или копировать иную информацию или нейтрализовать средства защиты.

Субъект преступления общий – физическое вменяемое лицо, достигшее 16-летнего возраста.

В части 2 ст. 273 УК РФ предусмотрено пять квалифицирующих признаков: три из них характеризуют способ (совершенное группой лиц по предварительному сговору, организованной группой, с использованием служебного положения), один – последствия (крупный ущерб), и еще один – мотив (корыстная заинтересованность). Признаки альтернативные, достаточно наличия хотя бы одного из них.

Часть 3 ст. 273 УК РФ предусматривает повышенную ответственность, если деяния, предусмотренные ч. 1 ил ч. 2, повлекли за собой тяжкие последствия или создали угрозу их наступления.

Содержание всех квалифицирующих признаков аналогично содержанию тех же признаков, включенных в ч. 2 и 3 ст. 272 УК РФ.

В статье 274 УК РФ предусмотрена ответственность за ***нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.***

[1] Приговор Вологодского городского суда Вологодской области от 08.10.2018 по делу № 1-726/2018 // ГАС «Правосудие».

Непосредственным объектом преступления являются общественные отношения, обеспечивающие правильную эксплуатацию компьютерной информации, информационно-телекоммуникационных сетей (далее – ИТКС), оконечного оборудования.

Предметом данного преступления являются средства хранения, обработки или передачи компьютерной информации, ИТКС, оконечное оборудование.

К средствам хранения, обработки или передачи компьютерной информации относятся электронные устройства, обеспечивающие реализацию информационных технологий (компьютер, сервер и т. д.). Как правило, указанные средства включают в себя аппаратное и программное обеспечение.

ИТКС – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[1].

Оконечное оборудование означает электронное устройство, используемое для связи пользовательского оборудования (компьютера, мультимедийного терминала и т. д.) с ИТКС (кабельный модем, сетевая карта).

По конструкции объективной стороны состав, предусмотренный ч. 1 ст. 274 УК РФ, материальный и включает три обязательных признака: 1) деяние в виде нарушения правил эксплуатации или правил доступа; 2) два уровня последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации и в виде крупного ущерба; 3) причинную связь между совершенным деянием и наступившими последствиями.

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации или ИТКС и оконечного оборудования представляет собой совершение действий (бездействия), связанных с нарушением правил эксплуатации либо аппаратного оборудования, либо программного обеспечения.

Нарушение правил доступа к ИТКС заключается в совершении действий (бездействия), которые связаны с несоблюдением правил пользования услугами по передаче данных в сети (например, несанкционированная рассылка спама, подмена IP-адреса, нелегальный доступ к различным ресурсам).

Для признания преступления оконченным необходимо, чтобы наступило хотя бы одно из последствий первого уровня (уничтожение, блокирование, модификация, копирование компьютерной информации) и последствие второго уровня (крупный ущерб). Содержание последствий обоих уровней было раскрыто при анализе состава преступления, предусмотренного ч. 1 ст. 272 УК РФ.

Диспозиция ч. 1 ст. 274 УК РФ имеет бланкетный характер и требует обращения к нормативным актам, регламентирующим соответствующие предписания. Верховный Суд РФ неоднократно разъяснял, что при вменении ли-

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ.

цу факта преступного нарушения каких-либо правил необходимо выяснять, в чем конкретно состояло нарушение, имеется ли причинная связь между допущенными нарушениями и наступившими последствиями[1]. Суд, установив в своем решении наличие такой связи, обязан сослаться не только на нормативные правовые акты, которыми предусмотрены соответствующие требования и правила, но и на конкретные нормы (пункт, часть, статья) этих актов, нарушение которых повлекло предусмотренные уголовным законом последствия, а также указать, в чем именно выразилось данное нарушение[2].

Субъективная сторона по отношению к последствиям может быть выражена виной в виде умысла или неосторожности. Виновный:

– осознает общественную опасность нарушения соответствующих правил, предвидит возможность или неизбежность наступления последствий в виде неправомерного воздействия на компьютерную информацию и крупного ущерба и либо желает наступления этих последствий, либо не желает, но сознательно их допускает или относиться к ним безразлично,

или

– предвидит возможность наступления последствий в виде неправомерного воздействия на компьютерную информацию и крупного ущерба и без достаточных к тому оснований рассчитывает на их предотвращение либо не предвидит наступления этих последствий, хотя при необходимой внимательности и предусмотрительности должен был и мог их предвидеть.

Субъект преступления специальный – физическое, вменяемое, достигшее 16-летнего возраста лицо, на которое в установленном порядке возложена обязанность соблюдать установленные правила эксплуатации или доступа.

Квалифицированный состав рассматриваемого деяния будет иметь место в том случае, если кроме указанных выше двух уровней последствий по неосторожности наступили еще тяжкие последствия или была создана угроза их наступления. Содержание тяжких последствий было раскрыто ранее.

Статья 274[1] УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» по существу представляет собой совокупность норм, специальных по отношению к общим нормам, заключенным в ст. 272, 273, 274 УК РФ. Основное отличие специальных норм состоит в том, что речь в них идет о компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации.

---

[1] См., например: Постановление Пленума Верховного Суда РФ от 05.06. 2002 № 14 «О судебной практике по делам о нарушении правил пожарной безопасности, уничтожении или повреждении имущества путем поджога либо в результате неосторожного обращения с огнем» // СПС «КонсультантПлюс».

[2] См., например: Постановление Пленума Верховного Суда РФ от 29.11.2018 № 41 «О судебной практике по уголовным делам о нарушениях требований охраны труда, правил безопасности при ведении строительных или иных работ либо требований промышленной безопасности опасных производственных объектов» // СПС «КонсультантПлюс».

Под критической информационной инфраструктурой (далее – КИИ) понимаются объекты ККИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Объекты КИИ – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ. К субъектам КИИ относятся государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей[1].

Составы преступления, сформулированные в ч. 1, 2 и 3 ст. 274[1] УК РФ, являются самостоятельным и соотносятся между собой как основные.

В части 1 ст. 274[1] УК РФ предусмотрена ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации. Норма является специальной по отношению к норме, предусмотренной ч. 1 ст. 273 УК РФ. Если в ст. 273 УК РФ идет речь о воздействии на любую компьютерную информацию и средства ее защиты, то в ч. 1 ст. 274[1] УК РФ – на информацию, содержащуюся в КИИ РФ, и средства ее защиты. В качестве наказания в общей норме есть ограничение свободы, в специальной – только принудительные работы или лишение свободы (срок выше на 1 год).

Основным непосредственным объектом преступления выступают общественные отношения, обеспечивающие сохранность информации, содержащейся в КИИ РФ. Предметом являются компьютерные программы или компьютерная информация, заведомо предназначенные для неправомерного воздействия на КИИ РФ или нейтрализации средств ее защиты.

По конструкции объективной стороны состав формальный и включает один обязательный признак: 1) деяние в виде создания, распространения или использования вредоносных программ или информации. Преступление окончено с момента совершения хотя одного из них.

---

[1] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ // СПС «КонсультантПлюс».

Субъективная сторона характеризуется виной в виде прямого умысла. Виновный осознает общественную опасность создания, распространения или использования программ, неправомерно воздействующих на КИИ РФ или средства ее защиты, и желает эти деяния совершать.

Субъект общий – физическое вменяемое лицо, достигшее 16 лет.

В части 2 ст. 274[1] УК РФ установлена ответственность за неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ РФ, или иных вредоносных компьютерных программ, если он повлек причинение вреда КИИ РФ. В отличие от приведенной норма общая (ч. 1 ст. 272 УК РФ) не акцентировала внимание на способах воздействия и включала только четыре вида последствия: уничтожение, блокирование, модификация или копирования компьютерной информации. Ответственность, если говорить о наказании в виде лишения свободы, в санкции специальной нормы выше на четыре года.

Основной непосредственный объект анализируемого состава включает общественные отношения, охраняющие порядок доступа к охраняемой компьютерной информации, содержащейся в КИИ РФ. Последняя будет выступать в качестве предмета.

Состав ч. 2 ст. 274[1] УК РФ сконструирован по типу материального. Объективная сторона объединяет деяние в виде неправомерного доступа к указанной выше информации, последствия в виде причинения вреда КИИ РФ, причинную связь между деянием и последствием.

Что понимается под неправомерным доступом было подробно рассмотрено выше. Последствия в виде причинения вреда КИИ РФ будут включать себя как те последствия, что указаны в диспозиции ч. 1 ст. 272 УК РФ (уничтожение, блокирование, модификация, копирование), так и любые иные, в результате которых КИИ подвергается опасности.

Способ совершения преступления может быть любой, в том числе путем использования компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ РФ, или иных вредоносных программ.

Субъективная сторона, как и в случае со ст. 272 УК РФ, выражена умышленной формой вины. Виновный осознает общественную опасность деяния в виде неправомерного доступа предвидит возможность или неизбежность наступления последствий в виде причинения ущерба КИИ РФ и, либо желает наступления этих последствий, либо не желает, но сознательно допускает их наступления или относится к их наступлению безразлично.

Субъектом может быть любое физическое вменяемое лицо, достигшее 16 лет.

Еще один самостоятельный состав преступления сформулирован в ч. 3 ст. 274[1] УК РФ, где установлена ответственность за нарушение правил эксплуа-

тации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, или информационных систем, информационно-телекоммуникационных сетей (далее – ИТКС), автоматизированных систем управления, сетей электросвязи, относящихся к КИИ РФ, либо правил доступа к указанным информации, информационным системам, ИТКС, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда КИИ РФ. Данный состав представляет собой специальную разновидность состава, предусмотренного ч. 1 ст. 274 УК РФ.

Основной непосредственный объект – это совокупность общественных отношений, обеспечивающих безопасность компьютерной информации, содержащейся в КИИ РФ или информационных систем, ИТКС, автоматизированных систем управления, сетей электросвязи, относящиеся к КИИ РФ.

Предметом данного преступления являются средства хранения обработки или передачи информации, информационные системы, ИТКС, автоматизированные системы управления, сети электросвязи.

Часть указанных терминов была раскрыта выше.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[1]. Автоматизированная система управления – комплекс аппаратных и программных средств, информационных систем и ИТКС, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами. Сеть электросвязи – это технологическая система, включающая в себя средства и линии связи и предназначенная для передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

По конструкции объективной стороны состав является материальным и включает три обязательных признака: 1) деяние в виде нарушения правил эксплуатации или правил доступа; 2) последствия в виде причинения вреда КИИ РФ; 3) причинную связь между деянием и последствием.

По отношению к последствиям форма вины может быть как умышленной, так и неосторожной.

Субъект специальный, физическое вменяемое лицо, достигшее 16 лет и наделенное обязанностью соблюдать правила эксплуатации или доступа.

Признаки, квалифицирующие деяния, предусмотренные ч. 1, 2 или 3 ст. 274[1] УК РФ, аналогичны квалифицирующим признакам, рассмотренным при анализе составов преступлений, предусмотренных ст. 272 УК РФ.

К сожалению, в открытом доступе пока нет судебных решений по уголовным делам, возбужденным по признакам преступлений, предусмотренных ст. 274[1] УК РФ.

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ.

Контрольные вопросы

1. Что понимается под неправомерным доступом для целей ст. 272 УК РФ?

2. Какая сумма образует крупный ущерб применительно к преступлениям главы 28 УК РФ?

3. Что понимается под распространением для целей ст. 273 УК РФ?

4. Кто может быть субъектом преступления, предусмотренного ст. 274 УК РФ?

5. Как соотносятся между собой по степени общественной опасности составы преступлений, предусмотренные ч. 1, 2 и 3 ст. 274^1 УК РФ?

ТЕМА 3. КОМПЬЮТЕРНОЕ ДОКАЗАТЕЛЬСТВО

Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ под *информацией* следует понимать не зависящие от формы представления сведения о лицах, предметах, фактах, событиях, явлениях и процессах, уменьшающие степень их неопределенности для субъекта (получателя). Всю существующую информацию можно назвать социальной по источнику возникновения в ней следует выделить компьютерную информацию. Таким образом, компьютерная информация является видовым понятием по отношению к социальной информации.

Выделение компьютерной информации как самостоятельного вида обусловлено прежде всего источником ее возникновения – компьютером, интеллектуальной машиной, способной к созданию качественно новой информации.

Такую способность дает компьютеру программное обеспечение, по сути, являющееся формализованным отображением интеллекта своих создателей.

Компьютерная информация содержится на соответствующих носителях (носители компьютерной информации): магнитные, магнитооптические, оптические накопители, запоминающие устройства в виде интегральных схем (например, оперативная память персонального компьютера) и иные материальные объекты и устройства, способные хранить информацию в числовом машиночитаемом виде.

Полем их совпадения являются созданные или полученные человеком с помощью компьютера, любым другим способом обработанные на нем сведения (включая их нахождение в его функциональных устройствах) о лицах, предметах, фактах, событиях, явлениях и процессах, протекающих в правовой сфере, используемые государством и обществом для решения задач правотворчества, правоприменительной и правоохранительной деятельности, защиты прав и свобод личности, а также программы (наборы команд), предназначенные для обработки указанных сведений.

В этом поле находится и компьютерная информация, используемая в разном качестве и в различных целях на досудебных стадиях уголовного судопроизводства.

Основной функцией компьютера является обработка информации.

Однако под *обработкой информации* компьютером следует понимать не только обработку формализованной информации (данных), но и сам процесс формализации информации. Термин «обработка информации» должен трактоваться достаточно широко. Отсюда следует вывод, что информация, получаемая, хранимая и воспроизводимая компьютером, должна быть отнесена к категории компьютерной информации как информация, прошедшая компьютерную обработку.

Соответственно, *условиями возникновения компьютерной информации* являются:

1) непосредственно обработка информации компьютером;

2) создание новой информации в процессе обработки имеющейся. Создателями же ее выступают человек (пользователь) и компьютер: один – ставя задачу, другой – ее решая.

Создателем информации может являться не только отдельный компьютер, но и компьютерная сеть, так как зачастую компьютеры в сети бывают сориентированы на решение одной общей задачи, поэтому единая ценностно-смысловая порция информации создается несколькими сетевыми компьютерами, взаимодействующими между собой.

Любая информация, в том числе и компьютерная, непременно имеет носитель и форму выражения (информационный код).

По способу представления носители компьютерной информации предлагается разделить на три вида:

– традиционные носители – бумажные;

– машинные носители;

– компьютерные сети.

Преступление – это событие прошлого. Поэтому выяснение обстоятельств, имеющих значение для уголовного дела, происходит посредством доказательств. Познание прошлого события возможно благодаря отражению – свойству материи, в силу которого все явления, вещи и процессы реального мира находятся во взаимосвязи и взаимозависимости. Любой предмет материального мира отражает на или в себе признаки другого предмета, с которым взаимодействует в виде следов, отпечатков, образов. Способность вещей и людей к отражению делает их носителями информации об обстоятельствах, подлежащих доказыванию по уголовному делу. Сведения, полученные от объекта-носителя, облекаются в процессуальную форму с помощью процессуальных действий, производимых органом уголовного судопроизводства. В результате этой деятельности и возникает (а точнее, формируется) доказательство.

Обстоятельства, подлежащие доказыванию по ст. 73 УПК РФ, устанавливаются при помощи доказательств, которыми, в соответствии со ст. 74 УПК РФ, являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела. Основу доказательства составляют фактические данные. Это означает, что лишь сведения о конкретных фактах могут быть доказательствами. Отсюда следует, что предположения и догадки, основанные на слухах и не подтвержденные конкретными фактами не могут служить доказательствами (часть вторая ст.75 УПК РФ).

Именно в связи с этим особую сложность приобретает процесс доказывания преступлений, ответственность за совершение которых предусмотрена главой 28 УК РФ – «Преступлений в сфере компьютерной информации» – в связи с тем, что в этой категории преступлений достаточно сложно установить конкретные фактические данные, необходимые для расследования дела в силу отсутствия письменных и вещественных доказательств либо сложностей в их получении, а еще сложнее – получить достаточный для расследования и дальнейшего рассмотрения дела доказательственный материал.

При расследовании преступлений в сфере компьютерной информации таких фактов, как правило, не бывает, в силу чего особое значение приобретает правильное, с точки зрения УПК РФ, документальное закрепление тех фактов, которые составляют доказательственную базу и которые не могут быть восприняты непосредственно.

Если рассматривать место и значение компьютерной информации в теории уголовно-процессуальных доказательств, то за основу взята концепция трехзвенной структуры доказательств, предложенная А. А. Давлетовым:

1) источник сведений;

2) сведения об обстоятельствах, имеющих значение для дела;

3) процессуальная форма закрепления источника и сведений об обстоятельствах, имеющих значение для дела.

Компьютерная информация по своей сути является сведениями о фактах (обстоятельствах), что дает почву для исключения ее из предмета доказывания. Однако компьютерная информация не существует сама по себе вне субъекта, на вещном носителе. Процесс ее возникновения, передачи, уничтожения имеет материальное проявление. Из этого следует вывод о том, что компьютерная информация может не только выступать в качестве доказательств в уголовном судопроизводстве, но и входить в общий предмет доказывания (ст. 73 УПК РФ), а также в категорию иных обстоятельств, имеющих значение для уголовного дела, т. е. промежуточных фактов, входящих в предмет доказывания по конкретным уголовным делам (ч. I ст. 74 УПК РФ).

Компьютерная информация обладает следующими уникальными свойствами:

1) может быть в одном случае составляющей доказательства, а в другом – одним из обстоятельств, подлежащих установлению по делу, т. е. предметом доказывания;

2) может выступать частью орудия преступления (когда орудие в целом – компьютер);

3) может выступать средством совершения преступления;

4) факт ее создания может обозначать юридический факт возникновения уголовно-правовых отношений (ст. 273 УК РФ), а реальность совпадения этих фактов – служить основанием возникновения уголовно-процессуальных отношений.

Специальный механизм образования выделяет компьютерную информацию в самостоятельный вид доказательств. Способ образования компьютерной информации определяется алгоритмом соответствующей программы. Принимая во внимание, что вся материя обладает свойством отражения, то программа в данном случае является средством отражения фактов. Отражение происходит посредством аппаратных и программных средств опосредованно, через интеллектуальное сознание человека (разработчика программы). Сама же компьютерная информация непосредственно не воспринимается. Только с помощью аппаратных и программных средств становится возможным восприятие сведений, содержащихся в компьютерной информации. Однако и воспринятая с помощью аппаратных и программных средств компьютерная информация – это еще не доказательство. Данные сведения могут приобрести статус доказательств только тогда, когда приобретут надлежащую уголовно-процессуальную форму.

Статус доказательства компьютерная информация приобретает посредством следственных и процессуальных действий. Для того чтобы компьютерная информация стала доказательством, необходимо сначала осмотреть ее по правилам осмотра предмета. Во время осмотра компьютерная информация обязательно воспроизводится с помощью технических и программных средств с участием специалиста. Осмотр оформляется протоколом, в котором отражается краткое содержание сведений, содержащихся в осматриваемой компьютерной информации и имеющих отношение к обстоятельствам, подлежащим доказыванию, реквизиты воспроизводимой информации (реквизиты файла), программные средства, необходимые для воспроизведения информации. Содержание файла распечатывается и прилагается к протоколу осмотра в виде приложения. После чего выносится постановление о приобщении носителя компьютерной информации в качестве вещественного доказательства к материалам дела.

Из вышесказанного следует, что процесс формирования компьютерной информации (как и других доказательств) делится на две стадии: внепроцессуальную и процессуальную. На внепроцессуальном этапе образуются виртуальные следы в виде самой компьютерной информации, ее реквизитов и соответствующей компьютерной программы. На процессуальном этапе проис-

ходит восприятие и фиксация содержания компьютерной информации (виртуальных следов) в процессуальных документах. Переход от внепроцессуальной к процессуальной стадии происходит путем опосредованного познания. В отличие от иных видов процесс формирования компьютерного доказательства состоит в том, что сведения, содержащиеся в компьютерной информации, рассматриваемой как доказательство, являются результатом неоднократного отображения обстоятельств события преступления. Первоначально это создание сведений с помощью программных средств, далее обнаружение этих сведений с привлечением других программных средств, воспроизведение (отображение содержания данных сведений), отображение в сознании следователя, других участников следственного (судебного) действия, в процессуальных документах.

Контрольные вопросы

1. Дайте понятие доказательства.
2. Раскройте структуру доказательства.
3. Раскройте понятие доказательственной информации с электронных носителей.
4. Дайте понятие компьютерной информации.
5. Перечислите носители компьютерной информации.
6. Назовите особенности механизма формирования компьютерного доказательства.

Тема 4. Действия следователя на первоначальном этапе расследования преступлений в сфере компьютерной информации. Типичные следственные ситуации

§ 4.1. Особенности возбуждения уголовного дела по преступлениям в сфере компьютерной информации. Признаки подготовки, совершения и сокрытия компьютерных преступлений

Анализ уголовных дел свидетельствует о том, что в настоящее время раскрывается только 25 % преступлений в сфере компьютерной информации. Отчасти причина малого выявления данных составов преступлений связана с их латентностью. Потерпевшие не всегда заявляют в правоохранительные органы о совершенных в отношении них противоправных действиях. Несмотря на это самым распространенным источником информации о совершенном деянии являются заявления от граждан и организаций.

Поводами для возбуждения уголовных дел данной категории чаще всего служат:

– заявления граждан (чаще всего такие заявления поступают от лиц, являющихся в дальнейшем потерпевшими);

– рапорта об обнаружении признаков преступлений (в том случае если преступление выявлено сотрудниками правоохранительных органов в рамках следственных действий или оперативно-разыскных мероприятий);

– сообщения из иных источников (например, информация из средств массовой информации).

Одним из самых распространенных поводов являются сообщения предприятий и организаций, поступившие от руководителей или должностных лиц этих учреждений.

По оценкам практиков, из всего массива зарегистрированных компьютерных преступлений, факты их совершения были выявлены следующим образом:

– в результате регулярных проверок организаций собственными службами коммерческой безопасности – 31 %;

– с помощью агентурной работы, а также при проведении оперативных мероприятий по проверкам заявлений граждан – 28 %;

– случайно – 19 %;

– в ходе проведения налоговых, бухгалтерских ревизий – 13 %;

– в ходе расследования других видов преступлений – 10 %[1].

Учеными выделяются следующие признаки подготовки, совершения и сокрытия преступлений в сфере компьютерной информации:

[1] См.: *Сизов А. В.* Причины и условия совершения преступлений в сфере компьютерной информации // Информационное право. 2008. № 2 // СПС «КонсультантПлюс».

• появление в ЭВМ, системе ЭВМ или их сети фальшивых данных;

• несанкционированные изменения структуры файловой системы, программного обеспечения и конфигурации ЭВМ, системы ЭВМ или их сети;

• необычные (нестандартные) проявления в работе ЭВМ и их программного обеспечения; частые сбои в работе аппаратуры;

• жалобы клиентов на предоставление некачественного доступа к ЭВМ, системе ЭВМ, их сети или компьютерной информации; сверхурочная работа некоторых сотрудников на ЭВМ, в системе ЭВМ или их сети, нарушение установленного графика их эксплуатации; нерегламентированный доступ к ЭВМ, системе ЭВМ, их сети и к компьютерной информации отдельных субъектов;

• нарушение правил работы с компьютерной информацией и несанкционированные манипуляции с ней;

• чрезмерный интерес отдельных субъектов (клиентов, сотрудников) к содержанию чужих распечаток (листингов) и компьютерной информации определенной категории; случаи перезаписи отдельных данных и компьютерной информации без серьезных на то причин;

• применение на рабочем месте и вынос с работы личных машинных носителей информации под различными предлогами (записи игр и т. п.); исследование мусорных корзин (контейнеров) с технологическими отходами компьютерной обработки информации; случаи утечки конфиденциальной информации либо обнаружение негласных устройств ее получения;

• нарушение установленных правил оформления документов при работе с ЭВМ, системой ЭВМ, их сетью или компьютерной информацией; создание копий определенной категории данных и компьютерной информации, не предусмотренных технологическим процессом; несоответствие данных, содержащихся в первичных (исходных) документах, данным машинограмм и иным более поздним по времени создания документам; подозрительно частое обращение одного и того же пользователя к данным и компьютерной информации определенной категории[1].

Итак, преступления, предусмотренные ст. 272–274.1 УК РФ подследственны органам предварительного следствия. Данная категория дел относится к категории сложных. Раскрывать преступления в сфере компьютерной информации нелегко, так как в большинстве случаев они латентны. Поводами для возбуждения уголовных дел данной категории чаще всего служат заявления организаций, рапорта об обнаружении признаков преступлений, сообщения из иных источников.

[1] См.: *Дуленко В. А., Мамлеев Р. Р., Пестриков В. А.* Указ. соч.

§ 4.2. Особенности проверки сообщений о преступлениях в сфере компьютерной информации и организация взаимодействия следователя с оперативными сотрудниками правоохранительных органов

Как правило, возбуждению уголовного дела предшествует предварительная проверка материалов, поступивших в правоохранительные органы. Успех раскрытия и дальнейшего расследования зависит от оперативности действий служб в первые часы после совершения преступления; грамотного и эффективного взаимодействия между следователем и оперативником; привлечения к участию в проверке сообщения и производству процессуальных действий специалиста в области компьютерной техники.

В ходе проверки поступивших к следователю материалов при решении вопроса о возбуждении уголовного дела он должен четко представлять следующее:

– предмет преступного посягательства и его особенности;

– объект, на котором находится или находился предмет посягательства;

– условия его охраны;

– особенности деятельности объекта (порядок учета документации, виды отчетности, систему документооборота) и его структуру;

– характеристику используемой компьютерной техники;

– технологии производства;

– должностных лиц, являющихся руководителями организации, предприятия, их полномочия в отношении предмета посягательства;

– служебные обязанности работников объекта (их права и обязанности по отношению к предмету посягательства).

В материалах проверки, необходимых для принятия решения о возбуждении уголовного дела, с учетом специфики компьютерных преступлений должен содержаться ряд сведений и документов:

1) письменное заявление потерпевшего – гражданина или представителя юридического лица либо протокол принятия устного заявления о преступлении, составленный в соответствии с действующим уголовно-процессуальным законодательством;

2) рапорт об обнаружении признаков преступления и приложенные к нему материалы, полученные в ходе производства оперативно-разыскных мероприятий, ревизий, документальных и иных проверок;

3) письменное объяснение заявителя, в котором содержатся данные о времени и месте совершения и обнаружения преступления, предмете преступного посягательства и его индивидуальных признаках (название компьютерной информации, место ее нахождения, особые условия доступа к ней и ее машинному носителю, их индивидуальные признаки и др.);

4) документы либо их копии, подтверждающие право собственности (владения, распоряжения или использования) на компьютерную информацию,

ЭВМ, систему ЭВМ или их сеть, подвергшиеся преступному воздействию: письменный договор на получение услуг сети Интернет, электросвязи по конкретному абонентскому номеру или обслуживание по банковской карте в определенной кредитно-финансовой организации; пластиковая карта (банковская, телефонная, проездная, удостоверительная, парковочная и иная); документ о праве обладания (пользования) программой для ЭВМ, базой данных, электронным ресурсом сети Интернет, электронной цифровой подписью; документ, в котором отражены конфиденциальные сведения, несанкционированно распространенные кем-либо в сети Интернет;

5) письменное заключение специалиста и (или) заключение экспертов, проводивших исследование средств хранения, обработки, защиты или передачи компьютерной информации и информационно-телекоммуникационных сетей, вредоносных компьютерных программ, охраняемой законом компьютерной информации;

6) идентификационные данные о владельце (собственнике, пользователе) компьютерного устройства и его программного обеспечения, возможно, осуществившем несанкционированный доступ к компьютерной информации, например: IP-адрес, IMEI или иной идентификатор устройства в информационно-телекоммуникационной сети либо сети электросвязи, а также логин, пароль и номер абонента в сети электросвязи (номер телефона), с помощью которых был осуществлен такой доступ;

7) протокол осмотра места происшествия, предметов и документов, в т. ч. электронных носителей информации, электронных документов, электронных сообщений, сайта или страницы в сети Интернет;

8) документы, подтверждающие факт распространения вредоносных компьютерных программ или электронных носителей с такими программами: кассовый, товарный или иной чек; протокол проведения соответствующего оперативно-разыскного мероприятия и приложенные к нему документы.

Все вышеуказанные документы и содержащиеся в них сведения необходимо оценить с позиций законности получения, достоверности и достаточности для принятия того или иного процессуального решения. В этих целях исключительно важное значение имеют консультации со специалистами[1].

Решение о возбуждении уголовного дела принимается не только на основании материалов предварительных проверок заявлений потерпевших, организаций и должностных лиц, но и, как указывалось выше, по материалам органов, осуществляющих оперативно-разыскную деятельность при реализации оперативных разработок, результатов оперативно-разыскных мероприятий по выявлению преступлений в сфере компьютерной информации и лиц, их совершивших.

В соответствии со ст. 11 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» ее результаты могут служить по-

[1] См.: *Вехов В. Б.* Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации // Эксперт-криминалист. 2013. № 4. С. 3–4.

водом и основанием для возбуждения уголовного дела и использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства, регламентирующими собирание, проверку и оценку доказательств.

В материалах проверки также могут быть и иные документы, предоставляемые по результатам оперативно-разыскных мероприятий (далее – ОРМ), такие как:

– постановление о предоставлении результатов ОРД следователю;

– постановление о рассекречивании этих материалов;

– протоколы ОРМ (оперативного наблюдения, проверочной закупки при распространении носителей с вредоносными компьютерными программами, оперативного эксперимента и т. д.);

– стенограммы прослушивания телефонных переговоров и иных сообщений по преступлениям средней тяжести, тяжким и особо тяжким, детализации телефонных соединений абонентов с обязательным получением судебного решения;

– протоколы об изъятии образцов для сравнительного исследования с участием специалистов;

– протоколы (акты) изъятия компьютерной техники и электронных носителей информации;

– справки об исследовании компьютерной техники и других видов необходимых первоначальных исследований и другие материалы в зависимости от каждой конкретной ситуации.

Результаты оперативно-разыскных мероприятий, ревизий, документальных и иных проверок, включая рапорт сотрудника, выявившего преступление, регистрируются в дежурной части и передаются в следственное подразделение с сопроводительным письмом о передаче материалов проверки от имени начальника органа дознания (руководителя оперативного подразделения). Процедура передачи материалов, полученных оперативным путем, дознавателю предусмотрена инструкцией, утвержденной в соответствии с приказом МВД России, МО РФ, ФСБ России, ФСО РФ, ФТС, СВР РФ, ФСИН, ФСКН РФ, СК РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68.

Закон запрещает в процессе доказывания использовать результаты ОРД в случае, если они не отвечают требованиям, предъявляемым к доказательствам (ст. 89 УПК РФ), иначе доказательства будут признаны недопустимыми.

Так, Самарский областной суд в своем апелляционном определении по уголовному делу в отношении Рябченко А. П., обвиняемого по п. в ч. 3 ст. 146, ч. 2 ст. 272, ч. 2 ст. 273 УК РФ, указал, что помимо отмеченных доказательств вина Рябченко А. П. в совершении инкриминируемых ему преступлений подтверждается:

– протоколом осмотра места происшествия с участием Рябченко А. П. от ДД.ММ.ГГГГ с фототаблицей, в ходе которого в квартире, расположенной по адресу: <адрес>, были обнаружены и изъяты: системный блок с установлен-

ными программными продуктами «Компас-3D V15. 2.0», жесткий диск «Verbatim 500 Gb», денежные средства в сумме 1200 рублей, выданные закупщику ФИО2 для проведения проверочной закупки;

– протоколом явки с повинной Рябченко А. П. от ДД.ММ.ГГГГ;

– заявлением представителя потерпевшего ООО о привлечении к уголовной ответственности Рябченко А. П. за нарушение авторских прав правообладателя в размере 1 971 100 рублей, связанное с установкой программного продукта «Компас-3D V15»;

– свидетельством о государственной регистрации программы для ЭВМ №*** в отношении системы трехмерного моделирования «Компас-3D V15», правообладатель ООО;

– справкой о стоимости с прейскурантом цен трех программ «Компас-3D V15. 2.0» и библиотек в общей сумме 1 971 100 рублей;

– заключением эксперта от ДД.ММ.ГГГГ №***, согласно которому на представленном системном блоке обнаружен программный продукт «Компас-3D V15. 2.0» с признаками контрафактности, установленный ДД. ММ.ГГГГ с дистрибутива, находящегося на представленном жестком диске объемом 500 Гб, активированный с помощью самостоятельного копирования модифицированных библиотек и программных компонентом с жесткого диска в корневую систему программного продукта на системном блоке, применив которые, осуществляется возможность нейтрализации системы защиты от несанкционированного использования, предусмотренной правообладателем, и воспроизводства программы;

– зафиксированными результатами оперативно-разыскных мероприятий, проведенных сотрудниками правоохранительных органов, по результатам которых был задержан Рябченко А. П., в том числе: заявлением гражданина П., актом исследования денежных средств, в ходе которого денежные купюры в сумме 1200 рублей были помечены и выданы гражданину П., актом проверочной закупки об установке Рябченко А. П. за денежное вознаграждение в сумме 1200 рублей контрафактного программного обеспечения «Компас-3D»[1].

Полученные в приведенном примере доказательства были проверены судом с соблюдением положений ст. 87 УПК РФ. С учетом требований ст. 88 УПК РФ им дана надлежащая оценка с точки зрения относимости, допустимости и достоверности, а в совокупности – достаточности для разрешения уголовного дела по существу. Суд оценил, что приведенные в приговоре доказательства были получены в соответствии с требованиями уголовно-процессуального закона.

Важной составляющей проверочных материалов при возбуждении уголовного дела являются также:

[1] Апелляционное определение судебной коллегии по уголовным делам Самарского областного суда № 22-2611/2018. URL: https://rospravosudie.com/court-samarskij-oblastnoj-sud-samarskaya-oblast-s/act-581971950/

– объяснения сотрудников (персонала) потерпевшей организации;

– администраторов сети, инженеров-программистов, разработавших программное обеспечение и осуществляющих его сопровождение (т. е. отладку и обслуживание);

– операторов и специалистов, занимающихся эксплуатацией и ремонтом компьютерной техники;

– системных программистов, инженеров по средствам связи и телекоммуникационному оборудованию;

– специалистов, обеспечивающих информационную безопасность, работников службы безопасности и других лиц.

Из данных объяснений можно выяснить следующие обстоятельства:

– обстоятельства обнаружения факта преступления (признаков его совершения, способов и средств, наступивших негативных последствий);

– наличие и функционирование информационной защиты, ее недостатки;

– иные причины и условия, которые могли быть использованы для совершения противоправных действий.

Для принятия решения должностное лицо, осуществляющее проверку сообщения, совместно с оперативными службами должно изучить достаточное количество справочной литературой, знать основные нормативные акты федерального и ведомственного уровня. Здесь особое значение имеет взаимодействие со специалистами для получения информации технического характера. Оказать помощь следователю в данной ситуации могут любые лица, обладающие необходимыми знаниями и опытом для дачи консультаций по делу. Это квалифицированные сотрудники различных организаций, осуществляющих свою деятельность в сфере информации, информатизации и защиты информации.

Можно выделить несколько подразделений и служб, оказывающих содействие в раскрытии такого рода преступлений:

• Федеральной службы по техническому и экспортному контролю;

• центров защиты информации;

• оперативно-технических подразделений правоохранительных органов;

• подразделений «К» при БСТМ МВД России[1];

• межрегиональных Центров защиты информации, функционирующих на базе гражданских высших учебных технических заведений;

• исследовательских институтов и лабораторий, а также учебных заведений.

К основным направлениям работы Управления «К» МВД России относятся:

1. Борьба с преступлениями в сфере компьютерной информации.

2. Пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет.

[1] Бюро специальных технических мероприятий – подразделение МВД России, одним из направлений деятельности которого является борьба с преступлениями в сфере компьютерных технологий. Образовано 19 октября 1992 г.

3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

4. Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий.

5. Борьба с международными преступлениями в сфере информационных технологий.

6. Международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий[1].

БСТМ МВД России активно взаимодействует с правоохранительными органами иностранных государств, как на двусторонней, так и многосторонней основе (ООН, СНГ, СЕ, ЕС, ШОС, АТР и др.).

Собрав необходимые сведения, следователь переходит к изучению поступивших материалов доследственной проверки с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка передачи в органы следствия. В случае необходимости он принимает меры к получению недостающей информации путем возвращения материалов в орган дознания с соответствующим письменным указанием о проведении дополнительных проверочных и следственных действий, оперативно-разыскных мероприятий.

Надзор за исполнением законов при приеме, регистрации и разрешении сообщений о преступлениях в сфере компьютерной информации и их расследованием возложен на органы прокуратуры. Прокурору необходимо руководствоваться не только положениями уголовно-процессуального законодательства, но и требованиями ведомственных приказов.

Таким образом, чтобы законно и оперативно принять решение и возбудить уголовное дело по компьютерным преступлениям и организовать их расследование на первоначальном этапе, необходимо грамотное и четкое взаимодействие не только между следователем и оперативными службами, но и с операторами связи и специалистами в сфере компьютерных технологий. Это взаимодействие должно быть спланировано и отражаться в плане совместных следственных и оперативно-разыскных мероприятий по уголовному делу.

§ 4.3. Типичные следственные ситуации, версии и действия на первоначальном этапе расследования компьютерных преступлений

По данным статистического опроса сотрудников правоохранительных органов и судов по вопросам уголовно-правового противодействия преступлениям, совершаемым в сфере использования информационно-коммуникационных технологий[2], на вопрос о том, испытывают ли практики трудности при квалификации и расследовании компьютерных преступлений, 60 % ответили, что испытывают, и 40 % затруднились с ответом.

---

[1] См.: Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii

[2] См.: *Хисамова З. И.* Указ. соч. С. 215.

Причины возникающих трудностей в расследовании данных уголовных дел мы видим в следующем.

Во-первых, рост развития компьютерных технологий значительно обгоняет правовое регулирование проблемных вопросов законодателем. Это касается не только уголовного процесса, но и многих других отраслей права, положения которых должны регулировать отношения, возникающие в сферах, где используются информационно-телекоммуникационные технологии.

Во-вторых, деятельность должностных лиц, осуществляющих раскрытие и расследований компьютерных преступлений, требует серьезного совершенствования (повышения квалификации). Причем это замечание актуально не, только для юристов и правоохранителей, но и программистов, «айтишников».

Указанные выводы подтверждают необходимость разработки четкого алгоритма действий должностных лиц правоохранительных органов, которые сталкиваются с организацией расследования преступлений в сфере компьютерных технологий.

На первоначальном этапе необходимо определить предмет доказывания и его пределы. Соответственно, в ходе расследования данного рода преступлений подлежат установлению, а в дальнейшем доказыванию такие обстоятельства, как:

– факт создания и использования вредоносных программ, несанкционированного доступа к компьютерной информации;

– место и время несанкционированного проникновения в систему или сеть;

– надежность средств защиты компьютерной информации;

– способ совершения преступления;

– лица, совершившие, их виновность и мотивы;

– последствия неправомерного доступа к компьютерной информации;

– обстоятельства, способствовавшие созданию и использованию вредоносных программ.

На первоначальном этапе расследования необходимо выдвинуть версии совершенного преступления, которые делятся на общие и частные.

Выдвигаются следующие общие версии:

– преступление имело место при тех обстоятельствах, которые подтверждены материалами проверки;

– заявление о преступлении ложное (преступление было инсценировано).

Частные версии выдвигаются в отношении личности преступника, мотивов совершения преступления, способов несанкционированного доступа или создания и использования вредоносных программ, размера причиненного ущерба и т. д.

Далее необходимо разобраться со следственными ситуациями, возникающими на данном этапе расследования.

Следственная ситуация характеризуется прежде всего объемом и достоверностью исходной криминалистически значимой информации, имеющейся в распоряжении следователя и оперативного сотрудника.

На момент принятия решения о возбуждении уголовного дела о преступлении в сфере компьютерной информации чаще всего складываются следующие типичные следственные ситуации:

1. Отсутствуют сведения о совершенном преступлении (о причинах и способе) и личности правонарушителя.

2. Имеются сведения о преступлении, но нет сведений о личности преступника.

3. Известны все обстоятельства совершенного преступления, личность преступника установлена.

В условиях первой и второй следственных ситуаций целесообразно проводить следующие первоначальные следственные действия:

1. Допрос потерпевшего (заявителя).

2. Допрос свидетелей (лиц, на которых указано в исходной информации как на возможных очевидцев преступления).

3. Осмотр места происшествия с участием специалиста.

4. Проведение оперативно-разыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, обнаружения следов и других вещественных доказательств.

5. Выемка и последующий осмотр средств электронно-вычислительной техники, предметов, материалов и документов (в том числе, находящихся в электронной форме на машинных носителях) с участием специалиста.

6. Назначение судебной компьютерно-технической, бухгалтерской и иных видов экспертиз.

7. Производство поисковых действий, направленных на установление личности и местонахождения подозреваемого.

Планирование дальнейших следственных действий производится в зависимости информации, полученной от реализации вышеуказанных мероприятий.

В следующей (третей) ситуации в условиях очевидности, когда нам известны все обстоятельства преступления и личность преступника, целесообразно приведение таких следственных и процессуальных действий, как:

1. Возбуждение уголовного дела.

2. Вызов необходимых специалистов для участия в осмотре места происшествия (если он не был произведен ранее). Подготовка соответствующих научных и технико-криминалистических средств и материалов.

3. Осмотр места происшествия.

4. Задержание подозреваемого, личный обыск.

5. Допрос подозреваемого.

6. Выемка или обыск на рабочем месте и по месту проживания (в жилище) подозреваемого.

7. Осмотр обнаруженных и изъятых вещественных доказательств, документов, удостоверяющих личность задержанных, а также документов, характеризующих те производственные операции, в процессе которых допущены нарушения и обнаружены преступные действия (в том числе документов на электронных носителях информации).

8. Допрос свидетелей и лиц, названных в документах, переданных в органы предварительного расследования, как допустивших нарушения, ответственные за работу конкретных ЭВМ и других компьютерных устройств, по фактам установленных нарушений.

9. Проверка подозреваемых по различным видам учетов.

10. Истребование, а при необходимости производство выемки:

а) нормативных актов и документов, характеризующих порядок и организацию работы на предприятии – месте обнаружения следов преступления (в т. ч. с охраняемой законом информацией, бланками строгой отчетности, по использованию ЭВМ и т. п.);

б) документов, отражающих работу субъекта с конкретной компьютерной информацией – предметом преступления, ЭВМ или системой ЭВМ, например, журнала оператора ЭВМ, электронного журнала фиксации осуществленных операций, электронного реестра регистрации соединений абонентов в сети ЭВМ или электросвязи.

11. Назначение экспертиз, проведение ревизий, документальных проверок.

Далее должностному лицу, осуществляющему расследование, предстоит анализ полученной информации и решение вопроса о привлечении лица в качестве обвиняемого. Виды следственных, процессуальных действий и оперативных мероприятий, их последовательность и процедура производства должны определяться каждой конкретной следственной ситуацией, складывающейся по уголовному делу. Порядок производства отдельных следственных действий будут рассмотрен ниже.

Контрольные вопросы

1. Назовите поводы для возбуждения уголовных дел по преступлениям в сфере компьютерной информации.

2. Опишите признаки подготовки, совершения и сокрытия преступлений в сфере компьютерной информации.

3. Каков перечень проверочных материалов при возбуждении уголовного дела по преступлениям в сфере компьютерной информации?

4. Назовите ряд сведений и документов в материалах проверки, необходимых для принятия решения о возбуждении уголовного дела, с учетом специфики компьютерных преступлений.

5. Какие подразделения и службы оказывают содействие в раскрытии преступлений в сфере компьютерной информации?

6. Назовите обстоятельства, подлежащие доказыванию по компьютерным преступлениям.

7. Опишите типичные следственные ситуации, возникающие по преступлениям в сфере компьютерной информации.

8. Перечислите общие и частные версии, выдвигаемые по преступлениям в сфере компьютерной информации.

Тема 5. Особенности подготовки и проведения отдельных следственных действий по преступлениям в сфере компьютерной информации

§ 5.1. Особенности подготовки и производства осмотра места происшествия, предметов, документов

Осмотр как следственное действие имеет важнейшее значение для расследования преступлений в сфере компьютерной информации, поскольку, как правило, производится чаще всего на стадии возбуждения уголовного дела. Речь идет не только о таком виде осмотра, как осмотр места происшествия, но и осмотр предметов, документов, в частности осмотр машинного носителя и компьютерной информации. Рассмотрим два этих вида осмотра с точки зрения тактических особенностей.

Прежде всего, следует руководствоваться общими правилами обращения с компьютерной техникой и носителями компьютерной информации.

1. Все включения/выключения компьютерной техники и других технических средств, производятся только специалистом или под его руководством.

2. Использование криминалистической техники во избежание разрушения носителей компьютерной информации и микросхем памяти, должно быть согласовано со специалистом[1].

3. Диапазон допустимых температур при хранении и транспортировке компьютерной техники и машинных носителей информации должен варьироваться в температурных пределах от 0 до +50 градусов Цельсия.

4. Необходимо не допускать попадания на рабочие части компьютеров мелких посторонних элементов (частиц и порошков).

5. Не следует трогать без крайней необходимости рабочую поверхность съемных носителей компьютерной информации, осуществлять их хранение и транспортировку без специальных упаковочных средств.

6. Если же возникают вопросы, связанные с устройством и функционированием компьютерной техники, следует обращаться исключительно к специалисту.

Необходимо заметить, что осмотр как следственное действие в рамках производства по уголовным делам, связанным с компьютерной информацией, производится, как уже было отмечено, с участием специалиста в данной области. Законодатель в ст. 58 УПК РФ устанавливает, что специалистом является лицо, которое, во-первых, обладает соответствующими специальными знаниями, во-вторых, привлекается для содействия в обнаружении, закреплении и изъятии предметов и документов, для применения технических средств в исследовании материалов уголовного дела, для постановки

[1] См.: *Чистова Л. Е.* Расследование преступлений в сфере незаконного оборота сильнодействующих или ядовитых веществ: монография. М.: Юрлитинформ, 2014. С. 48.

вопросов эксперту или для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию. Специалист также содействует следователю в случаях, когда необходимо установить место электронного носителя, обнаруженного при осмотре места происшествия, в компьютерной технике, разъяснить следователю принципы работы компьютера и соответствующего оборудования.

Вместе с тем в каждом случае привлечения лица в качестве специалиста для оказания содействия в ходе следственного действия необходимо убедиться в том, что лицо обладает необходимыми специальными познаниями в интересующей должностное лицо области. Специальные познания могут относиться к отдельным аспектам работы в сфере компьютерной информации, и в каждом конкретном случае следователь должен определить, специалист какого рода необходим при производстве следственных действий.

Результативность такого взаимодействия напрямую зависит от эффективной работы следователя и специалиста. До декабря 2018 г. законодатель определял случаи, когда участие специалиста являлось обязательным. Однако в настоящее время ч. 3.1 ст. 183 УПК РФ утратила силу. Теперь копирование информации с электронных носителей возможно без обязательного участия специалиста.

Помимо участников следственного действия целесообразно привлечение сотрудников полиции к обеспечению деятельности следственно-оперативной группы для исключения противодействия в ее работе, охраны места происшествия в процессе производства осмотра и т. д.

Часть 1.1 ст. 170 УПК РФ устанавливает возможность привлечения понятых в ходе производства осмотра для удостоверения факта, хода, содержания и результатов. Понятые в этой ситуации в силу специфики следственного действия должны быть как минимум сведущи в компьютерной технике и порядке работы на ней на уровне пользователей (осведомленность понятых может быть установлена путем постановки соответствующих вопросов). При этом не рекомендуется приглашение понятых из числа работников организации, в которой проводится осмотр, что продиктовано их возможной причастностью к совершению компьютерного преступления.

В качестве участников могут быть приглашены представители администрации осматриваемой организации. Таковыми могут быть руководитель организации или его заместитель, а также представитель службы безопасности или вневедомственной охраны организации[1].

Как правило, возникает необходимость и в приглашении собственника электронного носителя, вызвавшего процессуальный интерес со стороны должностных лиц.

[1] См.: Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учеб.е пособие / под ред. Б. Я. Гаврилова. М.: Проспект, 2017. С. 74.

В первую очередь необходимо определиться с тем, что следует понимать по термином «место происшествия» в случае, когда речь идет о производстве по делам о преступлениях в сфере компьютерной информации. В указанном контексте термин подразумевает пространство, в пределах которого осуществлялись преступные действия, наступили вредные последствия, можно обнаружить следы преступления, предусмотренного гл. 28 УК РФ:

1) место, где осуществляется обработка компьютерной информации, фактически идет речь о предмете преступления;

2) сервер, сохранивший свидетельства о работе системы за определенный период или о предмете посягательства;

3) место, где осуществлялось использование технических средств для незаконного доступа к электронной информации, использования, создания, распространения вредоносного программного обеспечения, непосредственного нарушения правил эксплуатации компьютерной техники;

4) место наступления вредных последствий, место хранения машинных носителей и информации, полученной в результате неправомерного доступа;

5) применительно к преступлениям в сфере мобильных коммуникаций значение имеет территория, на которую распространяется «зона покрытия».

Выезжая на место происшествия, следователь должен быть обеспечен следующей аппаратурой:

– ноутбук с диском большой емкости, дисководом, приводом CD-ROM;

– соединительные кабели;

– загрузочные носители с «исследовательским» и сервисным программным обеспечением;

– принтер;

– внешний винчестер с программным обеспечением;

– видеокамера, фотоаппарат;

– программное обеспечение (текстовый и табличный редактор, диагностические программы, программы сбора информации о файловой системе, антивирусные программы, программы определения настроек аппаратуры и программ);

– материал для упаковки изъятого оборудования.

В первую очередь при осмотре места происшествия следователь обращает внимание на место расположения электронных носителей информации, в качестве которых выступают сервер (главный компьютер локальной сети, расположение персональных компьютеров, возможные периферийные устройства и т. д.).

По прибытии на место происшествия в первую очередь следователь выполняет следующие необходимые действия:

1) всем присутствующим лицам запрещается работа с компьютерными средствами и электронной информацией в пределах осуществления следственного действия. Указанный запрет необходим для того, чтобы избежать

изменения или повреждения информации, которая содержится на компьютерном объекте;

2) целесообразно удаление с места происшествия всех лиц, которые не вовлекаются в производство осмотра места происшествия. Оптимальным будет нахождение указанных лиц в помещении, где исключена возможность использования средств связи;

3) следует обеспечить охрану места происшествия, особое внимание уделив местам работы с компьютерной техникой, точкам доступа к электрическим щитам, пультам. В том случае если осматривается значительное по масштабу место происшествия, сотрудников, которые задействованы в осуществлении указанной задачи, следует расположить так, чтобы все необходимые места по возможности просматривались;

4) если на рабочем месте имеется локальная компьютерная сеть, необходимо извне заблокировать ее работу, например, отключить от телефонного кабеля шнур, модем и др.);

5) нередко возникает ситуация, когда в необходимый момент активируется программа уничтожения информации на компьютере. С этой целью с обязательным участием специалиста необходимо приостановить или отметить действие указанной программы, в том числе отключить компьютер от питания.

Осуществление такого следственного действия, как осмотр места происшествия, при всей его процессуальной значимости по возможности не должно создавать существенных затруднений для работы организации, в которой он проводится, за исключением случаев, когда вся работа с использованием компьютерной техники приостанавливается для получения сведений, имеющих значение для уголовного дела. Определиться с оптимальным механизмом производства осмотра поможет специалист. В частности, в организации может существовать резервная компьютерная система, на которую можно переключиться в необходимый момент. Ранее отмечалось, что в случае лояльного отношения участников к производимому следственному действия можно не блокировать работу организации в целом, а ограничиться определенными мерами, такими как удаление работников с рабочих мест в отдельное помещение, лишение их возможности использования технических средств связи и т. д.

После осуществления указанных мероприятий сотрудники полиции переходят к следующим действиям:

1) в случае осмотра места происшествия, в пределах которого функционирует локальная компьютерная сеть, привлекают системного администратора той организации, в помещении которой производится осмотр. Как правило, такое лицо не только знает все особенности работы локальной сети и компьютеров, но и отвечает за надлежащее функционирование локальной сети;

2) всех потенциальных свидетелей, то есть лиц, чья деятельность так или иначе касается работы объектов и предметов, исследование которых представляет процессуальный интерес, следует опросить раздельно, желательно с участием специалиста, который окажет необходимую помощь должностному лицу, как по содержанию задаваемых вопросов, так и по тактике осуществления этого действия;

3) после того как должностное лицо определит окончательно круг лиц, которые должны быть вовлечены в производство осмотра места происшествия, оно осуществляет обязательные требования закона по разъяснению прав и обязанностей участникам осмотра порядка процессуальных действий, которые будут осуществляться на месте происшествия, уведомлению участников о том, какие технические средства будут использоваться при производстве следственного действия и т. д.;

4) следует обратить внимание на правила участия понятых при производстве осмотра и в случае их привлечения проверить соответствие требованиям, установленных ст. 60 УПК РФ. Необходимо обратить внимание, что вся специальная техника и компьютерные программы, которые будут использованы должностными лицами при осмотре места происшествия, предварительно тестируются в присутствии понятых с целью удостоверения их надлежащего качества и пригодности к использованию. Понятые должны быть поставлены в известность о том, с какой целью указанные средства будут использоваться при осмотре. После выполнения указанных действий, следователь начинает непосредственный осмотр места происшествия, определяя его границы, количество и расположение рабочих мест, устанавливает факт подключения компьютеров к сети Интернет и к локальной компьютерной сети, если таковая имеется в осматриваемом помещении, то есть фактически определяет вид, количество и расположение объектов, которые будут подвергнуты осмотру, а также их электронное соединение.

Должностное лицо в ходе осмотра компьютера (вне зависимости от того, функционирует ли он в системе локальной компьютерной сети или нет) должно установить следующие моменты (особенности осмотра компьютера):

1) расположение компьютера, сопутствующих периферийных устройств (печатающего устройства, дисплея, клавиатуры, дисководов и пр.), их качественные характеристики;

2) изучить качество соединения между собой компьютера и периферийных устройств;

3) установить факт наличия подключения компьютера к сети Интернет или работы указанного компьютера в составе локальной компьютерной сети;

4) исследовать качественные характеристики переключателей на осматриваемых объектах, а также наличие и состояние индикаторных ламп;

5) отразить факт и содержание информации, имеющейся на экране компьютера, а также световые сигналы, которые располагаются на соответствующих индикаторах объекта;

6) изучить качественные характеристики соединительного кабеля, отсутствие внешних повреждений, следов подключения иных устройств;

7) обратить внимание на наклейки, записи, обозначения, имеющие отношение к работе компьютера, их содержание;

9) установить факт подключения к компьютеру технических устройств и аппаратуры, не предназначенной для работы на данном рабочем месте;

10) обратить внимание на программы, которые в момент осмотра выполняются на компьютере, отразить в протоколе характеристики этих программ;

11) изучить вопрос наличия и состояния защиты компьютерной информации на рабочем места, имелись ли факты нарушения указанной защиты, иное воздействие на объект;

12) установить наличие электронных носителей информации, как подключенных в настоящий момент к объекту осмотра, так и находящихся на рабочем месте, изучить их содержание и качество имеющейся информации.

В соответствии с УПК РФ осмотр предметов можно осуществлять как в рамках осмотра места происшествия, так и как самостоятельное следственное действие. В нашем случае, речь идет о машинном носителе компьютерной информации.

При осмотре применяются традиционные правила для его производства. Так, начинается осмотр с описания внешних и общих признаков осматриваемого предмета. Обязательно указываются его технические характеристики, основные реквизиты используемого программного устройства (тип, название, модель, марка, номера и др.).

После указанных действий следователь переходит к осмотру «внутренней» информации, то есть информации, которая содержится на осматриваемом объекте, с детальным указанием ее индивидуальных признаков.

Когда следователь осматривает отдельный предмет, который может представлять процессуальный интерес, обязательно обращает внимание на следующие аспекты:

1) где находится осматриваемый предмет, в том числе на рабочем месте;

2) характеристики окружающей среды, в условиях которой хранится осматриваемый предмет (температура, влажность и др.);

3) в случае если предмет находится в упаковке, коробке или иной емкости – ее внешние признаки, характер и цвет материала;

4) на упаковке или на самом предмете могут иметь место надписи, наклейки, внешние обозначения, которые следует описать;

5) внешние характеристики описываемого предмета, в том числе размер, цвет, вид;

6) место изготовления предмета, имеется ли на нем защита от записи;

7) существование особых признаков предмета, в том числе повреждений, сколов, гравировки и др.;

8) предназначение предмета, а именно для работы с каким типом компьютерной техники он может работать;

9) объем информации, который может вмещать осматриваемый предмет (гигабайты, мегабайты).

Любое следственное действие, за исключением производства судебной экспертизы, оформляется соответствующим протоколом. В нашем случае это протокол осмотра места происшествия или протокол осмотра предметов, документов, в которых фиксируется как общее состояние объекта либо обстановка места происшествия, так и отдельные признаки, свойства и состояния объектов.

Необходимо отметить, что все действия, которые осуществлялись должностными лицами в ходе производства осмотра, должны обязательно указываться в протоколе осмотра. Кроме того, фиксируется и результат произведенных действий (например, осуществлялось копирование информации на иной носитель, к компьютеру подключались/отключались периферийные устройства, иные материальные объекты и др.).

При оценке таких доказательств необходимо установить, каким образом был создан файл, в результате человеческой манипуляции (так как в промежутке между созданием и копированием может быть произведена коррекция либо проявлен субъективный фактор) или в результате работы программ и техники (например, видеозапись камер наружного наблюдения, которая была скопирована с жесткого диска). В первом случае подлинность электронного файла может оказаться под сомнением и потребует проведения дополнительной экспертизы для проверки достоверности. Во втором видеозапись осуществлялась без человеческого вмешательства, а следовательно, если при выемке не было допущено процессуальных нарушений, сомнения в ее достоверности не должны иметь место[1].

В протоколе осмотра места происшествия указываются следующие характеристики:

– внешние признаки осматриваемого объекта (технические), характеристика его установки, эксплуатации;

– взаимодействие, расположение компьютерных средств, характер соединений между ними (в том числе, беспроводные), наличие и взаимодействие с периферийными устройствами;

– конструктивные особенности помещения (окна, дверные проемы, вентиляция, электрические розетки и щиты и др.);

– схема расположения рабочих мест в целом в пределах осматриваемого места;

– средства защиты компьютерной информации от незаконного доступа извне, технические характеристики указанных средств, их количество и внешнее описание;

[1] См.: *Федосеева Е. Л., Литвин И. И.* Особенности использования технических средств при расследовании уголовных дел // Обеспечение прав и законных интересов граждан в деятельности органов предварительного расследования: сб. статей. Орел: ОрЮИ МВД России им. В. В. Лукьянова, 2017. С. 236.

– следы внешнего воздействия, в том числе следы повреждения, негативного воздействия, а также изменения и модификации осматриваемого предмета;

– следы преступления, которые не связаны непосредственно с воздействием на компьютерные объекты (взлом двери, отпечатки следов обуви и др.);

– технические средства, примененные при копировании информации;

– порядок применения технических средств;

– электронные носители информации, к которым эти средства были применены, и полученные результаты (ч. 3 ст. 164.1 УПК РФ).

В протоколе следственного действия отражаются следующие сведения об осматриваемой компьютерной информации:

– объем носителя, который занят информацией, и объем носителя, который свободен; операционная система, ее тип;

– какие файлы содержит информация, название, количество, вид документов;

– информация о виде файла (только для чтения, скрытый и др.);

– наличие и характеристика программ, которые содержатся на осматриваемом предмете, в том числе тех, которые были удалены с носителя.

– если с носителя была удалена информация, повреждена или скрыта, следует отразить тип сокрытия; в случае ее последующего восстановления – отразить объем восстановленной информации, какими программными средствами было это сделано и др.;

– характеристика текстовых файлов (шрифт, размер, объем, выделения текста и др.);

– факт наличия установленной антивирусной программы, название, тип, год, является ли она лицензионной или нет;

– наличие или отсутствие вирусов, вредоносных программ (название, тип, и др.);

– факт копирования информации, имеющейся на электронном носителе, дата, объем и др.).

Следует остановиться на правилах обращения с изъятой компьютерной техникой, в том числе, ее перемещения и хранения (ч. 2.1 ст. 82, 164.1 УПК РФ): 1) перемещение и хранение компьютерной техники осуществляется в выключенном состоянии;

2) упаковка изъятых предметов должна исключать возможность деформации, воздействия на все изъятые компьютерные устройства;

3) машинные носители информации должны упаковываться отдельно друг от друга;

4) по возможности упаковку средства вычислительной техники и машинные носители информации нужно производить в ту тару, в которой данная техника поставляется предприятием-изготовителем. В противном случае системный блок помещается в полиэтиленовый (либо холщовый) пакет, горловина завязывается и прошивается бечевкой, затем опечатывается;

5) информацию из оперативной памяти компьютера необходимо изымать путем ее переноса на физический носитель с использованием стандартных паспортизированных программных средств;

6) процедура изъятия электронных носителей информации и содержащейся на этих носителях информации регламентируется нормой об особенностях изъятия электронных носителей информации и копирования с них информации при производстве следственных действий (ст. 164.1 УПК РФ).

К протоколу прилагаются электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия (ч. 3 ст. 164.1 УПК РФ).

§ 5.2. Особенности подготовки и проведения допроса

Допрос является также следственным действием, которое, как правило, осуществляется на первоначальном этапе расследования. Особенность данного действия состоит в том, что следователь сталкивается не только с необходимостью обладания знаниями о работе компьютера, его периферийных устройств, электронного носителя информации, но и с использованием специальной терминологии, которая может быть использована в разных значениях, в том числе отличных от общеупотребительных. В данном случае опять возникает необходимость консультации со специалистов в данной области при подготовке к допросу.

При подготовке к допросу необходимо:

1. Изучить материалы дела, определить очередность проведения допросов.

2. Предварительно изучить личность допрашиваемого.

Для выбора тактики допроса и определения круга вопросов, следует получить сведения о лице по месту жительства, учебы, работы, досуга.

3. Получить консультацию специалиста и составить план допроса. Расследование преступлений в сфере компьютерной информации и высоких технологий сопряжено с необходимостью использования специальной терминологии, зачастую не вполне понятной следователю, но абсолютно ясной допрашиваемому. В связи с этим следователю целесообразно проконсультироваться со специалистом, предварительно согласовав с ним формулировки вопросов, подлежащих выяснению.

Проконсультироваться следует до начала допроса, выяснив следующие основные вопросы:

1. Что явилось предметом преступного посягательства, какую ценность и для кого могла представлять компьютерная информация?

2. Каков принцип осуществления неправомерного доступа к компьютерной информации?

3. Какое воздействие было оказано на компьютерную информацию – уничтожение, блокирование, модификация, копирование?

4. Какие последствия повлекли указанные действия?

5. Какой минимальной квалификацией должно обладать лицо для совершения преступления? Насколько использование служебного положения облегчило (могло облегчить) совершение преступления? Могло ли преступление быть совершено в одиночку или это возможно только в группе?

Специалист, ознакомившись с имеющейся у следователя информацией, может дать собственный ответ, конечно же, с определенной долей вероятности. С другой стороны, следователю может потребоваться помощь специалистов других отраслей знаний – экономики, политики, искусства и др., чтобы понять цель преступного воздействия на компьютерную информацию, оценить ее значимость и др. Еще на стадии подготовки допроса следователь должен определить уровень компетентности подозреваемого в области информационных технологий. Эта характеристика будет основополагающей в выборе тактики допроса, в частности при определении необходимости приглашать к участию в допросе специалиста.

Допрос подозреваемого, обвиняемого

В ходе проведения допросов подозреваемых, обвиняемых по уголовным делам о преступлениях в сфере компьютерной информации и высоких технологий следует выяснить:

А. Обстоятельства общего характера:

1) где и кем (в какой должности) работал подозреваемый;

2) состоит ли на учете у нарколога, психиатра, имеет ли травмы головы;

3) какое имеет образование, специальности, дипломы;

4) наличие профессиональных навыков и опыта работы с компьютерной техникой и программным обеспечением, уровень владения компьютерной техникой (попросить высказать собственную оценку); каков уровень его квалификации;

5) наличие (отсутствие) на работе правомерного доступа к компьютерной технике и конкретным видам программного обеспечения;

6) перечень конкретных операций с компьютерной информацией, которые подозреваемый (обвиняемый) выполняет на своем рабочем месте; к какой компьютерной информации имеет доступ; какие операции с информацией он имеет право проводить;

7) кто научил его работать с конкретным программным обеспечением;

8) закреплены ли за ним по месту работы идентификационные коды и пароли для пользования компьютерной сетью, ЭЦП; какова его категория доступа к информации;

9) какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети);

10) к каким видам программного обеспечения имеет доступ подозреваемый;

11) каков источник его происхождения;

12) наличие компьютера по месту жительства, круг лиц, им пользующихся;

13) какова конфигурация компьютера, имеющегося по месту жительства (по месту работы, изъятого при обыске);

14) какое программное обеспечение установлено на компьютере; переустанавливал ли операционную систему и если да, то когда;

15) обнаруживались ли программы, источник происхождения которых неизвестен;

16) установлены ли на компьютере антивирусные или защитные программы;

17) наличие правомерного доступа к сети Интернет и работе в Интернете;

18) какие ники, электронные почтовые ящики, сайты, домашние страницы принадлежат подозреваемому (обвиняемому) в сети Интернет;

19) кто настраивал удаленный доступ к сети, для выхода в Интернет;

20) услугами каких провайдеров пользовался для выхода в Интернет.

21) наблюдались ли сбои в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время;

22) обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения;

23) обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети;

24) имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника, и какие именно;

25) не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации;

26) не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения;

27) неизвестны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей;

28) ознакомлен ли он с порядком работы с информацией, инструкциями о порядке проведения работ.

Б. Обстоятельства, предшествовавшие совершению преступления:

1) когда возникло намерение совершить преступление, кто или что повлияло на это решение;

2) почему выбрал именно данный объект для преступного посягательства;

3) каковы мотивы и цель совершения преступления;

4) откуда подозреваемый мог узнать пароль (код) доступа к информации;

5) из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ.

В. Обстоятельства совершения преступления:

1) место и время совершения преступления;

2) способ проникновения в помещение, где установлена компьютерная техника или способ осуществления неправомерного доступа и компьютерную систему, сеть;

3) приемы преодоления информационной защиты: подбор или хищение ключей и паролей; отключение средств защиты; разрушение средств защиты; использование несовершенства защиты;

4) от кого получил данные об используемых в потерпевшей организации мерах защиты информации и способах ее преодоления;

5) какие средства использованы при совершении преступления: технические, программные, носители информации, комбинированные;

6) способ сокрытия неправомерного доступа;

7) количество фактов незаконного вторжения в информационные базы данных; создания, использования и распространения вредоносного ПО; нарушения правил работы ЭВМ, их системы или сети;

8) использовалось ли для совершения преступления служебное положение, и в чем это конкретно выразилось;

9) наличие сговора с другими лицами и данные о них, кто инициатор;

10) детали состоявшейся преступной договоренности;

11) каково распределение ролей между участниками преступления;

12) каковы конкретные действия по подготовке преступления;

13) раскаивается ли в содеянном.

Основными тактическими задачами допроса потерпевших и свидетелей при расследовании дел рассматриваемой категории являются: выявление элементов состава преступления в наблюдавшихся ими действиях, установление обстоятельств, места и времени совершения значимых для расследования действий, способа и мотивов его совершения и сопутствующих обстоятельств, признаков внешности лиц, участвовавших в нем, определение предмета преступного посягательства, размера причиненного ущерба, детальные признаки похищенного, установление иных свидетелей и лиц, причастных к совершению преступления.

Допрос потерпевшего

В ходе допроса потерпевших можно выяснить обстоятельства выявления преступления и его последствия, предварительно оценить причиненный ущерб, узнать способы защиты информации, порядок организации охраны объекта, точные данные о предмете преступного посягательства, предварительные данные о личности виновного и ряд других обстоятельств.

Допрос свидетелей

При расследовании преступлений, предусмотренных гл. 28 УК РФ, в качестве свидетелей могут выступать: программисты; сотрудник, отвечающий за информационную безопасность или администратор; сотрудник, занимающийся техническим обслуживанием; операторы ЭВМ; начальник вычислительного центра или руководитель предприятия (организации); администраторы сети; сотрудники компании мобильной связи; работники бухгалтерии и другие лица.

Формулировка вопросов для выяснения интересующей следствие информации может быть следующей:

1) не проявлял ли кто-либо интереса к компьютерной информации, программному обеспечению, компьютерной технике данного предприятия, организации, учреждения, фирмы или компании;

2) не появлялись ли в помещении, где расположена компьютерная техника, посторонние лица, не зафиксированы ли случаи работы сотрудников с информацией, не относящейся к их компетенции;

3) не было ли сбоев в работе программ, хищений носителей информации и отдельных компьютерных устройств;

4) зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств защиты компьютерной информации;

5) как часто проверяются программы на наличие вирусов, каковы результаты последних проверок;

6) как часто обновляется программное обеспечение, каким путем, где и кем оно приобретается;

7) каким путем, где и кем приобретается компьютерная техника, как осуществляется ее ремонт и модернизация;

8) каков на данном объекте порядок работы с информацией, как она поступает, обрабатывается и передается по каналам связи;

9) кто еще является абонентом компьютерной сети, к которой подключены компьютеры данного предприятия, организации, учреждения или фирмы, каким образом осуществляется доступ в сеть, кто из пользователей имеет право на работу в сети, каковы их полномочия;

10) как осуществляется защита компьютерной информации, применяемые средства и методы защиты и др.;

11) имели ли место случаи неправомерного доступа к компьютерной информации ранее, если да, то как часто;

12) могли ли возникшие последствия стать результатом неосторожного действия лица или неисправности работы ЭВМ, системы ЭВМ, сбоев программного обеспечения и т. п.;

13) каков характер изменений информации;

14) кто является собственником (владельцем или законным пользователем) скопированной (уничтоженной, модифицированной, блокированной) информации и др.

При допросе свидетелей на последующем этапе расследования неправомерного доступа к компьютерной информации, возникает необходимость детализировать ранее установленные обстоятельства либо выяснить факты, которые стали известны при проведении других следственных действий. В этот период выясняется:

1) при каких обстоятельствах свидетель наблюдал преступников (процесс совершения преступления);

2) в чем состоял способ совершения преступления;

3) какую роль выполнял каждый из соучастников неправомерного доступа к компьютерной информации;

4) знает ли свидетель, какую цель преследовал обвиняемый, совершая неправомерный доступ к компьютерной информации;

5) кто из работников предприятия, организации, учреждения, фирмы, компании мог способствовать совершению преступления;

6) имели ли место подобные проявления ранее, если да, то как на них реагировали руководители предприятия, организации, учреждения, фирмы, компании;

7) как свидетель характеризует обвиняемого и его окружение;

8) что способствовало совершению преступления.

Контрольные вопросы

1. Опишите общие правила обращения с компьютерной техникой и носителями компьютерной информации.

2. Каковы необходимые действия следователя по прибытии на место происшествия?

3. Укажите особенности осмотра компьютера.

4. Каковы правила обращения с изъятой компьютерной техникой, в том числе ее перемещения и хранения?

5. Перечислите вопросы, выясняемые при проведении допросов у потерпевших по уголовным делам о преступлениях в сфере компьютерной информации.

6. Каковы вопросы, выясняемые при проведении допросов подозреваемых, обвиняемых по уголовным делам о преступлениях в сфере компьютерной информации?

7. Какие вопросы следует выяснить при проведении допроса свидетелей по уголовным делам о преступлениях в сфере компьютерной информации?

Тема 6. Особенности подготовки, назначения и проведения экспертиз по преступлениям в сфере компьютерной информации

Судебная экспертиза – это действие, которое также является типичным для первоначального этапа расследования преступлений, связанных использованием информационных технологий. Судебную экспертизу можно определить как регламентированное Уголовно-процессуальным кодексом исследование компьютерной информации, технических средств, программного обеспечения компьютерной системы, проводимое с целью получения информации, имеющей значение для уголовного дела.

Объекты такой экспертизы могут быть сгруппированы по следующим классам:

1 класс «Материальные объекты»:

а) компьютеры, в том числе когда возникает необходимость выяснить возможность использования их для получения неправомерного доступа к электронной информации);

б) аппаратура, которая позволяет вводить информацию в компьютер или выводить ее из него, т. е. периферийные устройства (принтеры, плоттеры, сканеры и т. д.);

в) активное и пассивное сетевое оборудование, сетевые аппаратные средства (сетевые платы, каналы связи, специальные устройства, поддерживающие функционирование сети (маршрутизаторы, концентраторы, коммутаторы);

г) интегрированные системы (например, ЭВМ-органайзеры, которые могли применяться для хранения информации о времени незаконного распространения порнографических материалов);

д) пейджеры (например, когда они могли использоваться для хранения информации о местах сбыта поддельных денег);

е) мобильные телефоны (например, когда они могли использоваться для неправомерного доступа к охраняемой законом компьютерной информации);

ж) встроенные системы на основе микропроцессорных контроллеров (иммобилайзеры, транспондеры, круиз-контроллеры и т. п.);

з) любые комплектующие всех указанных компонентов (аппаратные блоки, платы расширения, микросхемы и т. п.).

2 класс «Программные объекты»:

а) системное программное обеспечение:

– операционная система (например, когда она является предметом неправомерного доступа);

– вспомогательные программы (утилиты; например, когда они являются предметом неправомерного доступа);

б) прикладное программное обеспечение (общего назначения: текстовые редакторы и т. д.; специального назначения: для решения задач в определенной области науки).

3 класс «Информационные объекты»:

а) текстовые и графические документы, изготовленные с использованием компьютерных средств (например, когда документы составлялись в процессе изготовления поддельных денег);

б) данные в формате мультимедиа (например, когда они являются предметом незаконного использования объектов авторского права);

в) информация в форматах баз данных и других приложений, имеющая прикладной характер (например, когда она являются предметом создания вредоносных программ для ЭВМ).

Согласно ч. 2 ст. 195 УПК РФ судебная экспертиза производится государственными судебными экспертами и иными экспертами из числа лиц, обладающих специальными знаниями, то есть в экспертном учреждении и вне экспертного учреждения. Какая форма будет избрана в каждом конкретном случае, зависит от выбора следователя или ходатайства обвиняемого. Если вопрос о назначении экспертизы решается в суде, форма будет избрана судом по согласованию со сторонами, участвующими в процессе. Выбор экспертного учреждения осуществляется с учетом вида экспертизы, объектов исследования и характера вопросов, которые подлежат разрешению.

Следует иметь в виду, что по делам данной категории могут назначаться экспертизы других классов и родов: трасологические – для анализа следов взлома, дактилоскопические – следов рук, как на внешних, так и на внутренних поверхностях компьютеров и их комплектующих. Судебно-экономические экспертизы, в частности финансово-экономические и бухгалтерские, назначаются, когда, например, преступления в сфере движения компьютерной информации связаны с преступлениями в кредитно-финансовой сфере. Весьма распространены технико-криминалистические экспертизы документов, когда компьютер используется как средство для изготовления поддельных документов, фальшивых денежных билетов и пр. При использовании средств прослушивания переговоров назначаются фоноскопические экспертизы.

На этапе подготовки материалов, предоставляемых в распоряжение экспертов при назначении соответствующей судебной экспертизы следователь выносит постановление, в котором должны быть отражены элементы, указанные в ст. 195 УПК РФ, определяет объект, подлежащий передаче на экспертизу, прилагает его к постановлению о ее назначении, передает вместе с постановлением эксперту. Следователь представляет на экспертизу, как правило, не образцы для сравнительного исследования, так как основная масса исследований реализует диагностическую задачу: установить наличие чего-либо, свойства чего-либо, причинную связь между произошедшим событием и свойствами чего-либо.

Примерный перечень вопросов, решаемых в рамках КТЭ[1]:

[1] См.: *Россинская Е. Р., Усов А. И.* Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. С. 46.

1. Вопросы по исследованию аппаратных средств:

– Относится ли представленное устройство к аппаратным компьютерным средствам?

– К какому типу (марке, модели) относится аппаратное средство? Каковы его технические характеристики и параметры?

– Каково функциональное предназначение представленного аппаратного средства?

– Какое первоначальное состояние (конфигурацию, характеристики) имело аппаратное средство?

– Каково фактическое состояние (исправен, неисправен) представленного аппаратного средства? Имеются ли в нем отклонения от типовых (нормальных) параметров, в т. ч. физические дефекты?

– Является ли неисправность данного средства следствием нарушения определенных правил эксплуатации?

– Каковы причины изменения функциональных (потребительских) свойств в начальной конфигурации представленного аппаратного средства?

– Является ли представленное аппаратное средство носителем информации?

– Какой вид (тип, модель, марку) имеет представленный носитель информации?

– Доступен ли для чтения представленный носитель информации?

2. Вопросы по исследованию программных средств:

– Какова общая характеристика представленного программного обеспечения, из каких компонент (программных средств) оно состоит?

– Обладают ли программные средства признаками контрафактности?

– Каков состав соответствующих файлов программного обеспечения, каковы их параметры (объемы, даты создания, атрибуты)?

– Какое общее функциональное предназначение имеет программное средство и является ли оно вредоносным?

– Какова совместимость конкретного программного средства с программным и аппаратным обеспечением компьютерной системы?

– Имеются ли в программном средстве отклонения от нормальных параметров (например, свойства инфицирования, недокументированных функций)?

– Имеет ли программное средство защитные возможности (программные, аппаратно-программные) от несанкционированного доступа и копирования?

– Имеются ли на носителях информации тексты (коды) с первоначальным состоянием программы?

– Подвергался ли алгоритм программного средства модификации по сравнению с исходным состоянием?

– Какой вид имело программное средство до его последней модификации?

– С какой целью было произведено изменение каких-либо функций в программном средстве?

– Направлены ли внесенные изменения в программное средство на преодоление его защиты?

– Каким способом были произведены изменения в программе (преднамеренно, воздействием вредоносной программы, ошибками программной среды, аппаратным сбоем и др.)?

– Имеются ли в программном средстве враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютерной системы?

– Правильна ли начальная настройка программы бухгалтерского учета и корректны ли действия пользователя?

3. Вопросы по исследованию информации (данных):

– Как отформатирован носитель информации, и в каком виде на него записаны данные?

– Каковы характеристики физического и логического размещения данных на носителе информации?

– Какие свойства, характеристики и параметры (объемы, даты создания-изменения, атрибуты и др.) имеют данные на носителе информации?

– Какого вида (явный, скрытый, удаленный, архив) имеется информация на носителе?

– К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа, запись пластиковой карты и др.) и какими программными средствами они обеспечиваются?

– Каким образом организован доступ (свободный, ограниченный и пр.) к данным на носителе информации и каковы его характеристики?

– Какие свойства, характеристики имеют выявленные средства защиты данных и какие возможны пути ее преодоления?

– Какие признаки преодоления защиты (либо попыток несанкционированного доступа) имеются на носителе информации?

– Каково содержание защищенных данных?

– Какие несоответствия типовому представлению имеются в выявленных данных (нарушение целостности, несоответствие формата, вредоносные включения и пр.) имеются в данных?

– Каковы пользовательские (потребительские) свойства и предназначение данных на носителе информации?

– Какие данные о собственнике (пользователе) компьютерной системы (в т. ч. имена, пароли, права доступа и пр.) имеются на носителях информации?

– Какие данные с представленных на экспертизу документов (образцов) и в каком виде (целостном, фрагментарном) находятся на носителе информации?

– Каково первоначальное состояние данных на носителе (в каком виде, какого содержания и с какими характеристиками, атрибутами находились определенные данные до их удаления или модификации)?

– Каким способом и при каких обстоятельствах произведены действия (операции) (блокирование, модификация, копирование, удаление) определенных данных на носителе информации?

– Какая имеется причинная связь между действиями (вводом, модификацией, удалением и пр.) с данными и имевшим место событием (например, нарушением в работе компьютерной системы, в т. ч. сбои в программном и аппаратном обеспечении)?

– Какова степень соответствия (или несоответствия) действий с конкретной информацией специальному регламенту или правилам эксплуатации определенной компьютерной системы?

4. Вопросы, комплексного исследования компьютерной системы (при экспертизе целостной компьютерной системы):

– Является ли представленное оборудование компьютерной системой?

– Является ли представленное оборудование целостной компьютерной системой или же ее частью?

– К какому типу (марке, модели) относится компьютерная система?

– Какой состав (конфигурацию) и технические характеристики имеет компьютерная система?

– Какое функциональное предназначение имеет компьютерная система?

– Имеет ли компьютерная система какие-либо отклонения от типовых (нормальных) параметров, в т. ч. физические (механические) дефекты?

– Какие эксплуатационные режимы задействованы (установлены) в компьютерной системе?

– Существуют ли в компьютерной системе недокументированные (сервисные) возможности? Какие это возможности?

– Какие носители информации имеются в представленной компьютерной системе?

– Реализована ли в компьютерной системе какая-либо система защиты информации?

– Какая система защиты информации имеется в представленной компьютерной системе? Каков тип, вид и характеристики этой системы защиты? Каковы возможности по ее преодолению?

– Какова стоимость производственных и эксплуатационных дефектов компьютерных средств?

Контрольные вопросы

1. Дайте понятие судебной экспертизы.
2. Каковы объекты судебной компьютерно-технической экспертизы?
3. Дайте перечень вопросов, решаемых в рамках судебной компьютерно-технической экспертизы.
4. Назовите вопросы по исследованию программных средств компьютерной техники.
5. Перечислите вопросы комплексного исследования компьютерной системы, решаемые в рамках судебной компьютерно-технической экспертизы.

Тема 7. Предупреждение компьютерных преступлений, меры обеспечения предупреждения компьютерных преступлений

Сотрудниками правоохранительных органов выработана система способов для предотвращения совершения любого компьютерного преступления. Это подтверждается анализом международного опыта борьбы с преступностью. В качестве профилактики используются различные меры, которые направлены на выявление и устранение причин, способствующих совершению противоправных деяний. Правильно организованная профилактическая работа оказывает позитивное воздействие на уровень, структуру и динамику преступности, поскольку данные мероприятия сконцентрированы против истоков преступности.

Известно, что преступления в сфере компьютерной безопасности имеют очень высокую степень латентности, что способствует постоянному росту количества совершенных преступлений данной категории.

Между тем многие работники органов внутренних дел, в том числе и сотрудники следственных подразделений, на недостаточном профессиональном уровне подготовлены к осуществлению профилактических мероприятий. Для выработки правильного алгоритма действий, направленных на профилактику совершения преступлений данной категории, правоохранительным органам следует знать причины, которые способствуют совершению преступлений в сфере компьютерных преступлений.

В последнее десятилетие отмечается увеличение количества компьютерной техники, как в различных организациях, так и у граждан, в связи с чем возрос объем обрабатываемой и хранящейся информации. Указанные обстоятельства влекут рост обмена информационных данных через телекоммуникационные сети.

Анализ современного состояния свидетельствует о несовершенстве профилактических мер, направленных на защиту компьютерных систем и их сетей, а также программного обеспечения. Отсутствует государственная политика в сфере обеспечения информационной безопасности. Кроме того, не

выработан необходимый алгоритм использования в работе на компьютере программного обеспечения, базы данных и аппаратных средств поддержания сетевых технологий. При этом при осуществлении работы с компьютерными сведениями, которые охраняются законом, пользователи нарушают установленные правила.

Наряду с вышеперечисленными, специалистами выделяются и другие причины, послужившие совершению противоправных действий данного вида:

- электронная почта недостаточно защищена;
- в своей работе на компьютере пользователи допускают небрежность;
- кадровая политика при приеме людей на работу характеризуется некачественной работой по изучению личности кандидатов;
- обязанности по разработке программного обеспечения и эксплуатация техники зачастую возлагается на одного сотрудника;
- пользователи редко меняют пароли или они не достаточно надежные;
- не делают копии программ либо нарушают сроки их хранения;
- ЭВМ необоснованно используется в конкретных технологических процессах и операциях;
- администрации не осуществляет надлежащего контроля за деятельностью своих подчиненных сотрудников, которые задействованы на различных стадиях обработки компьютерной информации;
- руководство неправильно организует межличностные взаимоотношения с подчиненными[1].

Меры предупреждения компьютерных преступлений в научной литературе подразделяются на три основных группы: правовые; организационно-технические и криминалистические[2].

К первой группе профилактики преступлений этой категории относятся законодательные положения, предусматривающие уголовную ответственность за указанные выше противоправные деяния[3].

Данные мероприятия включают выработку норм, которые предусматривают ответственность в соответствии с УК РФ за совершение преступлений в сфере компьютерной информации, способствуют совершенствованию гражданского и уголовного законодательства. К правовым мерам относятся также предмет общественного контроля за создателями компьютерных систем и заключение международных договоров об их ограничениях, если они смогут

---

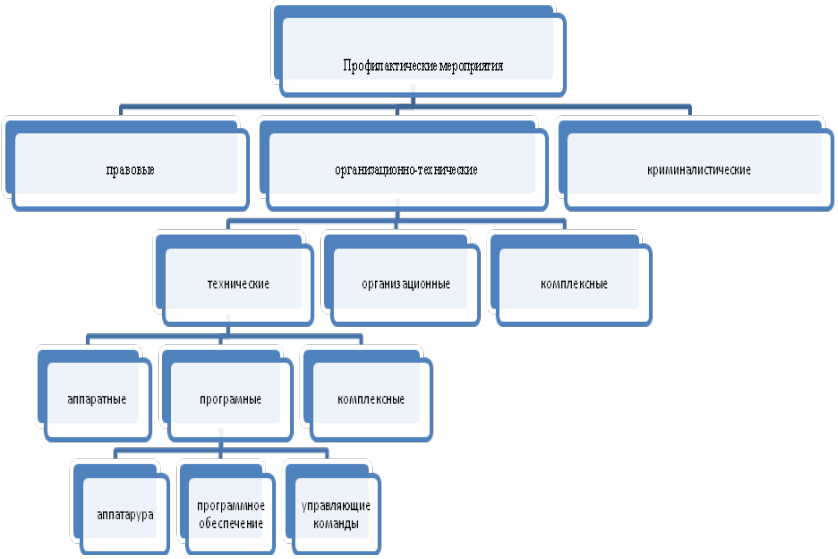
[1] См.: *Егорышев А. С.* Обзор обстоятельств, способствующих неправомерному доступу к компьютерной информации // Вестник Калининградского института МВД России. 2002. № 2. С. 185–187.

[2] См.: *Керимов В. Э., Керимов В. В.* Профилактика и предупреждение преступлений в сфере компьютерной информации // Черные дыры в российском законодательстве. 2000. № 1. С. 34.

[3] См.: *Бражник С. Д.* Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. … канд. юрид. наук. Ижевск, 2002.

оказать влияние на военные, экономические и социальные стороны жизни стран, подписавших соглашение.

Систему данных мер можно рассмотреть на предлагаемой схеме.



Мировая история законодательства свидетельствует о том, что первый шаг, сделанный в строну профилактики компьютерных преступлений был сделан в США – это нормативно-правовой акт «Computer crime act of 1978», который принят в 1978 г. в американских штатах Флорида и Аризона. После чего в других штатах страны появились схожие акты, которые явились вехой в дальнейшем совершенствовании законодательства для реализации мер предупреждения данных преступлений[1].

В России аналогичные нормативно-правовые документы появились только в 90-х гг. XX столетия и послужили фундаментом для развития в этом направлении. Это Закон РФ от 23.09.1992 № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»[2], а также Федеральный закон «Об информации, информатизации и защите информации» от 20.02.1995 № 24-ФЗ[3]. В настоящее время данные законы утратили законную силу, но в первом десятилетии приняты другие

[1] См.: *Вехов В. Б.* Компьютерные преступления: способы совершения и раскрытия. М.: Право и Закон, 1996.

[2] О правовой охране программ для электронных вычислительных машин и баз данных: закон РФ от 23.09.1992 № 3523-1. URL:http://www.consultant.ru.

[3] Об информации, информатизации и защите информации: Федеральный закон от 20.02.1995 № 24-ФЗ. URL: http://www.consultant.ru.

федеральные законы «О связи» от 07.07.2003 № 126-ФЗ[1] и «Об информации, информационных технологиях и о защите информации» от 27.06.2006 № 149-ФЗ[2]. В указанных актах содержатся определения основных компонентов информационной технологии; закреплены категории доступа определенных субъектов к конкретным видам сведений и установлены уровни секретности информации.

Основополагающим этапом предупреждения преступлений данной категории считают Уголовный кодекс РФ, вступивший в силу в 1996 г. В указанном законе компьютерная информация закреплена как объект уголовно-правовой охраны.

Принятие данного документа привело наше законодательство в соответствие с общепринятыми международными правовыми нормами развитых зарубежных стран. При этом Уголовный кодекс РФ имеет ряд несовершенств, в связи с этим возникают проблемы, которые затрудняют предупреждение и расследование компьютерных преступлений.

Кроме того, в системе МВД России недостаточно специалистов в области компьютерной безопасности; не выработаны соответствующие методические рекомендации по проведению следственных действий, направленных на изъятие и оценку доказательств, и др.

Второй группой мероприятий по защите средств компьютерной информации от противоправных посягательств считают меры организационно-технического характера, которые подразделяются на организационные, технические и комплексные методы профилактики.

Организационные меры служат самым эффективным средством сохранения информации. Как ранее указывалось, важнейшей причиной, способствующей совершению компьютерных преступлений, в большинстве случаев является недостаточная организация контроля за работой подчиненных сотрудников.

При этом для результативности профилактических мероприятий бывает достаточно выполнить ряд действий:

1) изучить документацию в учреждении, организации;

2) ознакомиться с полномочиями каждого сотрудника;

3) определить возможные способы утечки информации;

4) устранить выявленные слабые места в защите.

Зарубежный опыт показывает, что самой действенной мерой в этом направлении служит введение в штатное расписание организации должности специалиста по компьютерной безопасности или специальной службы, в зависимости от конкретной ситуации.

---

[1] О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (действ. ред.). URL: http://www.consultant.ru.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.06.2006 № 149-ФЗ.

В обязательном порядке необходимо для всех лиц, имеющих право доступа к компьютерной информации установить категории допуска. Следует определить область служебных интересов каждого лица, виды информации, к которым он имеет право доступа, а также вид разрешения этого доступа, определяемый правомочиями лица на совершение тех или иных манипуляций со средствами компьютерной техники, исходя из его прямых функциональных обязанностей.

Кроме организационных мер, важное профилактическое значение в борьбе с преступлениями данной категории имеют меры технического характера, которые подразделяются на аппаратные, программные и комплексные. Данная классификация вызвана характером и спецификой охраняемого объекта.

Применение аппаратных методов обеспечивает безопасность средств связи компьютерной техники от нежелательного влияния со стороны, а также предупреждает утечку секретных сведений.

Данные методы применяются с помощью различных технических устройств:

1) источников бесперебойного питания, которые предохраняют от скачкообразных перепадов напряжения;

2) устройств экранирования аппаратуры, линий проводной связи и помещений, в которых размещается компьютерная техника;

3) устройств комплексной защиты телефонии;

4) оборудования, которое предоставляет возможность пользователю допуск лишь на защищаемые объекты средств компьютерной техники;

5) устройств идентификации и установления терминалов и пользователей при попытках неразрешенного доступа к компьютерной сети;

6) средств охранно-пожарной сигнализации;

7) средств защиты портов компьютерной техники и т. д.

Последние устройства наиболее эффективны для защиты компьютерных сетей от несанкционированного в них доступа и выполняют одновременно несколько защитных функций. Некоторые из них мы рассмотрим ниже.

Компьютер защиты порта сверяет код санкционированных пользователей с кодом в запросе. Если пользователь не определен, то компьютер автоматически разрывает связь с вызывающим абонентом. Указанные действия предохраняют компьютерную систему от совершения компьютерного преступления.

Отдельные средства, отвечающие за безопасность портов, маскирует существование портов на линии телефонной связи через синтезирование человеческого голоса, отвечающего на вызов абонента.

Следующая защитная функция направлена против способа совершения компьютерного преступления методом «маскарад». Преступник, который узнал код зарегистрированного пользователя, используя его, осуществляет несанкционированный доступ через любого телефонного абонента, выдавая себя за законного пользователя. В ответ на это средство защиты портов, в

памяти которого хранятся не только коды доступа, но и идентификационные номера телефонов, разрывает связь и автоматически выполняет установление связи с пользователем по второму реквизиту.

Для непосредственной защиты информации используют программные методы защиты, которые осуществляются в трех направлениях: а) аппаратура; б) программное обеспечение; в) данные и управляющие команды.

Самыми известными и широко распространенными программными профилактическими методами защиты информационных ресурсов от компьютерных вирусов являются программные антивирусные средства. Современные программы в кратчайшие сроки могут обнаружить и распознать вирус в информационных ресурсах, а также вылечить его.

При этом совместно с антивирусной программой нужно применять комплексные организационно-технические меры, которые заключаются в уведомлении сотрудников о возможном риске при совершении вирусного посягательства; запрете приносить на рабочее место непроверенные программные средства; проверке всех файлов, которые поступают из внешней компьютерной сети; создании архивов копий программ, которые используются в непосредственной работе организации; проведении проверки файлов; установке на персональном компьютере системы защиты информационных данных.

Для безопасности передачи компьютерной информации при ее передаче зачастую применяют различные методы шифрования данных перед их вводом в канал связи или на физический носитель с последующей расшифровкой. Как показывает практика, указанные меры позволяют достаточно надежно скрыть смысл сообщения.

Например, общеизвестная программа Diskreet из программного пакета Norton Utilities позволяет кроме шифрования магнитных носителей информации выполнять функцию блокировки клавиатуры и экрана вычислительной техники, а также может обезопасить информационные объекты на уровне файлов или виртуальных дисков винчестера. А для того чтобы возобновить нормальную работу, следует ввести пароль.

Программные методы защиты идентифицируют личность пользователя и определяют операции, какие он может выполнять и к каким данным у него имеется допуск. Выработано четыре метода, позволяющих установить личность пользователя, а именно: по предмету, которым он владеет; личному идентификационному коду, по антропометрическим характеристикам личности, а также по электронной цифровой подписи, которая основана на использовании криптографической системы с открытым ключом.

Таким образом, к средствам профилактики преступлений в сфере компьютерной информации можно отнести: совершенствование действующего уголовного, уголовно-процессуального и информационного законодательства; улучшение судебной практики; подготовку специалистов в этой области; разработку программно-аппаратных систем компьютерной защиты; закрепление в трудовых договорах (контрактах) положений о юридической ответст-

венности лиц за разглашение конфиденциальных сведений о системе защиты служебной информации; постоянный контроль руководителей за установкой и обновлением систем компьютерной защиты в государственных и муниципальных организациях; создание в нашей стране национальной операционной системы для компьютерных устройств, а также системы фиксации, идентификации преступлений в сфере компьютерной информации и компьютерных преступников; создание новых и совершенствование существующих методик выявления компьютерных преступлений с привлечением специалистов в области информационной безопасности.

Резюмируя вышесказанное, можно сделать вывод о том, что главными причинами и условиями совершения преступлений в сфере компьютерной информации являются: информационный прогресс общества, отсутствие или несоответствие средств защиты данных, отсутствие соответствующих служб безопасности, а также высокая латентность преступлений данного вида, позволяющая преступникам избегать наказания и совершать новые преступные посягательства. В связи с развитием науки перечень мер, направленных на предупреждение компьютерной преступности, может быть расширен. Но только интегративные и комплексные профилактические мероприятия, применяемые сотрудниками правоохранительных органов, смогут оказать положительное влияние на уровень информационной безопасности России и повысить эффективность предупреждения компьютерных преступлений.

Контрольные вопросы

1. Расскажите о причинах, способствующих совершению противоправных действий в сфере компьютерной информации.
2. В чем заключается система мер предупреждения компьютерных преступлений?
3. Каковы меры предупреждения компьютерных преступлений организационно-технического характера?
4. Опишите аппаратные методы обеспечения безопасности средств связи, компьютерной техники.
5. Охарактеризуйте программные методы защиты информации.

Заключение

Расширение и развитие информационной сферы закономерно влечет за собой появление технических, социальных и правовых проблем. Среди последних наиболее острой является проблема уголовного преследования за преступления, совершаемые в сфере компьютерной информации и высоких технологий.

Указанное обстоятельство обусловлено низким состоянием правовой культуры населения, его уровня грамотности в сфере компьютерных технологий в сравнении со специалистами в данной области. Это обстоятельство отягощается дополнительными факторами, такими как высокий уровень латентности преступлений в сфере компьютерной информации, отсутствие у некоторых категорий граждан даже базовых знаний в указанной области. Расследование преступлений такого вида представляет существенную сложность, сопряжено с использованием информационных технологий, обусловлено особым способом совершения преступления. Все это способствует возникновению трудностей и в обнаружении процессуально значимой информации, ее фиксации, изъятии и исследовании.

Отсутствие достаточного числа лиц, осуществляющих производство по уголовным делам, которые обладают специальными познаниями в области расследования преступлений, связанных с информационными технологиями, объясняет и отсутствие механизма осуществления оптимального противодействия рассматриваемым преступлениям.

Для грамотной организации работы по выявлению и расследованию данного вида преступлений сотрудникам правоохранительных органов необходимо знать положения уголовно-процессуального законодательства, касающиеся обстоятельств, подлежащих доказыванию, правила производства и процессуального оформления следственных и иных процессуальных действий, уметь ориентироваться в вопросах организационно-технической подготовки следственных действий и тактики их проведения, четко представлять способы собирания и исследования криминалистической информации о компьютерных преступлениях и лицах, их совершивших.

Безусловно, компьютерные преступления являются актуальным видом преступлений, механизм их расследования требует опыта и знания предмета деятельности. Более того, перечень преступлений, закрепленных в Уголовном кодексе в соответствующей главе, постоянно изменяется и дополняется, что, в свою очередь, требует дополнительных сведений и профессионального мастерства.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru/
2. Уголовный кодекс Российской Федерации (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru/
3. Уголовно-процессуальный кодекс Российской Федерации (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru/
4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ [Электронный ресурс]. – URL: http://www.garant.ru/
5. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ ФЗ [Электронный ресурс]. – URL: http://www.garant.ru/
6. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ [Электронный ресурс]. – URL: http://www.consultant.ru/
7. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ [Электронный ресурс]. – URL: http://www.consultant.ru/
8. О государственной тайне: закон РФ от 21.07.1993 № 5485-1 [Электронный ресурс]. – URL: http://www.consultant.ru/
9. О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1 [Электронный ресурс]. – URL: http://www.consultant.ru/
10. О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ [Электронный ресурс]. – URL: http://www.consultant.ru/
11. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ [Электронный ресурс]. – URL: http://www.consultant.ru/
12. О правовой охране программ для электронных вычислительных машин и баз данных: закон РФ от 23.09.1992 № 3523-1 [Электронный ресурс]. – URL: http://www.consultant.ru/
13. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 [Электронный ресурс]. – URL: http://www.consultant.ru/
14. Об организации прокурорского надзора за исполнением законов при приеме, регистрации и разрешении сообщений о преступлениях в органах дознания и предварительного следствия: приказ Генерального прокурора Российской Федерации от 05.09.2011 № 277 (ред. от 05.12.2016) [Электронный ресурс]. – URL: http://www.consultant.ru/
15. Об организации прокурорского надзора за процессуальной деятельностью органов дознания: приказ Генеральной прокуратуры РФ от 26.01.2017 № 33 [Электронный ресурс]. – URL: http://www.consultant.ru/

16. Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия: приказ Генерального прокурора Российской Федерации от 28.12.2016 № 826 [Электронный ресурс]. – URL: http://www.consultant.ru/

17. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, Следственного комитета Российской Федерации от 27.09.2013 № 776/703/509/507/1820/42/535/398/68 [Электронный ресурс]. – URL: http://www.consultant.ru/

Научная и учебная литература, периодические издания

18. *Антонова Э. Ю.* Доказывание как вид познания и его теоретическое и практическое значение / Э. Ю. Антонова // Пробелы в российском законодательстве. – 2015. – № 1. – С. 209–213.

19. *Бражник С. Д.* Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. … канд. юрид. наук / С. Д. Бражник. – Ижевск, 2002.

20. *Вехов В. Б.* Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации / В. Б. Вехов // Эксперт-криминалист. – 2013. – № 4. – С. 2–4.

21. *Гайфутдинов Р. Р.* Понятие и квалификация преступлений против безопасности компьютерной информации: дис. … канд. юрид. наук / Р. Р. Гайфутдинов. – Казань, 2017.

22. *Грибунов О. П.* Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие / О. П. Грибунов, М. В. Старичков. – Москва: ДГСК МВД России, 2017. – 160 с.

23. *Давлетов А. А.* Уголовное судопроизводство Российской Федерации: учеб. пособие / А. А. Давлетов. – Екатеринбург: УрЮИ МВД России, 2017. – 348 с.

24. *Дворецкий М.* Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ / М. Дворецкий, А. Копырюлин // Уголовное право. – 2007. – № 4. – С. 30.

25. *Дуленко В. А.* Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации [Электронный ресурс]: учеб. пособие / В. А. Дуленко. – Уфа: УЮИ МВД России, 2007. – 187 с. // URL: https://www.bestreferat.ru/referat-199192.html.

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

27. *Зигура Н. А.* Природа компьютерной информации как доказательства / Н. А. Зигура // Вестник Южно-Урал. гос. ун-та. Сер. Право. – 2009. – № 28(161). – С. 50–52.

28. Киберпреступность в России [Электронный ресурс]. – URL: http://www.tadviser.ru/index.php.

29. *Козлов В. Е.* Об отдельных аспектах криминалистического обеспечения противодействия преступлениям, совершаемым с использованием средств компьютерной техники / В. Е. Козлов // Вестник Академии МВД Республики Беларусь. – 2018. – № 1 (35). – С. 86–92.

30. Комментарий к уголовному кодексу Российской Федерации: в 2 т. (постатей.) / под ред. А. В. Бриллиантова. – Москва: Проспект, 2017. – Т. 2.

31. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) // СПС «Консультант Плюс».

32. *Попов К. И.* Правовые основы противодействия преступлениям в сфере компьютерной информации в сети интернет / К. И. Попов, А. В. Майоров // Вестник УрФО. Безопасность в информационной сфере. – 2013. – № 3 (9). – С. 38–42.

33. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учеб. пособие / под общ. ред. Б. Я. Гаврилова. – Москва: Проспект, 2017. – 160 с.

34. *Федосеева Е. Л.* Особенности использования технических средств при расследовании уголовных дел / Е. Л. Федосеева, И. И. Литвин // Обеспечение прав и законных интересов граждан в деятельности органов предварительного расследования: сб. статей. – Орел: ОрЮИ МВД России им. В. В. Лукьянова, 2017. – С. 235–238.

35. *Хисамова З. И.* Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. … канд. юрид. наук / З. И. Хисамова. – Краснодар, 2016. – 222 с.

36. *Чистова Л. Е.* Расследование преступлений в сфере незаконного оборота сильнодействующих или ядовитых веществ: монография / Л. Е. Чистова. – Москва: Юрлитинформ, 2014. – 232 с.

Содержание

Расследование преступлений в сфере компьютерной информации

Учебное пособие

Редактура и компьютерная верстка *И. Б. Бебих*

Подписано в печать 18.09.2019. Формат 60х84 1/16
Печать трафаретная. Бумага офисная
Усл. печ. л. 4,5. Уч.-изд. л. 4,5
Тираж 81 экз. Заказ № 41

Типография научно-исследовательского
и редакционно-издательского отдела
Уральского юридического института МВД России

620057, Екатеринбург, ул. Корепина, 66