Федеральное государственное автономное
образовательное учреждение
высшего профессионального образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт

Кафедра уголовного процесса и криминалистики

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Д. Назаров
подпись инициалы, фамилия
«14» июня 2017 г.

БАКАЛАВРСКАЯ РАБОТА

_____
код – наименование направления

Способы совершения преступлений в сфере компьютерной информации

Научный руководитель	_____ подпись, дата	доцент, к.ю.н. должность, ученая степень	И.Г. Иванова инициалы, фамилия
Выпускник	_____ подпись, дата		А.С. Нестерова инициалы, фамилия

Красноярск 2017

Содержание

Введение

Преступления в сфере компьютерной информации в России и в мире имеют очень быструю динамику развития, число пострадавших от киберпреступников увеличивается с каждым днем. Если в 60-х годах компьютерные сети использовались в основном в военных и научных целях, где главной опасностью являлась утрата секретной информации, а также несанкционированный доступ к ней, то в 70-е годы на первый план вышли проблемы экономической преступности в сфере компьютерных технологий – взломы банковских компьютерных сетей, промышленный шпионаж. В 80-х годах широко распространенными преступлениями стали взломы и незаконное распространение компьютерных программ.

Активные пользователи сети интернет появились еще в 80-х годах XX века в США, однако, только в середине 90-х годов подобная активность зародилась в России. Знания множества талантливых людей, проживавших на территории бывшего СССР, остались недооцененными, а также мало оплачивались в 90-е годы, это и породило всплеск компьютерных преступлений, а также преступлений с использованием компьютеров и интернет сетей. Его последствия начинают сглаживаться для России только сейчас.

В настоящее время можно отметить качественную трансформацию преступности в сфере компьютерной информации – она приобретает экономическую и политическую окраску. Растет количество экономических преступлений, совершенных с использованием электронных средств, а их способы становятся все более изощренными и технически совершенными. Это требует от правоохранительных органов постоянной работы по разработке новых технических средств, приемов противодействия киберпреступности, которая стала носить межгосударственный характер. Все указанное обуславливает актуальность выбранной темы бакалаврской работы.

Объектом исследования выступают общественные отношения, подвергающиеся посягательству различными способами с использованием средств компьютерной техники.

Целью работы является всестороннее изучение и описание способов совершения преступлений в сфере компьютерной информации.

Для достижения указанной цели, были поставлены следующие задачи:

- описать криминалистическую характеристику преступлений в сфере компьютерной информации; дать характеристику способу совершения преступления, как основного элемента криминалистической характеристики, обозначить его значение и связь с другими элементами; проанализировать российское законодательство и законодательство СНГ, регулирующее отношения в сфере компьютерной информации.

- раскрыть способы совершения преступлений в сфере компьютерной информации, предусмотренные главой 28 УК РФ; проанализировать применение данных способов с использованием опубликованной судебной практики и заключений экспертов.

Нормативно-правовую базу исследования составили федеральный закон «Об информации, информационных технологиях и о защите информации», федеральный закон «О ратификации Соглашения о сотрудничестве государств-участников Содружества независимых государств в борьбе с преступлениями в сфере компьютерной информации», постановление Правительства Российской Федерации «О сертификации средств защиты информации», уголовное законодательство Российской Федерации.

Теоретической основой работы послужили труды В.Б. Вехова, Г.Г. Зуйкова, Е.А. Маслакова, М.М. Малыковцева, В.А. Образцова, А.Л. Осипенко, Н.Н. Федотова, Е.А. Шаркова, Н.П. Яблокова и многих других ученых.

Практической базой работы явились справки о компьютерно-техническом исследовании, полученные в отделе «К» ГУ МВД России по

Красноярскому краю, опубликованная судебная практика из справочных правовых систем «РосПравосудие», «СудПрактика», уголовные дела из архива Красноярского краевого суда.

Структурно работа состоит из введения, двух глав, заключения, списка использованных источников и приложений. Во введении обоснована актуальность темы бакалаврской работы, описаны ее цель, задачи, теоретическая и практическая база. В первой главе раскрываются вопросы криминалистической характеристики преступлений в сфере компьютерной информации, способа совершения преступления как основного элемента криминалистической характеристики преступления. Во второй главе раскрыты различные способы совершения преступлений в сфере компьютерной информации. В заключении сделаны основные выводы.

1 Криминалистическая характеристика преступлений в сфере компьютерной информации. Способ совершения преступления, как основной элемент криминалистической характеристики, его значение и связь с другими элементами

1.1 Понятие и структура криминалистической характеристики преступлений в сфере компьютерной информации.

Переходя к криминалистической характеристике преступлений в сфере компьютерной информации и описанию способов их совершения, необходимо несколько слов сказать о понятии криминалистической характеристики преступления вообще.

В научный оборот данное понятие введено в 60-х годах XX века, его появление было обусловлено необходимостью разработки ряда частных методик по расследованию различных видов преступлений. В настоящее время данная тема не теряет своей актуальности в связи с постоянно изменяющейся окружающей обстановкой, а также с появлением новых видов преступлений[1]. Однако в научной литературе нет единства мнений по поводу понятия и содержания криминалистической характеристики преступлений.

Так, Н.П. Яблоков под криминалистической характеристикой преступления понимает систему описания криминалистически значимых признаков вида, группы и отдельного преступления, проявляющихся в особенностях способа, механизма и обстановки его совершения, дающую представление о преступлении, личности его субъекта и иных обстоятельствах, об определенной преступной деятельности, и имеющая своим назначением обеспечение успешного решения задач раскрытия, расследования и предупреждения преступлений[2].

1Милюс А.И. К вопросу о криминалистической характеристике краж нефти и нефтепродуктов / А. И. Милюс // Вестник Кемеровского государственного университета. – 2014. – № 2. – С. 274.

2 Яблоков Н.П. Криминалистическая характеристика преступлений и типичные следственные ситуации как важные факторы разработки методики расследования преступлений / Н.П. Яблоков // Вопросы борьбы с преступностью.– 1979. – № 30. – С. 21.

По мнению В.С. Бурдановой, криминалистическая характеристика преступления выступает в качестве типовой информационной модели, совокупности данных или сведений, полученных в результате специальных исследований[3].

Исходя из вышесказанного, можно сделать вывод о том, что криминалистическая характеристика представляет собой систему типичных признаков, которые зависят от вида преступления. Знание указанных признаков способствует решению задач, стоящих перед следователем. Сталкиваясь в очередной раз с преступлением, следователь воспроизводит в памяти похожие дела из своей практики, затем выдвигает предположение, что данное преступление – типично, и применяет способы поиска доказательств, приносившие успех в аналогичных делах ранее. Полагаем, именно такой формализованный опыт, система знаний о преступлении определенного вида или группы называется криминалистической характеристикой преступлений.

Ученые на протяжении многих лет пытались конкретизировать состав сведений, подлежащих включению в криминалистическую характеристику преступления, а также определить ее значение в методике расследования.

Так, А.В. Самойлов описал основные требования, которые должны предъявляться к критериям отбора каждого из элементов криминалистической характеристики преступлений:

1) теоретическая доказанность (в том числе подтвержденная практикой органов дознания и предварительного следствия);

2) значимость тех или иных из них для научного и практического решения задач по выявлению, раскрытию преступлений и осуществлению уголовного преследования[4].

3 Бурданова В.С. Криминалистическая характеристика преступлений, связанных с незаконным оборотом наркотиков / В.С. Бурданова // Прокурорско-следственный работник. –1998. – № 3. – С.7.

4 Самойлов А.В. Современное состояние учения о криминалистической характеристике преступлений / А. В. Самойлов // Российский следователь. – 2010. – № 22. – С. 5.

По мнению С.А. Бесснова, криминалистически значимыми признаками, подлежащими включению в содержание криминалистической характеристики преступлений, являются следующие:

1) обстановка преступления (место, время и другие обстоятельства);
2) способ совершения и сокрытия преступления;
3) материальные следы преступления и вероятные места их нахождения (в том числе механизм следообразования);
4) предмет преступного посягательства;
5) личность потерпевшего;
6) личность преступника[5].

С.И. Коновалов определил иерархию структурных элементов криминалистической характеристики преступлений. Основанием построения явилась частота их употребления при разработке учеными криминалистических характеристик различных по видам преступлений. Им определена следующая иерархическая цепочка:

1) способ совершения преступления, субъект преступления (особенности личности), обстановка совершения преступления, объект (предмет) преступного посягательства, следы преступления (механизм следообразования);

2) связи между структурными элементами;

3) личность жертвы (виктимологический аспект), мотив, цель, установка, условия совершения преступления, преступные связи (коммуникационный аспект), типичные ситуации совершения преступления, особенности сокрытия преступления, механизм преступления, типичные следственные ситуации (характер исходных данных и особенности их обнаружения), состояние борьбы с определенным видом преступления, связь с другими видами преступлений;

5 Бессонов С.А. К вопросу о структуре и природе криминалистической характеристики преступлений / С. А. Бессонов // Вестник Поволжского института управления. – 2014. – № 4(43). – С. 54.

4) орудия и средства преступной деятельности, результат преступной деятельности (последствия)[6].

Полагаем, что с предложенной С.И. Коноваловым иерархией структурных элементов криминалистической характеристики преступления трудно согласиться, поскольку, помимо структурных элементов преступления (механизма его совершения, обстановки и т.д.), им также сюда необоснованно включены и структурные элементы процесса расследования преступлений (типичные следственные ситуации и т.д.).

Традиционно в структуру криминалистической характеристики преступления включаются сведения о: предмете преступного посягательства, обстановке совершения преступления (с учетом времени, места и других условий), способе и механизме совершения преступления, его последствиях следах, личности преступника и потерпевшего.

По мнению В.Б. Вехова, в криминалистическую характеристику преступлений в сфере компьютерной информации должны входить криминалистически значимые сведения о личности правонарушителя, мотивации и целеполагании его преступного поведения, типичных способах, предметах и местах посягательств, а также о потерпевшей стороне[7].

Похожую позицию занимает и Н.Н. Лысов, который включает в структуру криминалистической характеристики способы совершения компьютерных преступлений, следовую картину, личность преступника и условия, способствующие совершению компьютерных преступлений[8].

Н.Г. Шурухнов включил в состав криминалистической характеристики неправомерного доступа к компьютерной информации следующие элементы:

6 Коновалов С. И. Теоретико-методологические проблемы криминалистики: монография / С.И. Коновалов. – Ростов-на-Дону: РЮИ МВД России, 2001. – С. 85.

7 Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В. Б. Вехов; под ред. Б.П. Смагоринского. – М.: Право и Закон, 1996. – С. 28.

8 Лысов Н.Н. Содержание и значение криминалистической характеристики компьютерных преступлений / Н.Н. Лысов // Проблемы криминалистики и методики ее преподавания: Тезисы выступл. участников семинара-совещания преподавателей криминалистики. – М., 1994. – С. 54.

1) данные о способах подготовки, совершения и сокрытия преступления;

2) данные об орудиях (средствах) совершения преступления;

3) данные об обстановке и месте совершения преступления;

4) данные о следах;

5) данные о предмете преступного посягательства;

6) данные о виновных лицах[9].

Г.В. Семенов предлагает расширить состав криминалистической характеристики за счет включения в нее описания механизма следообразования, а также мотива и цели совершения преступлений[10].

Таким образом, при анализе подходов тех или иных ученых к определению понятия и содержания криминалистической характеристики преступлений в сфере компьютерной информации можно судить об их согласовании с общим представлением о данной криминалистической категории.

1.2 Предмет преступления.

Предметом преступления выступает компьютерная информация.

Согласно примечанию к статье ст. 272 УК РФ, под компьютерной информацией понимаются сведения (сообщения и данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В соответствии с п. 1 ст. 2 федерального закона от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и защите

9 Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: учебное пособие / Ю.В. Гаврилин, А.В. Пушкин, Е.А. Соцков, Н.Г. Шурухнов; под общ. ред. Н.Г. Шурухнова. – Изд. 2-е, перераб. и доп. – М.: ЮИ МВД РФ, Книжный мир, 2004. – С. 320.

10 Семенов Г.В. Криминалистическая характеристика неправомерного доступа к компьютерной информации в системе сотовой связи / Г.В. Семенов // Юридические записки. Криминалистические средства и методы исследования преступлений. – 2001. – № 10. – С. 187.

информации», информация – это сведения (сообщения, данные) независимо от формы их представления[11].

В соглашении «О сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации», которую Российская Федерация ратифицировала 01.10.2008 года, под компьютерной информацией понимается информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети[12]. Из этого определения можно сделать вывод, что компьютерной является любая информация, которая содержится на электронном материальном носителе.

В научной литературе выделяются следующие характеристики компьютерной информации:

1) она объёмна и быстро обрабатываема;

2) она очень легко и, как правило, бесследно уничтожаема;

3) она обезличена, т.е. между ней и лицом, которому она принадлежит, чаще всего нет жесткой связи;

4) она может находиться лишь на машинном носителе (дискете, магнитной ленте, лазерном диске, полупроводниковых схемах и др.), в самой ЭВМ (оперативной памяти – ОЗУ);

5) она может создаваться, изменяться, копироваться, применяться (использоваться) только с помощью ЭВМ;

6) она легко передаётся по телекоммуникационным каналам связи компьютерных сетей, причём практически любой объём информации можно передать на любое расстояние;

7) она относительно проста в пересылке, преобразовании, размножении; при её изъятии, в отличие от изъятия вещи, она легко сохраняется в первоисточнике; доступ к одному и тому же файлу,

11 Об информации, информационных технологиях и защите информации: федеральный закон от 27.07.2006 г. № 149-ФЗ // Российская газета. – № 165. – 29.07.2006.

12 О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: федеральный закон от 01.10.2008 г. № 164-ФЗ // Собрание законодательства РФ. – 06.10.2008. – № 40. – Ст. 4499.

содержащему информацию, могут одновременно иметь несколько пользователей[13].

По мнению Н.А. Зигуры, компьютерная информация – это сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации, а также набор команд (программ), предназначенные для использования в электронно-вычислительной машине (ЭВМ), системе ЭВМ или управления ими[14].

В свою очередь В.А. Мещеряков полагает, что компьютерная информация является информацией, представленной в специальном (машинном) виде, предназначенном для ее автоматизированной обработки, хранения и передачи, которая находится на материальном носителе и имеет собственника, установившего порядок ее создания (генерации), обработки, передачи и уничтожения[15].

Исходя из смысла, вкладываемого в понятие «компьютерная информация» и её функционала, можно сделать вывод о том, что помимо отдельных качественных характеристик данного явления имеется потребность в совершенствовании понятийно-терминологического аппарата таких понятий, как компьютерная информация, носитель информации и т.п.

Так, на наш взгляд, термин «электронно-вычислительная машина» является пережитком далекого прошлого и с современной реальностью борьбы с преступлениями в сфере компьютерной информации и мобильных коммуникаций имеет мало общего.

Сравнительно недавно в России появились первые биометрические паспорта, имеющие пластиковую страницу с электрочипом, содержащим в

13 Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. … канд. юрид. наук: 12.00.08 / Шарков Александр Евгеньевич. – Ставрополь, 2004. – С. 30.

14 Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: дис. … канд. юрид. наук: 12.00.09 / Зигура Надежда Анатольевна. – Челябинск, 2010. – С. 15.

15 Понятие «компьютерная информация» с точки зрения ее уголовно-правовой защиты [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/ponyatie-kompyuternaya-informatsiya-s-tochki-zreniya-ugolovno-pravovoy-zaschity

себе всю информацию о владельце документа. В немецкой компании DN-Systems создано устройство, способное на перехват сигналов с этих чипов, что влечет за собой копирование полученной информации на другой чип и, как следствие, её подделку или блокирование.

В связи с появлением подобных новых носителей компьютерной информации встает вопрос: могут ли чипы, паспорта, смартфоны, банкоматы, устройства, содержащие микропроцессоры (компьютеризированная бытовая техника: стиральные машины, телевизоры и т.д.) считаться электронно-вычислительной машиной или нет. Или для подобных устройств требуется введение нового термина, на качественно новом уровне отражающего конструктивное содержание и особенности информации, в них содержащейся.

Исходя из вышесказанного, можно сделать вывод:

1) компьютерная информация, являясь предметом рассматриваемой группы преступлений, трактуется по-разному в различных нормативных актах, будь то Уголовный кодекс РФ, соглашение «О сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации» или федеральный закон от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

2) в научной литературе отсутствует единство мнений по вопросу о том, как представлена компьютерная информация во вне: согласно одной точке зрения, она представлена в электронно-цифровой форме на материальном носителе, по мнению других, она представлена в специальном (машинном) виде;

3) требует усовершенствования понятийно-терминологический аппарат относительно таких понятий, как: компьютерная информация, носитель информации, электронно-вычислительная машина;

4) требуется введение новых понятий, характеризующих конструктивное содержание и особенности информации, содержащейся на новейших гаджетах, бытовых устройствах.

1.3 Личность преступника.

Личность преступника является одним из основных элементов криминалистической характеристики преступления определенного вида или группы.

В криминалистике личность субъекта, совершившего преступление, устанавливается через познание ее отдельных свойств и качеств, получающих отражение в следах преступления, с тем, чтобы затем использовать эти знания в качестве средств воздействия на данную личность при производстве следственных действий[16].

Среди лиц, совершающих преступления в сфере компьютерной информации, могут быть, как высококвалифицированные специалисты, так и любители, имеющие различный уровень образования и социального статуса.

С начала 90-х годов XX века пик хакерской деятельности в мире приходился на возраст 16-19 лет, на сегодняшний день диапазон расширился от 12-33 лет (рисунок 1).

1990–2000 года 2001–2016 года

16 Ведерников Н.Т. Личность преступника в криминалистике и криминологии / Н.Т. Ведерников // Вестник Томского государственного университета. – 2014. – № 384. – С. 148.

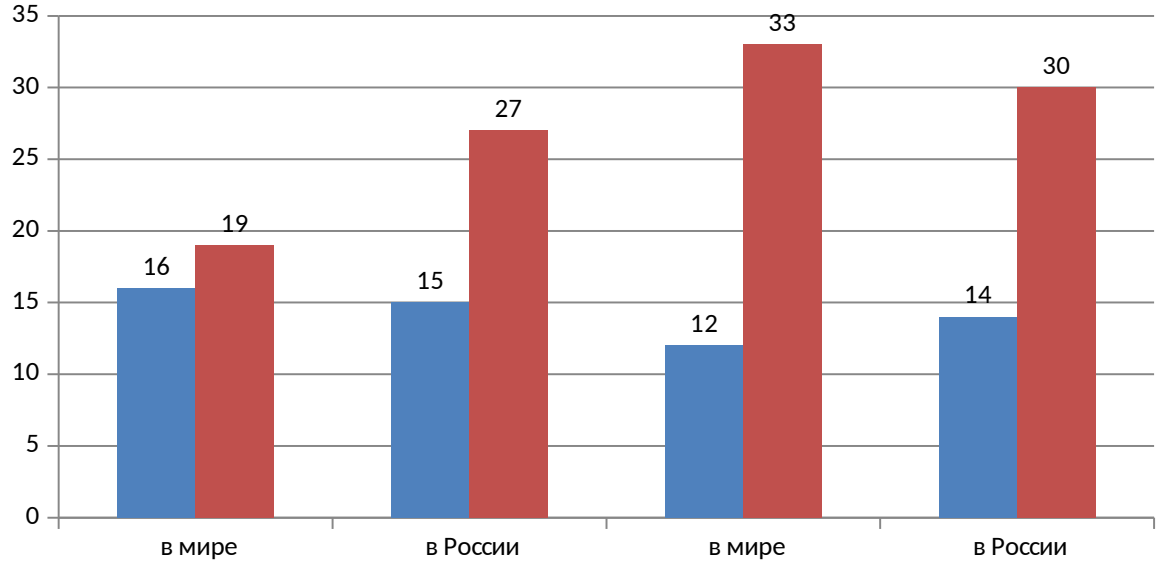


Рисунок 1 – Диапазон возрастных групп киберпреступников

Возрастной диапазон обусловлен массовостью в овладении компьютерной техникой, а так же внедрением технологий высокоскоростной передачи данных, особенной такой не защищенной как Wi-Fi.

Сведения о поле лиц, характеризуют рассматриваемые преступления, как деяния для мужчин (от 86% до 92%), доля женщин колеблется от 4,8 до 12,2%. Однако просматривается возрастающая динамика доли женщин–преступниц по причине профессиональной ориентации некоторых специальностей (секретарь, делопроизводитель, бухгалтер, контролер, кассир и другие) по использованию в работе средств компьютерной техники. Все чаще встречаются факты пособничества женщин совершению преступлений в сфере компьютерной информации.

В криминалистической литературе неоднократно рассматривалась классификация лиц, совершающих преступления в сфере компьютерной информации. Одна группа, которую очень часто выделяют и которая находится у всех на слуху – «хакеры», профессионалы высокого класса, осуществляющие «взлом» систем компьютерной защиты и безопасности. Первоначально зародилось это движение в Америке среди молодежи, в частности, у сторонников неограниченной свободы – хиппи. С течением

времени интенсивность роста этой категории лиц возросла, среди причин можно выделить следующие:

а) институционализацию хакерства и ведение целенаправленной пропагандистской деятельности;

б) проявление заинтересованности криминальных и государственных структур в сотрудничестве с хакерами, что способствует резкому повышению их самооценки;

в) привлечение ряда известных хакеров после отбытия тюремного наказания на престижные должности в ведущие фирмы;

г) романтизацию образа хакера средствами массовой информации[17].

Также можно выделить такой вид преступников, как «кракеры». В отличие от «хакеров», исследующих вычислительную систему и обнаруживающих слабые места в ее системе безопасности, путем информирования пользователей и разработчиков системы, с целью последующего устранения найденных недостатков, «кракеры», осуществляя взлом компьютерной системы, действуют с целью получения несанкционированного доступа к чужой информации.

Среди «кракеров» выделяются три категории взломщиков:

«Вандалы» – самая известная и самая малочисленная часть кракеров. Их основная цель – взломать систему для ее разрушения. Такой тип кракеров обычно характерен для новичков.

«Шутники» – наиболее безобидная часть кракеров (в зависимости от предпочтения злых шуток), основной целью которых является известность. Достигается данная известность путем взлома компьютерных систем и внесением туда различных эффектов, выражающих их неудовлетворенное чувство юмора. Существенный вред «шутники» не наносят (разве что моральный). Это наиболее распространенный класс кракеров, обычно осуществляющих взлом Web-серверов оставляя там упоминание о себе. «Шутниками» могут быть и создатели вирусов, с различными визуально-

17 Скородумова О.Б. Хакеры / О.Б. Скородумова // Знание. Понимание. Умение. – 2005. – № 4. – С. 160.

звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок, квадратов и т.п.).

В качестве примера можно привести уголовное дело № 1- 176/2016, рассмотренное Харабалинским районным судом Астраханской области в отношении Сергеева Я.О., который, имея умысел на использование вредоносного сайта, с целью блокирования сайта Р., загрузил домашнюю страницу вредоносного сайта, ввёл свой логин и пароль, затем путем нажатия кнопки, запустил разновидность компьютерной атаки, целью которой являлось создание таких условий, при которых легитимный пользователь сайта Р. не мог получить к нему доступ около двух часов подряд, при входе обнаруживая черный фон вместо заглавной страницы[18].

«Взломщики» – профессиональные кракеры, пользующиеся наибольшим почетом и уважением в виртуальной среде. Основной задачей «взломщиков» является взлом компьютерной системы с целью кражи или подмены хранящейся там информации[19].

Обособленной группой являются создатели вирусов – вирмейкеры (от англ. virus – вирус и maker – создавать). Выделяется несколько категорий вирмейкеров:

1) Trader (англ. торговец) – коллекционеры вирусов. Сами вирусов не прописывают, но путем их коллекционирования налаживают обмен образцов между собой;

2) Destroyers (англ. разрушители) – создатели троянских программ-вандалов, занимающихся форматированием винчестеров, стиранием файлов на дисках. В большинстве своем деструкторы создают алгоритмы для массового поражения компьютерных систем;

3) Coder (англ. кодировщик) – начинающие вирмейкеры пробующие свои силы в написании вирусов;

18 Приговор Харабалинского районного суда Астраханской области по делу Сергеева Я.О. от 21.11.2016 года по уголовному делу № 1- 176/2016 // Справочная правовая система «РосПравосудие». – Режим доступа: https://rospravosudie.com.

19 Кто такие кракеры [Электронный ресурс]. – Режим доступа:http://it-sektor.ru/kto-takoyi-cracker-/-kraker.html.

4) Фанатики – создают группы вирмейкеров, вовлекая в них новых членов, придумывают и навязывают собственную идеологию, порой, выходя за рамки собственноручно созданных групп, пытаются влить идеологию в массы вирмейкеров;

5) Researcher (англ. исследователь) – подавляющий процент участников данной группы составляют западные вирмейкеры. Данная деятельность для них только хобби, в повседневности они либо профессиональные программисты, либо создатели антивирусных программ. Исследователи создают «образцы» вирусов для демонстрации возможностей нового штамма и отсылают на сайты антивирусов для поиска вариантов борьбы с ними;

6) Рядовые вирмейкеры – около 90% подобного типа людей занимаются вирмейкинком для того, чтобы выделиться среди своих сверстников.

Кроме создания вредоносных программ уголовно наказуемо и их применение. Лицо, использующее такую программу, тоже в большинстве случаев не реализует результаты своего труда непосредственно, а продает или передает их дальше, другим членам преступной группы.

Четвертый тип – это реализаторы результатов применения вредоносных программ, то есть спамеры, вымогатели, кардеры, мошенники[20].

Спамеры. Первый сообщник пишет и модернизирует программное обеспечение с целью незаметного проникновения на компьютер пользователя. Второй приобретает право пользования на данную программу, обеспечивает массовую рассылку и принимает обратный сигнал от благополучно внедрившихся вирусов, что помогает в будущем создать систематизированную зомби-сеть, оконченный вариант которой, целиком или частично, он продает третьему сообщнику. Третий, используя полученный продукт, занимается рассылкой спама, заказы на который

20 Федотов Н.Н. Форензика – компьютерная криминалистика: учебное пособие / Н.Н. Федотов. – М.: Юридический Мир, 2007. – С. 69.

принимает четвертый сообщник, полученное от заказчиков вознаграждение перечисляется третьему, как оплата услуг. И, наконец, пятый сообщник отвечает за сбор и систематизацию адресов электронных почт для рассылок спама, которые так же может продать.

Кардеры. Группа сообщников занимается сбором реквизитов банковских карт (номер карты, ФИО, срок действия, код безопасности). Данные с карточек клиентов снимаются незаметно, если человек, занимающийся этим, состоит в штате в качестве официанта или продавца. Еще больший объем карт проходит через руки менеджеров в фирмах и банках. Проводится тщательная проверка реквизитов карт, действительность и пригодность их для платежей. Также ими создаются и поддерживаются платные веб-сайты или псевдо-магазины с возможностью оплаты услуг карточками, которые служат для отмывания денег.

Фишеры. Phishing (англ. fishing – рыбная ловля) – связан со взломом страниц в социальных сетях. Доступ к информации из «списка друзей» преступник получает также обычно под видом «друга».

Ежегодно оборот в 50 млн. долларов приходится именно на продажу данных, похищенных с помощью фишинга. В Уголовном кодексе РФ отсутствует специальный состав преступления, предусматривающий ответственность за фишинг. В зависимости от специфики совершения, такие деяния квалифицируются по ст. 158, 183, 187 и 272 УК РФ, что вызывает сложности в правильности квалификации данного вида преступления. В 2014 году были предприняты первые попытки борьбы с фишингом: Национальный совет финансового рынка подготовил законопроект, предусматривающий изменение статей 159.3 и 187 УК РФ, а также дополнение в Уголовный кодекс. Был предложен следующий вариант санкции за фишинг: лишение свободы сроком до 10 лет и штраф в размере до двух миллионов рублей.

Инициатива была одобрена Центральным Банком России, но развитие законопроект не получил[21].

Таким образом, личность преступников по рассматриваемой группе преступлений дифференцирована и варьируется в зависимости от уровня образования и социального статуса человека.

1.4 Обстановка совершения преступлений.

Обстановка совершения преступления, как элемент криминалистической характеристики преступлений в сфере компьютерной информации, в научной литературе разработан не достаточно и нуждается в дальнейшем исследовании.

В.А. Образцов рассматривает обстановку совершения преступления как территориальную, климатическую, демографическую и иную специфику региона, в которой совершено преступление, а также обстоятельства, характеризующие непосредственно место, время, условия и другие особенности совершения преступления[22].

О.А. Кудряшова полагает, что обстановка выступает в качестве «несущего каркаса», который объединяет в единую систему, и все элементы механизма преступного деяния, и соответствующие изменения в материальной и социальной среде, как отражения противоправной или иной деятельности участников расследуемого события[23].

Традиционно местом преступления является место, где произошло деяние, значимое в криминалистическом и уголовно-правовом отношении. Нередко в силу особенностей использования технологии удаленного доступа, вредоносных программ местоположение некоторых программных и

21 Омарова Э.А. Мошенничество в финансово-кредитной сфере / Э.А. Омарова, Ю.М. Махдиева // Пути повышения финансовой стабильности регионов Северного Кавказа: взгляд молодых ученых: материалы Всероссийской научно-практической конференции студентов, аспирантов и молодых преподавателей. ФГБОУ ВО «Дагестанский государственный университет», г. Махачкала, (20-22 октября 2016 г.) / под общ. ред. Ю.М. Махдиевой. – Махачкала, 2016. – С. 130.

22 Образцов В.А. Теоретические основы раскрытия преступлений, связанных с ненадлежащим исполнением профессиональных функций в сфере производства / В. А. Образцов. – Иркутск, 1985. – С. 98.

23 Кудряшова О.А. Криминалистическое значение обстановки совершения преступления / О. А. Кудряшова // Вестник Южно-Уральского государственного университета. – 2011. – № 27. – С. 49.

аппаратных средств совершения преступления, отдельных технических и программных компонентов, например, электронной платежной системы преступника, не совпадают.

Местоположение любого из перечисленных элементов характеризуется двумя составляющими: местоположением в реальном пространстве (роль индивидуализирующей информации играет адрес местонахождения физического лица, организации, используемых ими аппаратно-программных средств) и местоположением, которое постоянно отождествляется в локальной и глобальной сети с уникальным номером – IP-адресом[24].

Данные преступления совершаются в специфической среде – виртуальном кибернетическом пространстве. Особенностью их является то, что в результате использования информационных сетей (проводных и беспроводных технологий) в одном преступлении одновременно могут быть задействованы множество компьютеров. Соответственно находиться эти компьютеры могут в пространственно удаленных друг от друга местах и даже в разных государствах[25].

Таким образом, обстановка совершения преступлений в сфере компьютерной информации, в силу своей не изученности, требует повышенного внимания, так как является «каркасом», отражающим деятельность участников события и вбирающим в себя все элементы механизма преступного деяния.

1.5 Личность потерпевшего.

На практике потерпевшими от компьютерных преступлений обычно выступают юридические лица. Это объясняется тем, что на данный момент в России в процесс компьютеризации втянуты различные учреждения,

24 Олиндер Н.В. Время и место совершения преступления как элемент криминалистической характеристики преступлений, совершенных с использованием электронных платежных средств и систем / Н.В. Олиндер // Вестник Самарского государственного университета. – 2014. – № 11-1. – С. 91.

25 Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В.В. Поляков // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114.

организации и предприятия всех форм собственности. Высокая продажная цена средств компьютерной техники на внутреннем рынке, тем более в условиях кризиса российской экономики, породила оставление большинства населения страны (физических лиц) вне сферы своего влияния.

Вторая группа потерпевших как раз те, кто пользуется услугами, предоставляемыми юридическими лицами, и попадают под действие кибератак, обрушивающихся на компанию-источник услуги.

Третья группа потерпевших страдает от «компьютерных пиратов». «Компьютерные пираты» – осуществляют кражу лицензированной компьютерной продукции путем её копирования, тиражирования и перепродажи преимущественно в Азиатских странах.

Кроме краж лицензированной компьютерной продукции, также распространены преступления, связанные с нейтрализацией защиты программ, которые позволяют произвести использование программного продукта без покупки официальной лицензии.

Так, 14.12.2016 года Кировский районный суд г. Красноярска рассмотрел уголовное дело № 1-606/2016 в отношении Любутина А.Л., который из корыстной заинтересованности распространил программу, заведомо предназначенную для нейтрализации средств защиты компьютерной информации. Находясь у себя дома, с неустановленного интернет-сайта он приобрел модифицированные файлы для нейтрализации защиты программы, позволяющие произвести использование программного продукта без покупки официальной лицензии. Указанную компьютерную информацию Любутин А.Л. записал на имеющийся у него съемный машинный носитель, который затем продал за денежное вознаграждение в размере 1 000 рублей Гаврилюку П.Л., действующему в рамках оперативно-розыскного мероприятия. Указанный съемный машинный носитель содержал вредоносную компьютерную информацию: модифицированные файлы, при использовании которых на компьютере пользователя нейтрализуются средства защиты компьютерной программы, тем самым устраняются

установленные производителем технические ограничения по защите авторских прав от незаконного использования, предусмотренные ст. 1299 ГК РФ, в соответствии с которой техническими средствами защиты авторских прав признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения[26].

В начале сентября 2015 года компания Symantec, занимающаяся разработкой программного обеспечения в области информационной безопасности и защиты информации, опубликовала результаты исследования, в котором участвовало 13 тысяч человек из 24 стран мира, в том числе из России: почти каждый второй гражданин в возрасте 18 лет за последние 12 месяцев становился жертвой киберпреступлений, что составляет в общей сложности 556 миллионов человек. Лидер по числу жертв – Россия.

Основным условием возникновения такого большого количества жертв компьютерных преступлений в России, на наш взгляд, является техническая безграмотность населения.

Для предупреждения преступности и повышения технической грамотности населения можно рекомендовать принять ряд мер:

1) в зависимости от знаний и навыков среднестатистического пользователя компьютера разработать руководство;

2) путем использования буклетов, рекламы и презентаций распространить выработанные рекомендации (руководства), также через использование интернет-сетей, а именно сайтов правоохранительных органов, в социальных сетях размещать ссылки с названием, привлекающим пользователя, как следствие, при переходе по ссылке будут отображаться указанные рекомендации;

26 Приговор Кировского районного суда г. Красноярска по делу Любутина А.Л. от 14.12.2016 года по уголовному делу № 1-606/2016 // Справочная правовая система «РосПравосудие». – Режим доступа: https://rospravosudie.com

3) организовать круглые столы в институтах повышения квалификации, в различных учебных заведениях, начиная со школьного уровня;

4) привлечь к сотрудничеству СМИ, а также магазины по продаже компьютерного оборудования, крупные технические компании и компании, занятые созданием антивирусных программ.

Если пользователь действительно захочет пойти навстречу данным мерам, в целях своей же безопасности, научится, как не стать жертвой компьютерного преступления, то в таком случае сеть интернет станет менее привлекательной для киберпреступников.

Одной из проблем потерпевших от подобных преступлений является и то, что они не могут обнаружить факт совершения данного противоправного деяния до тех пор, пока не наступят материальные последствия, и даже в этом случае большинство не обращаются в правоохранительные органы.

Р.И. Дремлюга полагает, что это обусловлено следующими причинами:

1) нежелание давать правоохранительным органам доступ в свой компьютер (личный или рабочий), открывать доступ к своим личным данным или данным, связанным с работой;

2) нежелание тратить время на обращение за защитой в правоохранительные органы;

3) неверие в то, что преступник будет наказан;

4) боязнь огласки инцидента: руководители коммерческих организаций боятся, что огласка подобных инцидентов привлечет новых преступников;

5) низкая правовая культура и правосознание[27].

27 Дремлюга Р. И. Интернет-преступность: монография / Р. И. Дремлюга. – Владивосток: Дальневосточный университет, 2008. – С. 154.

1.6 Следы преступных действий.

Различают криминалистическое понятие следов в широком и узком значении. В широком смысле «след» – это любые материальные последствия преступления, изменения объекта или вещной обстановки. К следам в узком специальном значении относятся материально-фиксированные отображения признаков внешнего строения одних объектов на других[28].

Следом компьютерного преступления будет являться любое изменение файловой системы, связанное с фактом свершившегося преступного деяния. Сама файловая система является совокупностью именованной области данных, представленной на носителе информации. И изменение местоположения этих информационных единиц, а также изменение наименования файлов, характеристик, формата, создание новых или удаление из системы каких-либо иных файлов выражает вмешательство в привычный уклад системы.

Из-за специфики средств, которыми совершаются данные преступления, следы представляют собой совокупность материально-фиксированных и виртуальных следов, первые – это отпечатки пальцев на устройствах периферии, элементах системного блока, вторые – на жестких дисках компьютеров, в истории браузеров, в истории точек восстановления системы, «кэше», cookie-файлы.

Виртуальные следы представляют собой зафиксированное в виде цифрового образа формальной модели изменение состояния информации в памяти абонентских электронных устройств (терминалов, биллинговых систем и т.п.), вызванное алгоритмом установленного программного обеспечения и связанное с событием преступления (имеющее уголовно-релевантное значение)[29].

Механизму подобного следообразования присущи следующие стадии:

28 Коржев М.А. Криминалистическое значение следов человека / М.А.Коржев // Инновационная наука. – 2015. – № 7-2. – С. 75.

29 Давыдов В.О. Методика расследования экстремистских преступлений, совершенных в компьютерных сетях: монография / В.О. Давыдов; под общ. ред. А.Ю. Головина. – М.: Юрлитинформ, 2014. – С. 46.

1) физическое проявление свойств следообразующих объектов (изображение, цифровой набор данных, температура, отсчеты времени, звук и др.);

2) преобразование исходной физической формы проявления следообразующего объекта в цифровую форму (аналогово-цифровое преобразование);

3) предварительная обработка, передача и хранение полученной цифровой информации[30].

Специфика следов в сфере компьютерной информации заключается в следующем: они не имеют геометрической формы, цвета, запаха и иных характеристик, традиционно рассматриваемых криминалистикой, в которых могли бы отразиться отельные черты преступника, например его ДНК, запах, папиллярный узор и тому подобное. Одни и те же электронно-цифровые следы-последствия могут быть образованы любым человеком, поэтому в механизме следообразования отсутствует непосредственный следовой контакт с преступником.

Исходя из вышесказанного, нельзя не отметить, что следы при расследовании преступлений в данной сфере имеют решающее значение, так как в большинстве случаев являются единственным источником информации и играют немаловажную роль при диагностике, позволяющей восстановить механизм совершения преступления.

1.7 Способ совершения преступления как основной элемент криминалистической характеристики преступлений в сфере компьютерной информации.

Способы подготовки, совершения и сокрытия преступления при их выделении в качестве самостоятельных элементов криминалистической

30 Давыдов В.О. Значение виртуальных следов в расследовании преступлений экстремистского характера / В.О. Давыдов, А.Ю. Головин // Известия Тульского государственного университета. Экономические и юридические науки, 2016. – № 3-2. – С. 255.

характеристики преступления помогают в отображении возможных вариантов преступного поведения лица, а также предметно представляют взаимоотражение каждого из видов способа друг на друге и на иных элементах криминалистической характеристики преступления.

В теории криминалистики способ преступления является интегральным понятием и охватывает большое количество отдельных криминалистически значимых признаков, не имеющих уголовно-правового значения, но играющих существенную роль в поисках следов преступления, в его раскрытии и установлении преступника.

Как элемент криминалистической характеристики способ указывает на предметно-операционную часть действия, где под действием понимается направление на достижение преступного результата, а в механизме заключается динамическая составляющая преступного события, получающая отражение в причинно-следственных и иных связях[31].

Г.Г. Зуйков отмечал, что способ совершения преступления представляет собой систему взаимосвязанных и взаимообусловленных действий по подготовке, совершению и сокрытию преступлений, детерминированных условиями внешней среды и свойствами личности, условиями места и времени и зачастую связанных с использованием соответствующих орудий и средств[32].

Существуют устоявшиеся подходы, согласно которым действия по сокрытию преступления в одном случае являются элементом способа совершения преступления, а в другом – находятся за его пределами. Так, В.П. Колмаковым в структуру способа совершения преступления включены действия, непосредственно направленные на совершение общественно

31 Князьков А.С. Криминалистическая характеристика преступления в контексте его способа и механизма / А.С. Князьков // Вестник Томского Государственного университета. Право. – 2011. – № 1. – С. 61.

32 Зуйков Г. Г. Поиск по признакам способов совершения преступлений: учебное пособие / Г.Г. Зуйков. – М.: НИиРИО ВШ МВД СССР, 1970. – С.16.

опасных деяний; действия же по сокрытию во всех случаях остаются за рамками способа совершения[33].

Сокрытие преступления через утаивание, уничтожение, маскировку или фальсификацию следов преступной деятельности, а также преступника направленно на воспрепятствование расследованию, однако оно не во всех случаях преследует цель уклонения от ответственности, порой субъект предпринимает действия по оттягиванию момента обнаружения следов преступления.

Следует отметить, что способ сокрытия преступления находит отражение в способе совершения, а нередко и в способе подготовки, в том случае, когда способ сокрытия заранее продумывается преступником и совпадает по своему характеру со способом подготовки.

Р.С. Белкин указывал на теоретическую значимость рассмотрения способа совершения преступления, как системы действий по подготовке, совершению и сокрытию преступления, предопределенных условиями внешней среды и психофизическими свойствами личности. Это понятие по своему содержанию отражает факт существования так называемого полноструктурного способа совершения преступления, когда он объединяет способы осуществления всех стадий преступного замысла[34].

Б.Н. Коврижных сделал предложение о возможности самостоятельного существования способа сокрытия, способа совершения и способа подготовки к преступлению, предложив рассматривать их в качестве составляющих способа преступления[35].

О.А. Крестовников определяет структуру способа совершения преступления в зависимости от конкретных обстоятельств. По его мнению, он может быть трехзвенной (включающей поведение субъекта до, во время и

33 Васильев А.Н. Проблемы методики расследования отдельных видов преступлений / А.Н. Васильев. – Москва: Изд-во МГУ. – 1978. – С. 27.

34 Курс криминалистики: В 3 т. Т. 3: Криминалистические средства, приемы и рекомендации / под общ. ред. Р.С. Белкина. – М.: Юристъ, 1997. – С.131.

35 Дудников А.Л. Криминалистическое понятие «способ преступления» / А.Л. Дудников // Проблемы законности. – 2012. – № 120. – С. 2.

после совершения преступления), двухзвенной (в различных комбинациях) и однозвенной (характеризовать поведение субъекта лишь во время самого преступного деяния)[36].

М.А. Атальянц, говоря о значении способа совершения преступления, указывает, что способ совершения преступления в отдельных случаях позволяет правильно определить объективную сторону того или иного преступления, наличие (или отсутствие) общественно опасного деяния, общественно опасные последствия и другие признаки состава[37].

На сегодняшний день в отечественной и зарубежной криминалистике не выведено определения, характеризующего способ совершения преступления в сфере компьютерной информации. Проблема нова для науки и находится в стадии теоретических разработок и осмысления. В то время как зарубежные ученые начали исследование данного вопроса с конца 70-х годов, отечественная криминалистическая наука обратилась всерьез к нему лишь с начала 90-х. Подобное двадцатилетнее отставание отечественной криминалистики от зарубежной по вопросу исследования компьютерных преступлений и способов их совершения, объясняется поздней информатизацией российского общества.

По нашему мнению, способ совершения преступления в сфере компьютерной информации – это совокупность приемов и методов, зависящих от уровня защищенности хранящейся информации на носителе и цели из-за которой происходит посягательство на данную информацию киберпреступниками для причинения вреда или угрозы причинения вреда общественным отношениям, находящимся в рамках киберпространства.

В первый частях статей 272–274 УК РФ не упоминается никаких способов совершения преступления, кроме как с «использованием

36 Крестовников О.А. Механизм и способ преступления в составе расследуемого события / О.А. Крестовников // Юридические записки. – 2013. – № 2. – С. 108.

37 Атальянц М.А. Значение способа совершения преступления для квалификации преступлений / М.А. Атальянц // Пробелы в российском законодательстве. – 2009. – № 4. – С. 221.

служебного положения», который является квалифицирующим признаком и содержится в отдельных частях данных статей (кроме 274 статьи УК РФ).

Так, в ч. 1 ст. 272 УК РФ объективная сторона преступления представлена в виде деяния, а именно «неправомерный доступ к охраняемой законом компьютерной информации» и общественно опасные последствия: «уничтожение, блокирование, модификация либо копирование компьютерной информации».

Примером копирования компьютерной информации может послужить уголовное дело, рассмотренное Ленинским районным судом г. Нижнего Новгорода по делу Борисовой Д.В., обвиняемой в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ.

Борисова Д.В., занимая должность менеджера, находясь в центре продаж и обслуживания ООО «***», обладая достаточными познаниями и имеющая практический опыт работы в глобальной информационно-коммуникационной сети, используя сотовый телефон, с помощью сетевой карты указанного устройства через Wi-Fi роутер осуществила выход в информационно-коммуникационную сеть через браузер Chrome, в котором, действуя умышленно, путем подбора реквизитов к доступу, а именно пароля и логина, осуществила неправомерный доступ к охраняемой законом компьютерной информации, расположенной и хранящейся на электронном почтовом ящике «***», находящемся в пользовании потерпевшего.

После чего, в продолжение своего преступного умысла Борисова Д.В., находясь по месту работы, войдя на электронный почтовый ящик «***» и получив возможность его пользования и администрирования, осуществила пересылку электронных почтовых писем с указанного почтового ящика на адрес электронного почтового ящика «***», находящегося в пользовании Борисовой Д.В., тем самым совершив копирование компьютерной информации[38].

38 Приговор Ленинского районного суда г. Нижний Новгород по делу Борисовой Д.В. от 11.06.2016 года по уголовному делу № 1-365/2016 // Справочная правовая система «Судпрактика». – Режим доступа: http://sud-praktika.ru.

В ч. 1 ст. 274 УК РФ также есть деяние «нарушение правил эксплуатации…, а также правил доступа к информационно-телекоммуникационным сетям» и последствия в виде «блокирования, модификации либо копирования компьютерной информации», причинивших крупный ущерб.

В качестве примера можно привести уголовное дело, рассмотренное Лефортовским районным судом г. Москвы по делу Анисимова А.В., обвиняемого в совершении преступления, предусмотренного ч. 1 ст. 274 УК РФ.

Анисимов А.В., имея умысел на нарушение правил эксплуатации средств хранения, передачи охраняемой компьютерной информации, повлекшее копирование компьютерной информации, находясь на своем рабочем месте, предоставленном ООО «Приват Трейд», используя средства авторизации (логин и пароль), предоставленные ООО «Приват Трейд» и имея в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, скопировал на USB-носитель информацию из базы данных ООО «Приват Трэйд», а именно: не менее 45 000 записей, содержащих не прошедших проверку имен, фамилий, никнеймов (имена, которые используется при регистрации на интернет сайтах), а так же адресов электронной почты. После чего Анисимов А.В. передал вышеуказанную информацию А.И.В.

Вышеуказанные действия Анисимова А.В. причинили ущерб ООО «Приват Трэйд» на общую сумму 1 155 600 рублей[39].

В ряде случаев блокирование выступает способом совершения преступлений, а не его последствиями: так, при установке специального программного обеспечения происходит блокировка доступа к защищенной информации, данный способ применяется уволенными сотрудниками, которые самостоятельно разрабатывают подобные вредоносные программы

39 Приговор Лефортовского районного суда г. Москвы по делу Анимисова А.В. от 13.01.2015 года по уголовному делу №1-6/2015 // Справочная правовая система «Судебные и нормативные акты РФ». – Режим доступа: http://sudact.ru.

или же заказывают их написание через интернет. Чаще всего в промышленном шпионаже преднамеренно используется способ блокирования работы средств защиты информации, а также происходит нарушение мер разграничения доступа или допуска к сведениям, данным или документам, отнесенным к коммерческой и иной тайне.

Блокирование может выступить и как последствие, вызвав недоступность информации, невозможность её использования и неспособность системы выполнять последовательность команд в том случае, когда при несанкционированном доступе, после выполнения набора действий, злоумышленник, достигая цели наиболее удобным для него способом, не думает о том, как скажется влияние вредоносной программы на системе после её использования.

То есть в одном случае, блокирование как способ целенаправленно преследует блокировку информационных данных, в другом блокирование как последствие представляет собой побочный эффект от использования запрещенных программ.

«Создание, распространение или использование компьютерных программ», перечисленные в ч. 1 ст. 273 УК РФ, должны определяться не как способы, а как альтернативные действия, так как способ всегда относится к какому-либо основному действию, отдельно от которого он существовать не может.

Полагаем, что российский уголовный закон нуждается в доработке и закреплении в нём способов совершения компьютерных преступлений, а не просто в перечислении последствий или условий доступа.

Судебно-следственная практика показала, что для совершения преступлений в сфере компьютерной информации преступники в большинстве случаев тщательно к ним готовятся[40]. Путем наведения справок, изучения режима работы на объекте, сбора данных о находящихся там

40 Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография / А.Л. Осипенко. – Омск: Омская академия МВД России, 2009. – С. 230.

средствах и технологиях. Наибольший интерес вызывают характеристики имеющихся программно-аппаратных средств, прежде всего, используемых средств технической защиты информации.

Подготовка нередко связана с изучением и приспособлением к выявленной обстановке. С этой целью в обстановку могут вноситься изменения, например, путем внедрения в операционную систему компьютера, принадлежащего жертве, вредоносной программы. Назначение таких программ заключается в снижении защиты компьютера и открытии возможности осуществления неправомерного удаленного доступа к нему по информационной сети.

Подводя итоги, можно отметить следующее:

Во-первых, понятие и элементы состава криминалистической характеристики киберпреступлений имеют согласованность с общим представлением о данной криминалистической категории. Однако отечественный понятийно-терминологический аппарат, используемый в сфере компьютерной информации, нуждается в совершенствовании.

Во-вторых, возникла насущная потребность в формулировании общепринятого определения, характеризующего способ совершения преступлений в сфере компьютерной информации.

2 Классификация способов совершения преступлений в сфере компьютерной информации

Преступления в сфере компьютерной информации охватываются статьями 272-274 УК РФ.

Попытки законодателя привести нормы главы 28 УК РФ в соответствие со сложившейся практикой не соответствуют современным тенденциям в области компьютерных технологий, при использовании в дефиниции статей некоторых технических терминов присутствует двойственность толкования.

В примечании 1 статьи 272 УК РФ под компьютерной информацией понимается информация, которая передается в форме электрических сигналов. Однако помимо эклектических сигналов существуют и другие способы передачи информации, такие, как электромагнитные сигналы, передающиеся посредством wi-fi, оптоволокно, где информация проходит в виде световых сигналов. Исходя из уголовно-правовой дефиниции, получается, что использование вышеназванных способов передачи компьютерной информации не охватывается правовым регулированием.

По мнению И.А. Кирсанова, другим проблемным вопросом является формулировка диспозиции ч. 1 ст. 272 УК РФ, подразумевающая наступление уголовной ответственности лишь в случае, если действия потенциального преступника привели к уничтожению, блокированию, модификации либо копированию компьютерной информации. Это означает, что сам по себе доступ к закрытой компьютерной информации не является преступлением[41].

Таким образом, лицо, путем взлома системы защиты любого устройства, ознакамливается с содержащимися там данными и остается безнаказанным. Применение же статьи 137 УК РФ, согласно которой

41 Кирсанов И. А. Компьютерное уголовное право: проблемы и пути решения / И.А. Кирсанов // Альманах современной науки и образования. – 2012. – № 6. – С. 72.

запрещается незаконный сбор информации, составляющей личную или семейную тайну, оправдано не во всех случаях.

Способы совершения преступлений в сфере компьютерной информации являются очень специфическими, часто не подпадающими под общепринятое традиционное понимание способа совершения преступления. Практическими работниками в настоящее время выделяется свыше 20 основных способов совершения преступлений в сфере компьютерной информации и около 40 их разновидностей.

Способы совершения преступлений в рассматриваемой сфере можно разделить на несколько больших групп, исходя из тех объектов, на которые направлены преступные посягательства:

• экономические преступления – самые распространенные, совершаемые по корыстным мотивам и включающие в себя компьютерное мошенничество, кражу компьютерных программ, различных видов услуг, предоставляемых посредством онлайн-контента, и экономический шпионаж;

• компьютерные преступления против личных прав и частной жизни – сбор данных о лице, разглашение закрытой информации, получение информации о расходах;

• преступления, посягающие на государственные и общественные интересы – эти преступления направлены против государственной и общественной безопасности, угрожающие обороноспособности государства.

Освоение и применение новейшего компьютерного оборудования, оснащенного последним программным обеспечением, дает возможность человеку находить обходные пути для совершения преступлений в сфере компьютерной информации. В течение нескольких последних лет отчетливо прослеживается тенденция развития способов совершения указанных преступлений путем обращения к сетевым технологиям, базирующимся на удаленном доступе пользователей к информационным базам данных.

2.1 Способы непосредственного доступа к компьютерной информации.

Н.М. Радько понимает под непосредственным доступом в оперативную систему компьютера доступ, осуществленный посредством преодоления парольной защиты на вход в систему, т.е. проникновение через воздействие на подсистему аутентификации данных пользователя, куда включает:

1) непосредственный доступ в оперативную систему компьютера посредством подбора паролей на вход;

2) непосредственный доступ в оперативную систему компьютера посредством сброса паролей на вход[42].

О.И. Семыкина полагает, что непосредственный доступ к компьютерной информации происходит через использование активных способов, связанных с непосредственным воздействием субъекта на компьютерную технику (в частности, когда виновный самостоятельно осуществляет взаимодействие с ЭВМ, системой ЭВМ или их сетью, загружая вредоносную программу и используя ее, а потерпевший либо не знает о самом факте внедрения вредоносной программы, либо не осознает ее вредоносный характер)[43].

Непосредственный доступ так же именуется «прямым», он осуществляется как лицами, работающими с информацией, так и теми, кто целенаправленно вторгается в закрытые зоны и помещения, где происходит обработка информации. Например, лицо, имеющее прямой умысел на незаконный доступ к компьютерной информации, держа при себе флеш-карту, либо определенные документы, которые указывают на то, что его можно отнести к типу людей, работающих на компьютере, прохаживается около запертой двери помещения, где в данный момент находится серверная. Дождавшись, когда в данное помещение войдет работающий в нем

42 Радько Н.М. Угрозы непосредственного доступа в операционную среду компьютера / Н.М. Радько // Информация и безопасность. – 2007. – № 2. – С. 317.

43 Семыкина О.И. Противодействие киберпреступности за рубежом / О.И. Семыкина // Журнал зарубежного законодательства и сравнительного правоведения. – 2016. – № 6. – С. 107.

сотрудник, он входит следом, через определенный промежуток времени при сопутствующей обстановке совершает неправомерный доступ к компьютерной информации.

Практика показывает, что преступники компьютерную информацию чаще перехватывают при ее передаче по телекоммуникационным каналам и компьютерным сетям. Сделать это им и проще, и безопаснее, чем при непосредственном проникновении в помещение.

Иным способом непосредственного доступа к компьютерной информации является неправомочное использование преступником технических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Он осуществляется в двух формах: физической и электронной.

Физическим поиском «отходов» является обследование рабочих мест программистов, содержимого мусорных баков, емкостей для технологических «отходов» для сбора оставленных или выброшенных физических носителей информации, а также обследование различной документации, оставленной на рабочем месте: записных книг, рабочих записей на листах бумаги, календарях и так далее, в целях поиска черновых записей, паролей доступа в систему и прочего.

Электронный вариант требует просмотра и последующего исследования данных, находящихся в памяти компьютера. Он основан на некоторых технологических особенностях функционирования средств компьютерной техники. Например, данные, записанные в последний момент работы, не всегда стираются из оперативной памяти компьютерной системы.

В названных целях могут просматриваться и восстанавливаться стертые файлы. В данном случае предполагается обязательное использование в качестве орудия преступления различных программных средств специального назначения. Одним из них является программный комплекс PCToolsDeluxe, содержащий универсальную программу восстановления

стертых файлов[44]. Подобные программы не требуют особых затрат, они легкодоступны и находятся в открытом доступе, их базовая составляющая всегда бесплатна, за отдельную плату добавляются функции, раскрывающие программу в полном объеме и увеличивающую скорость обработки и поиска восстанавливаемых данных.

Для доступа к личной информации преступники нередко прибегают ко взлому паролей, являющихся защитой в социальных сетях, в онлайн-играх, либо в программах, осуществляющих хранение конфиденциальной информации. Наиболее распространенными способами взлома паролей являются:

a) метод оптимизированного и неоптимизированного перебора;

b) подглядывание через плечо;

c) «метод пауков».

d) «выведывание» у пользователя

Относительно «выведывания» пароля у пользователя примером может послужить приговор Калининского районного суда г. Чебоксары Чувашской Республики от 13 декабря 2007 года по уголовному делу №1-785-97. 11.02.2007 года К., находясь у себя дома, используя городскую телефонную сеть с абонентским номером «***», персональный компьютер, имеющий доступ выхода к сети Интернет через DiaI-UPмодем, а также коммуникационный сервер филиала в Чувашской Республике ОАО «Б.» с IP-адресом «***», обладая специальными познаниями в информационных технологий, обманным путем получил от П. ответ на «контрольный вопрос», предназначенный для доступа на электронный почтовый ящик, после чего осуществил неправомерный доступ к охраняемой законом компьютерной информации, хранящейся на электронном почтовом ящике П. После незаконных действий, произведенных на почтовом сервере, К., находясь у себя в квартире, модифицировал (изменил) пароль на доступ в почтовый

44 Способы совершения преступлений в сфере компьютерной информации [Электронный ресурс] // Режим доступа: http://bestreferat.su/Gosudarstvo-i-pravo/Sposoby-sovershenija-prestuplenija-v-sfere-kompjuternoj-informacii/

ящик П., тем самым блокировал последнему доступ к хранящейся там информации. Затем без получения согласия потерпевшего, К. скопировал на свой компьютер хранящуюся в электронном почтовом ящике потерпевшего информацию личного характера и ознакомился с ней, а именно с двумя электронными письмами, составленными П., и состоянием его счета на электронном кошельке[45].

Оптимизированный и неоптимизированные методы перебора паролей существуют в ниже представленных вариациях:

1) неоптимизированный перебор. В этом случае злоумышленник последовательно опробует все возможные варианты пароля. Для паролей длиннее шести символов во многих случаях данный метод может быть признан неэффективным;

2) перебор, оптимизированный по статистике встречаемости символов и биграмм. Разные символы встречаются в паролях пользователей с разной вероятностью. При практическом применении данного метода злоумышленник вначале опробует пароли, состоящие из наиболее часто встречающих символов, за счет чего время перебора существенно сокращается. Для подбора паролей по данному методу злоумышленник может использовать множество программ, в основном ориентированных на взлом операционной системы. При этом можно выделить две базовые технологии: явное опробование последовательно генерируемых паролей с их подачей на вход подсистемы аутентификации и расчет значения хэш-функции и ее последующего сравнения с известным образом пароля;

3) перебор, оптимизированный с использованием словарей вероятных паролей. При использовании данного метода подбора паролей злоумышленник вначале опробует в качестве пароля все слова из словаря, содержащего наиболее вероятные пароли. Если подбираемый пароль отсутствует в словаре, злоумышленник может опробовать всевозможные комбинации слов из словаря, слова из словаря с добавленными к началу или

45 Уголовное дело № 1-785-97 // Архив Калининского районного суда г. Чебоксары. 2007 год.

к концу одной или несколькими буквами, цифрами и знаками препинания и т.д.;

4) перебор, оптимизированный с использованием знаний о пользователе. В этом случае в первую очередь злоумышленник пробует пароли, использование которых сотрудником представляется наиболее вероятным (имя, фамилия, дата рождения, номер телефона и т. д.);

5) перебор, оптимизированный с использованием знаний о подсистеме аутентификации операционной системы. Если ключевая система допускает существование эквивалентных паролей, при переборе из каждого класса эквивалентности опробуется всего один пароль[46].

«Подглядывание через плечо»: самоуверенные взломщики под видом технического обслуживающего персонала, рассыльного или любых других служащих проникают в офисы. Будучи одетыми в форменную одежду обслуживающего персонала она предоставляет своего рода пропуск на беспрепятственный доступ во все уголки офисного здания. Это позволяет «шпионам» записывать пароли, вводимые реальными сотрудниками, а также предоставляет отличную возможность увидеть все те пароли, которые многие так любят писать на стикеры и клеить прямо на мониторы своих компьютеров.

«Метод пауков»: большинство корпоративных паролей состоит из слов, связанных с бизнесом. Изучение корпоративной литературы, материалов веб-сайтов, сайтов конкурентов и даже список клиентов – основа для построения пользовательского списка слов, который затем используется для взлома. Действительно опытные хакеры автоматизировали процесс и запускают «паутинные» приложения, аналогичные тем, которые применяются ведущими поисковыми системами, чтобы определить ключевые слова, собрать и обработать списки для взлома[47].

46 Утребов Д.Р. Классификация угроз в системах управления базами данных / Д.Р. Утребов, С.В. Белов // Вестник Астраханского Государственного технического университета. – 2008. – № 1. – С. 89.

47 Топ-10 методов взломов паролей [Электронный ресурс] // Режим доступа: http://www.pcidss.ru /articles/39.html

При непосредственном доступе преступник всегда пытается уничтожить следы путем стирания отпечатков пальцев, уничтожением следов работы в компьютере: удаление истории посещения web-страниц, загрузки файлов, выполнения скриптов, буфер обмена, cookie.

2.2 Способы опосредованного доступа к компьютерной информации.

При реализации способов опосредованного (удаленного) доступа неправомерный доступ к определенному компьютеру и находящейся на нем информации осуществляется с другого компьютера, находящегося на расстоянии, через компьютерные сети[48].

Н.Г. Шурухнов определяет опосредованный способ доступа как отдачу команд с другого компьютера (через компьютерные сети), находящегося на определенном расстоянии, они в свою очередь подразделяются на две подгруппы: способы преодоления парольной, а также иной программной или технической защиты и последующего подключения к компьютерной системе; способы перехвата информации[49].

К способам опосредованного (удаленного) доступа к компьютерной информации можно отнести:

1. Подключение к телекоммуникационным кабелям авторизованного пользователя (т.е. телефонной линии) и получение доступа к его компьютерной информации, который в свою очередь делится на активный и пассивный перехват.

Примером перехвата информации через телекоммуникационные каналы является случай, рассмотренный Лесосибирским городским судом Красноярского края по уголовному делу № 15003100. Д., используя сетевой кабель и коннектор, самовольно подключил свой персональный компьютер к

48 Новик В.В. Криминалистические аспекты доказывания по уголовным делам / В.В. Новик. – М.: Litres, 2017. – С. 96.
49 Шурухнов В.В. Криминалистика: учебное пособие / В.В. Шурухнов. – М.: Изд-во Московского психолого-социального ун-та (МПСУ), 2011. – С. 187.

коммутатору сети передачи данных ООО «****», расположенному на чердачном помещении дома. После чего Д., располагая IP-адресами ООО «****», полученными им во время работы в данном обществе, без разрешения ООО «****», осознавая противоправность своих действий, неоднократно, незаконно выходил в сеть передачи данных ООО «****», не осуществляя соответствующей оплаты за подключение и за услуги использования данной сети, при этом блокируя работу ЭВМ законных пользователей сети передачи данных ООО «****»[50] (см. приложение А).

Такой способ неправомерного доступа имеет широкое распространение и шансы на вычисление гражданина, совершившего данное противоправное деяние, довольно высоки.

Непосредственный (активный) перехват. Осуществляется с помощью непосредственного подключения к телекоммуникационному оборудованию компьютера, компьютерной системы или сети, например, линии принтера или телефонному проводу канала связи, используемого для передачи данных, и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера. В связи с этим различают:

а) форсированный перехват, представляющий собой перехват сообщений, направляемых рабочим станциям (ЭВМ), имеющим неполадки в оборудовании или каналах связи;

б) перехват символов – выделение из текста, набираемого пользователем на клавиатуре, терминала, знаков, не предусмотренных стандартным кодом данной ЭВМ;

в) перехват сообщений – несанкционированное подключение специального терминала к линии связи, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ[51].

50 Уголовное дело № 15003100 // Архив Лесосибирского городского суда Красноярского края. 2007 год.

51 Казанцев С.Я. Информатика и математика для юристов: учебник / С.Я. Казанцев; под ред. С.Я. Казанцева, Н.М. Дубининой. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2010. – С. 490.

2. Путем проникновения через телефонную линию с помощью автоматизированного набора телефонного номера из определенного списка абонентов, с последующим подключением к его компьютеру.

Необходимо отметить, что такая попытка несанкционированного доступа может быть легко обнаружена. Органы предварительного расследования при поиске, как правило, исходят из данных, полученных от фирмы-провайдера, в первую очередь касающихся телефонного номера, с которого осуществлялся неправомерный доступ при использовании модемного соединения. Анализ ряда уголовных дел показал, что доказывание совершения проникновения строится на базе главного доказательства – телефонного номера, с которого происходило соединение с сервером провайдера.

Представляется, что подобное обстоятельство нельзя рассматривать в качестве универсального доказательства, поскольку к телефонным кабелям нередко имеется открытый доступ, распространены технические сбои на автоматической телефонной станции (АТС), а также возможно соучастие работников АТС в совершении неправомерного доступа. Все это создает благоприятные условия для использования преступниками подобных уязвимостей. Так, с помощью ноутбука можно подсоединиться к линии телефонной сети в многоквартирном доме, и тем самым осуществить выход в сеть Интернет с чужого телефонного номера, в том числе, воспользовавшись картой доступа в Интернет[52].

Подобный способ «взлома» нередко осуществляется с нескольких рабочих мест: в указанное время несколько (более 10) персональных компьютеров выполняют попытку несанкционированного доступа. Система безопасности может предотвратить несколько «атак», в свою очередь, пока система занята блокировкой, например, шести атак, оставшиеся четыре,

52 Поляков В.В. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации / В.В. Поляков, С.М. Слободян // Известия Томского политехнического университета. – 2007. – № 1. – С. 213.

оставшись незамеченными, получают незаконный доступ к компьютерной информации. Они постепенно начинают осуществлять поставленную перед собой задачу, при этом выполняя сложные операции для сокрытия преступления.

Примером может послужить приговор от 29.08.2011 года по уголовному делу № 1-304/11, рассмотренному Новотроицким городским судом Оренбургской области по делу Малькова А.Ю., обвиняемого в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ.

Мальков А.Ю. с целью облегчения неправомерного доступа к сети Интернет, находясь в квартире «***», действуя умышленно, при помощи персонального компьютера и ADSL-модема, принадлежащих «***», подключенных на ее имя к сети Интернет с абонентского номера №… (вызывающая станция), осуществляя доступ в сеть Интернет через Интернет-провайдера ОАО «***», просканировал IP-адреса 20-ти компьютеров, определил наличие работающих в сети ADSL-модемов.

Преодолев защиту, Мальков А.Ю. проник в настройки ADSL-модемов абонентов ОАО «***» и без согласия 20-ти легальных пользователей неправомерно получил доступ к охраняемой конфиденциальной информации, которую скопировал. Таким образом, Мальков А.Ю., осуществив неправомерный доступ к охраняемой законом компьютерной информации, получал за счет легальных пользователей провайдера «ОАО «***» доступ в сеть Интернет, что повлекло несанкционированное блокирование и нарушение работы системы ЭВМ или их сети, а также копирование и модификацию информации, что выражается в искажении учётно-статистических данных о пользователе, времени начала и продолжительности его работы, количестве соединений, поступающих на сервер статистики Оренбургского филиала ОАО «***»[53].

3. Проникновение с помощью паролей.

53 Приговор Новотроицкого городского суда Оренбургской области от 29.08.2011 года по уголовному делу № 1-304/11 // Справочная правовая система «РосПравосудие». – Режим доступа: https://rospravosudie.com.

С помощью этого метода нарушитель взламывает пароль для доступа к компьютерной информации. Для этих целей преступники разработали целый ряд специального программного обеспечения. Оно, как правило, приобретается на «теневом рынке» компьютерного обеспечения. Завладев паролем, незаконный пользователь получает доступ к компьютерной информации, выполняя любые операции с информацией, хранящейся на носителе: копирование, удаление, изменение или подмена данных, осуществление денежных переводов, подделку платежных поручений, регистрацию на сайтах от имени авторизованного пользователя и тому подобное.

Методы прямого и электромагнитного перехвата также относятся к методам опосредованного (удаленного) доступа к компьютерной информации.

Прямой перехват – самый простой способ доступа, он осуществляется через внешние каналы связи или путем прямого подключения к кабелям периферийных устройств.

В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения (ПЭМИ), возникающие при работе технических средств, а именно:

1) побочные электромагнитные излучения, возникающие вследствие протекания по элементам технических средств приема, обработки, хранения и передачи информации (далее – ТСПИ) и их соединительным линиям переменного электрического тока;

2) побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСПИ;

3) побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

- вывод информации на экран монитора;

- ввод данных с клавиатуры;

- запись информации на накопители на магнитных носителях;

- чтение информации с накопителей на магнитных носителях;

- передача данных в каналы связи;

- вывод данных на периферийные печатные устройства – принтеры, плоттеры;

- запись данных от сканера на магнитный носитель (ОЗУ).

Абсолютно все электронные устройства сопровождаются электромагнитным излучением, что является результатом нежелательных помех, возникающих в различных электронных приемных устройствах. Для перехвата побочных электромагнитных излучений ТСПИ могут использоваться как обычные средства радио-, радиотехнической разведки, так и специальные средства разведки, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН)[54].

4. Самым популярным способом совершения компьютерных преступлений на данный момент является доступ к социальным сетям, где количество активных пользователей в месяц (данные 2016 года) составляет от сотен миллионов до миллиарда человек: «Facebook», «Youtube», «Rambler», «Instagram», «Twitter», «VKontakte». Путем похищения страницы пользователя и «внедрения» на его страничку предполагаемых друзей, преступники заманивают его ничего не подозревающих друзей на сайты интернет-магазинов, специализирующихся на обмане клиентов[55].

5. Через сервис удаленного доступа Microsoft Windows у обычного пользователя или администратора есть возможность управления компьютером или сетью дистанционно, находясь в другом месте, городе, стране. Этот способ обеспечивает злоумышленнику получение полного

54 Хорев А.А. Технические каналы утечки информации, обрабатываемой техническими средствами / А.А. Хорев //Специальная техника. – 2004. – № 2. – С.3-4.

55 Рогозин В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий / В. Ю. Рогозин // Расследование преступлений: проблемы и пути их решения. – 2015. – № 6. – С. 10.

доступа к управлению компьютером, если же происходит подключение к компьютеру администратора, то доступ открывается ко всем компьютерам составляющим данную сеть. Программа автоматического подбора пароля позволяет с легкостью получить доступ к компьютеру, при условии, что система не имеет дополнительных средств защиты и отсутствует шифрование удаленного доступа, например, по физиологическим характеристикам: по отпечатку пальца, голосу, по рисунку сетчатки глаза.

Также путем использования программного обеспечения, предназначенного для удаленного администрирования, у пользователя данной программы есть возможность осуществлять операции с файлами на компьютере другого пользователя, путем подключения к его операционной системе.

Примером может послужить справка о компьютерно-техническом исследовании по уголовному делу № 24130500. На исследование представлено: накопитель на жёстких магниитных дисках (далее НМЖД) модели ST*** серийный номер S***. Выводы, сделанные экспертом на основе поставленных перед ним вопросов, следующие:

1) Имеется ли на представленном носителе информации программное обеспечение TeamViewer, предназначенное для удаленного администрирования? Если да то какова дата его установки, какой используется ID-номер? В каталоге «g:\ProgramFiles (x86)\TeamViewer» обнаружена удаленная программа TeamViewer, предназанченная для дистанционного администрирования, дата установки 24.02.2014, ID-номер 7*****

2) Имеется ли информация о том, когда и с каких IP-адресов или ID-номеров осуществлялось подключение к операционной системе, установленной на НЖМД? В файле «Connections_incoming.txt» содержится информация о том, что 24.11.2015 в период с 23:15 по 23:17 осуществлялось удаленное администрирование операционной системы, установленной на исследуемом НЖМД, посредством программы TeamViewer, пользователем

имеющим ID-номер 4*****, которого имя компьютера или имя пользователя записано как «К1***»

3) Имеется ли информация о логине «К1***», в какой программе, для чего используется? Логин «К1***» использовался при установке программы TeamViewer, а также пользователь с таким логином или именем компьютера осуществлял удаленное управление 24.11.2015 в период с 23:15 по 23:17 посредством данной программы.

4) Имеется ли на НЖМД информация о единвременном удалении большого количества файлов, содержащих фото-избражения, документы, видео-записи? На логическом диске F, предположительно, было осуществлено форматирование диска, при котором все находящиеся ранее на нем файлы были удалены. Также в личных каталогах пользователя «S***» удалены папки «Л***» и директории, в которых содержались аудио-записи, предположительно, созданные при записи телефоном с функцией диктофона[56] (см. приложение Б).

Как видно из вышеприведенного заключения, даже если преступником используется программное обеспечение для удаленного администрирования, у экспертных органов имеются возможности установления того, когда и с каких IP-адресов или ID-номеров осуществлялось подключение к операционной системе, установленной на НЖМД, даже если данное программное обеспечение удалено.

6. Дефейс – от английского deface – уродовать, искажать, коверкать. Представляет собой тип атаки, при котором преступник изменяет внешний вид сайта, в частности заглавной страницы, на которую заходит потерпевший с определенной систематичностью, вводя обычно пароль и логин для в хода в личный кабинет, что и становится желаемым результатом для преступника. В данном случае отличия от оригинальной страницы веб-сайта минимальны. На практике это осуществляется путём получения доступа на запись к директории, где хранятся данные веб-сервера.

56 Уголовное дело № 24130500 // Архив Красноярского краевого суда. 2015 год.

Встречаются единичные случаи дефейса вузовских сайтов, использующих уязвимое программное обеспечение[57].

7. Вредоносные программы. Большинство современных вредоносных программ создаются с целью извлечения выгоды.

Существует довольно много их разновидностей, в зависимости от предназначения:

1) троянские программы, предназначенные для создания зомби-сетей, используемых для рассылки спама, DoS-атак, организации фишерских сайтов.

Большинство пользователей при пользовании интернетом, недооценивают защиту своего компьютера до тех пор, пока не происходит кража конфиденциальной информации или не пропадают деньги с банковских счетов. Чаще всего в подобных нарушениях защиты используется так называемый botnet, его еще называют зомби-сетью или ботнетом. Botnet – это сеть компьютеров, зараженных вредоносной программой – ботом с дефектом алгоритма, который встраивается разработчиком. Данная программа позволяет получить доступ к данным компьютера с помощью удаленного доступа[58].

Также используются так называемые боты (Bot) для получения информации о балансе пользователя на его лицевом счете. Так, предметом исследования эксперта по уголовному делу № 23001500 являлся оптический носитель с файлом «install.apk». Были поставлены вопросы и получены в ходе компьютерно-технического исследования следующие ответы:

а. Имеется ли на представленном носителе вредоносное программное обеспечение? На указанном носителе представлено вредоносное программное обеспечение типа «Android.SmsBot.391.origin»,

57 Брумштейн Ю.М. Информационная безопасность сайтов высших учебных заведений: проблемы и решения / Ю. М. Брумштейн // Информационная безопасность регионов. – 2014. – № 1(14). – С. 39.
58 Алиева М.Ф. Botnet или Зомби-сети / М.Ф. Алиева, Т.Г. Чучминова // Наука. Образование. Молодежь. – 2016. – № 1. – С. 321.

предназначенное для несанкционированного блокирования и модификации компьютерной информации.

b. Каков механизм работы указанного вредоносного программного обеспечения? После установки на смартфоне под управлением операционной системы Android оно отправляет СМС-сообщения для получения информации о балансе пользователя на лицевом счете оператора связи, электронном кошельке платежной системы Qiwi, банковском счете Сбербанка, и отправляет указанные данные и данные о телефоне на удаленный сервер, после чего получает дальнейшие команды о переводе денежных средств путем отправки СМС-сообщений.

c. Имеются ли сведения об IP-адресах или Интернет-сайтах с которых происходит управление вредоносным программным обеспечением? Управление вредоносным программным обеспечением осуществляется посредством сайта «d***.com» (IP-адрес ****)[59] (см. приложение В).

Данное вредоносное программное обеспечение уникально. В зависимости от количества личных кабинетов, к которым привязан телефонный номер, на который отрпавляется СМС-сообщение, оно устанавливает личные кабинеты, где могут существовать лицевые счета пользователя с определенной суммой денег. Чем больше подобных личных кабинетов привязано к одному номеру, тем больше уязвим пользователь для подобного рода вредоносных программам.

1) Spyware (программа-шпион) – черви и троянцы, осуществляющие сбор информации о привычках пользования интернетом и наиболее часто посещаемых сайтах, осуществляет функцию запоминания нажатия клавиш и screen (копию) экрана компьютера, способны удаленно управлять компьютером, автоматически запускать инсталляцию программ, анализировать уязвимости, сканировать порты и взламывать пароли. В частности функция запоминания нажатия клавиш носит название keylogger (англ. key – клавиша и logger – регистрирующее устройство), может

59 Уголовное дело № 23001500 // Архив Кировского районного суда г. Красноярска. 2015 год.

выглядеть как приспособление миниатюрного размера, прикрепляемое между клавиатурой и компьютером или быть встроено в саму клавиатуру. Последней из нашумевших эпидемий червя, а котором был встроен keylogger является «Mydoom»[60].

2) Adware – несанкционированная реклама, проникающая на персональный компьютер. Порой к adware относятся не только вредоносные программы, но и те, которые отображаются с разрешения пользователя.

3) Rootkit (англ. Root – корень и kit – комплект) – программа, позволяющая сокрыть следы присутствия злоумышленника или «вредителя» во взломанной системе, путем закрепления и сокрытия файлов, процессов. Особенностью руткита является возможно действовать как keylogger, считывать и сохранять пароли, дистанционно запускать бота для осуществления DoS-атак, а также контролировать работу антивируса путем его отключения.

Руткиты написаны таким образом, чтобы избегать обнаружения антивирусными средствами и другими средствами безопасности, поэтому основной проблемой в борьбе с ними является их обнаружение и уничтожение. Существуют утилиты, специально созданные для поиска известных и неизвестных руткитов разными узкоспециальными методами, а также с помощью сигнатурного и поведенческого анализа[61].

4) Логические бомбы – при выполнении (невыполнении) определенных условий или в заданное время на компьютере автоматически уничтожается вся важная информация. Примером может послужить завод «АвтоВАЗ», на котором в 1982 году впервые в СССР была использована логическая бомба в компьютерной программе, остановившая сборочный конвейер. 26.04.1999 года вирус «CNI» активизировался в годовщину Чернобыльской аварии, он был написан тайваньским студентом и

60 Дедюрина О.В. Назначение программ-шпионов и методы противодействия им / О.В. Дедюрина, Т.Г. Долгова // Актуальные проблемы авиации и космонавтики. – 2014. – № 10. – С. 363.

61 Гонохова Д.Ю. Руткиты / Д. Ю. Гонохова // Перспективы развития науки и образования: сборник научных трудов по материалам XI международной научно-практической конференции, г. Москва, (30 ноября 2016г.); под общ. ред. А.В. Туголукова. – М., 2016. – С. 65.

представлял собой резидентный вирус, работающий только на операционных системах Windows 95\98\ME[62].

5) Ransomware – программы-вымогатели, шифрующие файлы после проникновения в компьютер жертвы, после чего предъявляют требования об уплате выкупа за возможность восстановления файлов пользователя.

Вирус отправляет запрос на сервер преступника. Происходит генерация уникального ключа, с помощью которого все файлы на компьютере жертвы шифруются. Ключ отсылается на сервер и хранится там. Вирус показывает пользователю окошко (либо меняет рабочий стол) с предупреждением и требованием выкупа. За расшифровку файлов потребуют определенное количество биткоинов (криптовалюта, используемая в интернете). При этом зашифрованные файлы невозможно открыть, сохранить, отредактировать, поскольку они наглухо зашифрованы стойким алгоритмом. При этом есть некоторые нюансы. Некоторые шифровальщики вообще выбрасывают ключ, а потому, заплатив выкуп, пользователь все равно не расшифрует свои фото, видео и другие файлы[63].

Самый последний случай применения ransomware-программы – это запуск во всемирную сеть 12 мая 2017 года компьютерного вируса-шифровальщика WannaCry, которым были заражены десятки тысяч компьютеров под управлением различных версий Windows. Вирус шифровал пользовательские файлы – документы и фото и т.д. (все пользовательские файлы приобретали одно расширение WNCRY и не открывались в программах). На экране пользователя появлялось красное окно приложения, в котором была надпись о том, что файлы зашифрованы и для их расшифровки необходимо заплатить 300 долларов через Биткоин.

Способ внедрения WannaCry очень прост: на зараженном компьютере запускается сканер портов, который ищет компьютеры с открытым TCP-портом 445 (порт протокола SMB). Когда такой компьютер найден, вирус

62 Холмогоров В. PRO Вирусы / В. Холмогоров. – М: Страта, 2015. – С. 42.
63 Бондаренко Е.С. Эволюция вирусов-шифровальщиков / Е.С. Бондаренко // Контентус. – 2016. – № 8(49). – С. 144.

подключается к нему, через этот порт посылает туда специальный пакет данных, который вызывает ошибку в работе Windows. В результате такой ошибки на этом компьютере можно выполнить зловредный код (загрузку и запуск вируса). Дальше запущенный вирус шифрует файлы на этом компьютере. А также ищет новые компьютеры для заражения[64].

Примером атаки вируса-шифровальщика может послужить случай, расследованный по уголовному делу № 23042100. На компьютерно-техническое исследование был представлен компакт-диск DVD+RSony 1130531+ REC2656. Выводы, сделанные экспертом на основе поставленных перед ним вопросов, следующие:

1) Имеется ли на представленном носителе информации вредоносное программное обеспечение, заведомо предназначенное для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации?

На компакт-диске файл «Акт_сверки.docx.rar» содержится вредоносное программное обеспечение, которое определяется антивирусными онлайн-сервисами и антивирусными программами как «Trojan-Ransom.Win32.Crypmod.wjl», которое по алгоритму и результату своей работы, заведомо предназначено для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации

2) Каков механизм действия указанной программы?

Исполняемый файл «Акт_сверки.docx.exe» работает по следующему алгоритму:

a. распространяется посредством электронных писем, в которых содержится ссылка на копирование исполняемого файла с удаленного сервера, находящегося под контролем злоумышленника;

64 Вирус WannaCry [Электронный ресурс]. – Режим доступа: http://ru.d-ws.biz/articles/viruses-wana-decryptor.shtml.

b. запускается по клику пользователя, необходимому для открытия файла;

c. несанкционированно и виузально не определяемо, загружает дополнительные модули необходимые для работы криптографических программ;

d. запускает криптографические программы со сформированным ключем для шифрования;

e. модифицирует криптографическим алгоритмом все электронные документы, фото- и видео-файлы, файлы архивов, файлы баз данных, файлы электронных подписей, при это изменяя их название, добавляя уникальный идентификатор и адрес электронной почты злоумышленника, чем блокирует доступ к информации содердащейся в указанных файлах;

f. отправляет ключ шифрования на командный сервер или адрес электронной почты злоумышленника;

g. удаляет свои исполняемые и служебные файлы, для затруднения идентификации и расшифровки файлов.

3) Возможно ли восстановить доступ для чтения и редактирования содержимого зашифрованных файлов в оригинальном виде, содержащихся на компакт-диске?

Доступ к информации, содержащейся в зашифрованных файлах, возможен только при правильной дешифровке исходным алгоритмом криптования и при использовании исходного ключа, который известен только злоумышленнику. Расшифровка антивирусными компаниями или самим владельцем информации без знания данного ключа путем поочередного подбора символов невозможна[65] (см. приложение Г).

Исходя из ответов эксперта, следователем было установлено, на что направлен такой вирус-шифровальщик, механизм его действия и возможность после его применения получить доступ к файлам.

65 Уголовное дело № 23042100 // Архив Красноярского краевого суда. 2015 год.

Доступ к информации, содержащейся в зашифрованных файлах, действительно не прост, по сути, без установления личности злоумышленника и получения от него исходного ключа получение такого доступа невозможно.

Вирусные вредоносные программы XXI века являются средством и элементом криминального бизнеса, а люди, прописывающие системные коды для них, действуют по заказу и в подавляющем большинстве случаев из корыстных побуждений. Заказ может быть как прямым, когда программисту поручается задание, после исполнения которого результат передается заказчику, так и непрямым, когда создатель вредоносных программ удовлетворяет потребности чёрного рынка своим «продуктом», путём его самостоятельной реализации.

2.3 Способы совершения преступлений в сфере компьютерной информации с использованием вредоносных программ.

Диспозиция ч. 1 ст. 273 УК РФ содержит в себе альтернативные действия (способы), предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации посредством компьютерной программы или иной компьютерной информации:

a) создание;

b) распространение;

c) использование.

Компьютерная программа или иная компьютерная информация в данном случае всегда будет являться вредоносной, однако определение понятия «вредоносная компьютерная программа» является одним из сложных и противоречивых вопросов, порождающих дискуссии ученых в области уголовного права и криминалистики.

Нужно отметить, что законодатель, дав определение компьютерной информации в примечании ст. 272 УК РФ, не посчитал необходимым аналогично закрепить в примечании ст. 273 УК РФ понятие «вредоносной компьютерной программы».

В практической деятельности при определении вышеназванного понятия нужно исходить из диспозиции ч. 1. ст. 273 УК РФ, и понимать под вредоносной компьютерной программой программу, заведомо предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

По мнению К.Н. Евдокимова, такой подход носит упрощенный и несколько поверхностный характер, но удобен для правоприменителя тем, что закрепляет перечень вредных последствий, которые причиняет или может причинить вредоносная компьютерная программа при совершении виновным общественно опасного деяния, что позволяет осуществить уголовно-правовую квалификацию его преступных действий[66].

В частности М.М. Малыковцев считает, что «вредоносная программа – это программа, специально написанная на любом языке программирования, использование и распространение которой в информационной системе, либо в информационно-телекоммуникационной сети приводит к неправомерному воздействию на информацию и (или) на средства компьютерной техники и связи, выражающемуся в незаконном уничтожении, копировании, повреждении, блокировании, искажении информации, и(или) иному нарушению установленного законным владельцем порядка работы указанных устройств»[67].

66 Евдокимов К.Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: монография / К.Н. Евдокимов. – Иркутск: ИЮИ (ф) АГП РФ. – 2013. – С.57.

67 Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.08 / Малыковцев Михаил Михайлович. – М., 2007. – С. 10.

Е.А. Маслакова определяет вредоносную программу как компьютерную программу, функционирование которой вызывает несанкционированное собственником компьютерной информации ее уничтожение, блокирование, модификацию либо копирование[68].

Под «вредоносными программами» подразумеваются программы, созданные с целью нарушения функционала электронно-вычислительных машин, их систем и сетей. Самыми распространенными видами вредоносных программ выступают:

1) компьютерный вирус – программы, присоединяющиеся к другим программам и выполнять различные нежелательные действия, самовоспроизводиться в нескольких экземплярах, нарушать функционирование программ, уничтожать и изменять отдельные папки и файлы и так далее;

2) троянский конь – вредоносная программа, проникающая в компьютер под видом доброкачественного программного обеспечения, выполняющая разнообразные несанкционированные функции;

3) логическая бомба – вредоносное программное обеспечение, проникающее на ЭВМ вместе с другой доброкачественной программой. Срабатывает при определенном условии. При этом не отделяется от программы-носителя и не самовоспроизводится[69].

4) Программы для взлома электронных почтовых ящиков.

Под компьютерными вирусами принято понимать разрушающие программные воздействия, обладающие следующими свойствами:

1) Способность к самодублированию – созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих его свойствами.

68 Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук: 12.00.08 / Маслакова Елена Александровна. – Орел, 2008. – С. 68.

69 Савельева И.А. Анализ статьи 273 УК РФ. Создание распространение и использование вредоносных компьютерных программ / И.А. Савельева // Наука сегодня: проблемы и перспективы развития: материалы международной научно-практической конференции в 2 частях. – Вологда, 2016. – С. 140.

2) Способность к ассоциированию с другими программами – наличие механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты компьютерной системы (заражающего механизма).

3) Способность к скрытию признаков своего присутствия в программной среде[70].

«Троянский конь» (TheTrojanHorse) – программа, позволяющая осуществлять скрытый, несанкционированный доступ к информационным ресурсам жертвы с целью получения данных, интересующих злоумышленника[71].

Троянский конь, как одна из форм вредоносной компьютерной программы, представляет собой программную закладку, которая встраивается в постоянно используемое программное обеспечение и по некоторому активизирующему событию моделирует сбойную ситуацию, парализуя нормальную работу компьютерной системы.

Установить такую программу можно с помощью электронной почты, Wi-Fi соединения или путем неправомерного подключения, т.к. защита компьютеров у большинства пользователей крайне низкая. В такой ситуации на зараженном компьютере останется вся информация о неправомерном подключении.

В настоящее время набирают обороты трояны-шифровальщики, применяемые для атак на бизнес, как на случайных, так и выборочных организаций, причем не только на Windows платформах, но и linux. Обычно загружается вредоносное ПО, зашифровывающее важные файлы, что выводит из строя работу основных приложений и требуется выкуп.

Троян семейства Zbot также остается популярным, так как шифрует свои файлы на нескольких уровнях для скрытности, а расшифрованный файл

70 Прохорова О.В. Информационная безопасность и защита информации: учебное пособие / О.В. Прохорова. – Самара: Изд-во Самарского гос. архитектурно-строительного ун-та (СГАСУ), 2014. – С. 87.

71 Рошко А.В. Информационное программно-математическое оружие / А.В. Рошко // Новые технологии в учебном процессе и производстве: Материалы XIII межвузовской научно-технической конференции, г. Рязань, (27-30 апреля 2015г.). – Рязань, 2015. – С. 117.

не хранится целиком и подгружается по частям. Троян ChePro способен атаковать практически любой онлайн-банкинг, так в своем вооружении имеет возможность делать скриншоты экрана, регистрировать нажатия клавиатуры и просматривать содержимое буфера копирования. В онлайн-банкинге может использоваться двухфакторная аутентификация, после ввода логина и пароля необходимо ввести одноразовый пароль, высылаемый в СМС-сообщении. Трояны семейства Faketoken подменяют страницу интернет-банкинга и методом социальной инженерии заставляют перейти по ссылке для загрузки Android-приложения, тем самым заражают смартфон. Далее, имея доступ к зараженному компьютеру и смартфону, перехватывают одноразовый пароль и получают доступ к личному кабинету[72].

Логическая бомба – это фрагмент программного кода или программа, осуществляющая вредоносные действия при наступлении определенных условий или по прошествии некоторого времени.

Программы для взлома электронных почтовых ящиков направлены на получение выгоды. Во-первых, в большинстве случаев существует заказчик, которому получение доступа к электронному почтовому ящику жертвы откроет новый доступ к истиной цели – личному кабинету одной из социальных сетей, к которому привязана данная почта. Во-вторых, подобные объявления часто встречаются в сети интернет, в них злоумышленники готовы предоставить свои услуги по взлому электронных почтовых ящиков за вознаграждение.

Примером подобного может послужить приговор Советского районного суда г. Красноярска от 29.07.2013 года по уголовному делу № 20051000. М. в период с января по апрель 2012 года использовала размещенные ею на интернет-сайтах компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной

72 Грицына А. С. Обзор внешних угроз, исходящих от современных киберпреступников / А. С. Грицына // Инновационные процессы в науке и обществе: сборник статей международной научно-практической конференции, г.Москва, (10 июня 2016г.). – М., 2016. – С. 11.

информации, а именно логинов и паролей от электронных почтовых ящиков законных пользователей без ведома последних.

М. разместила в сети Интернет сайт «Z***», содержащий объявление о предоставлении за денежное вознаграждение услуг по взлому электронных почтовых ящиков на почтовых серверах «Яндекс», «Майл», «Рамблер», «Вконтакте».

Сотрудник отдела «К» ГУ МВД России по Красноярскому краю в рамках контрольной закупки зарегистрировал в почтовом интернет-сервисе «Майл» электронный почтовый ящик «S***@mail.ru», после этого, привлеченный в качестве покупателя Т., оформил на сайте «Z***» заказ на «взлом» указанного почтового ящика «S***@mail.ru». На заказ о «взломе» М. ответила согласием.

Реализуя свой преступный умысел, М. запустила программу, ранее ею размещенную на сервере хостинг-провайдера и доступную по сетевому адресу «R***», путем ввода сетевого адреса в строке «адрес» web-браузера и нажатия кнопки «перейти», и указала в поле формы «получатель» электронный почтовый адрес «S***@mail.ru», в поле формы «сообщение» М. вставила содержимое электронного письма, содержащее неразборчивое изображение документа с печатью и гиперссылки с названием «посмотреть» и «скачать» предназначенные для переадресации владельца электронного почтового ящика «S***@mail.ru». Сотрудник отдела, действующий в рамках оперативного мероприятия, зашел на сайте «МАЙЛ РУ» и, авторизовавшись, открыл в электронном ящике письмо, полученное от М., затем нажал в нем на гиперссылку «посмотреть». На экране монитора отобразилась интернет-страница, оформленная аналогично странице авторизации «МАИЛ РУ» и содержащая в себе требование повторной авторизации. Таким образом, в результате действия программы, созданной М., информация о логине и пароле электронного почтового ящика «S***@mail.ru» скопировалась из памяти ЭВМ одного пользователя, то есть оперативного сотрудника, в файл, размещенный в директории интернет-сайта, управляемого М., а затем в

форме электронного письма поступила на электронный ящик самой М., после чего информация была переадресована оперативному сотруднику[73].

Подобный способ незаконного получения информации довольно таки не прост, программы данного типа обычно пишутся либо на заказ либо самими злоумышленниками. Как уже было сказано выше, в сети Интернет довольно часто встречаются объявления о взломе аккаунтов за вознаграждение, но цена за подобные действия варьируется в зависимости от сложности пароля и времени, которое уйдет на его взлом.

Выше перечисленные вредоносные программы могут быть запущены на компьютере как с помощью непосредственного, так и с помощью опосредованного доступа, однако большинство из них попадают на компьютер пользователя через флеш-карты памяти, при непосредственном её контакте с персональным компьютером пользователя, причем именно пользователь, сам того не подозревая, производит манипуляцию по вводу карты памяти, после обнаружения которой оперативная система подвергается угрозе со стороны вредоносной программы, маскирующейся под одну из файловых папок на введенной карте.

Использование вредоносного программного обеспечения путем перехвата вводимой с клавиатуры или выводимой на экран информации, может быть установлено вредоносное программное обеспечение, которое фиксирует всю информацию законного пользователя, или создает скриншоты во время процесса авторизации, а затем направляет копию этого файла преступнику. Некоторые вредоносные программы ищут существующий файл с паролями веб-браузера клиента, затем копируют этот файл, который (кроме хорошо зашифрованных) будет содержать легкодоступные сохраненные пароли из истории страниц, посещенных пользователем[74].

Примером использования вредоносного программного обеспечения, осуществляющего перехват вводимой с клавиатуры информации, может

73 Уголовное дело № 20051000 // Архив Советского районного суда г. Красноярска. 2013 год.
74 10 наиболее распространенных методов взлома паролей [Электронный ресурс] // Режим доступа:http://internetua.com/10-naibolee-rasprostranennih-metodov-vzloma-parolei

послужить случай, исследованный экспертом по уголовному делу № 23057100.

Объектом исследования эксперта являлся системный блок ЭВМ. На рабочем столе пользователя был обнаружен каталог «ActualSpy 2.8». В указанном каталоге обнаружен файл с инструкцией пользователя к программе ActualSpy (версия 2.8), в которой указано, что данное приложение является «шпионским» и предназначено для слежения за действиями пользователя ЭВМ, является программой-кейлогером, предназначенной для несанкционированного копирования информации о работе пользователя.

После запуска программы ActualSpy открывается окно, в котором отображается информация о перехваченной информации с ЭВМ, структурированная по соответствующим разделам: «Клавиатура» – запись всех нажатых пользователем клавиш, «Скриншоты» – скриншоты активного окна операционной системы, «Программы» – запуск программ, «Буфер» – данные содержащиеся в буфере обмена операционной системы, «Файлы» – открытые и измененные файлы, «Компьютер» – время включения и выключения компьютера, авторизация пользователя.

В подпункте «Отсылка отчета» указан электронный почтовый ящик ****@mail.ru, на который программа ActualSpy отсылает отчеты о перехваченной информации пользователя, в том числе информацию о нажатых клавишах (переписка пользователя, логины и пароли различных интернет-ресурсов), после отправки указанных данных они удаляются с НЖМД ЭВМ (согласно настройкам). Электронные письма от программы ActualSpy озаглавливаются «Отчёт от Actual Spy» и доставляются каждые 3 часа.

После создания скриншотов и записи информации на компакт-диск, ЭВМ выключается и отключается от периферийных устройств и сети электропитания[75].

75 Уголовное дело № 23057100 // Архив Красноярского краевого суда. 2015 год.

Данная программа-кейлогер довольно проста в использовании, требуемую информацию, которую необходимо перехватить, можно отметить в списке пункта меню «Настройки» программы ActualSpy – нажатые клавиши, скриншоты экрана, запуск программ, содержимое буфера обмена операционной системы, распечатанные документы, изменения файлов и папок, включение и выключение компьютера.

2.4 Способы совершения преступлений в сфере компьютерной информации, связанные с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Преступления, связанные с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, предусмотрены ст. 274 Уголовного кодекса РФ. Указанная статья является бланкетной и отсылает к конкретным инструкциям и правилам, устанавливающим порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и конечным оборудованием в ведомстве или организации. Эти правила должны устанавливаться правомочным лицом. Общих правил эксплуатации, распространяющихся на неограниченный круг пользователей глобальной сети Интернет, не существует.

Под правилами эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей понимаются:

1. Общие правила техники безопасности при работе с вычислительной техникой, соответствующие стандарты на обеспечение информационной безопасности.

2. Инструкции по эксплуатации компьютерной техники, составляемые её производителем, поставляемые вместе с нею и содержащие правила

использования вычислительной техники, определяемые её конструктивными и технологическими особенностями.

3. Правила по эксплуатации электронных вычислительных машин, их систем и сетей, устанавливаемые их владельцем[76].

Нарушение правил эксплуатации может выражаться как в полном игнорировании, так и в ненадлежащем соблюдении правил. Нарушение может быть выражено в форме действия или бездействия (совершение запрещённых действий или невыполнение виновным действий, предписанных правилами). Термины «нарушение правил» и «несоблюдение правил» в контексте статьи 274 УК РФ следует рассматриваться как равнозначные (синонимы)[77].

В теории и на практике отсутствует единое мнение относительно того, какие конкретно правила имеются в виду законодателем.

Д.И. Чистов указывает на нарушения установки техники, режима использования ЭВМ, эксплуатацию компьютера не по прямому назначению, отключение сигнализации, не проверку на вредоносные программы, не включение систем защиты информации, оставление без присмотра рабочего места и др. Несоблюдение данных правил может выражаться в виде их частичного или полного игнорирования, а также прямого их нарушения[78].

В.С. Комиссаров при описании этих правил ссылается на санитарно-эпидемиологические правила и нормативы «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» СанПиН 2.2.2/2.4.1340-03, утв. главным государственным санитарным врачом РФ 30.05.2003[79].

76 Гребеньков А.А. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей как информационное преступление / А. А. Гребеньков // Актуальные научные исследования в современном мире. – 2016. – № 9. – С.129.

77 Воробьев В.В. Проблемы применения состава ст. 274 УК РФ / В.В. Воробьев // Вестник КРАГСиУ. Серия «Государство и право». – 2015. – № 20. – С. 13.

78 Чистов Д.И. Конституционному реформированию уголовно-правовой политики – кибернетический подход / Д. И. Чистов // Юридический мир. – 2006. – № 10. – С. 15.

79 Комиссаров В.С. Преступления в сфере компьютерной безопасности: понятия и ответственность / В.С. Комиссаров // Юридический мир. – 1998. – № 2. – С. 22.

Преступления, предусмотренные ст. 274 УК РФ, могут совершаться путем совершения запрещённых действий или невыполнением виновным лицом действий, предписанных правилами:

1) нарушение установки техники;

2) нарушение режима использования компьютеризированной техники;

3) эксплуатация компьютера не по прямому назначению;

4) отключение систем защиты информации.

Нужно отметить, что нормативно разработанных правил эксплуатации компьютеров, их операционной системы или их сети вообще не существует. Для того чтобы привлечь лицо к уголовной ответственности за нарушение правил эксплуатации компьютеров, необходимо разработать технико-юридическую норму, в которой бы полностью отражался и регламентировался порядок обращения с компьютером, его оперативной системой или их сетью. До тех пор, пока этого не будет сделано, ст. 274 УК РФ применяться не будет. На настоящий момент практика по данной статье в России отсутствует.

Заключение

На сегодняшнем этапе развития российской правоохранительной системы и возможностей экспертных учреждений вопрос о выявлении, описании и изучении способов совершения преступлений в сфере компьютерной информации представляет особую актуальность в связи с тем, что современная преступность претерпевает качественную трансформацию и приобретает экономическую и политическую окраску. Растет количество экономических преступлений, совершенных с использованием электронных средств, а суммы причиненного ущерба неуклонно увеличиваются.

Российскому законодательству в сфере борьбы с компьютерной преступностью требуется совершенствование, так как отечественный понятийно-терминологический аппарат, используемый в сфере компьютерной информации – устарел, потерял актуальность и не соотносится с действительностью. Требуется свежий взгляд, отвечающий современным тенденциям, на такие понятия как: компьютерная информация, носитель информации и т.п.

Динамика развития и совершенствования способов совершения преступлений в сфере компьютерной информации растет с каждым днем, российскому законодателю давно пора уделить внимание проблеме, связанной с киберпространством, которое стало неотъемлемой частью жизни каждого, так как Россия, увы, все еще стоит на первом месте в мире по числу компьютерных атак, приходящихся на активных пользователей Интернета, где основным условием возникновения такого большого количества жертв

компьютерных преступлений, является компьютерная безграмотность населения.

Список использованных источников

I. Нормативно-правовые акты:

1. Уголовный кодекс Российской Федерации: федеральный закон Российской Федерации от 13.06.1996 г. № 63-ФЗ. – Новосибирск: Норматика, 2016. – 208 с.

2. Уголовно-процессуальный кодекс Российской Федерации: федеральный закон Российской Федерации от 18.12.2001 г. № 174-ФЗ. – Новосибирск: Норматика, 2016. – 256 с.

3. О ратификации Соглашения о сотрудничестве государств-участников Содружества независимых государств в борьбе с преступлениями в сфере компьютерной информации: федеральный закон Российской Федерации от 01.10.2008 г. № 164-ФЗ // Российская газета. – 2008. – 03 октября.

4. Об информации, информационных технологиях и о защите информации: федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ // Российская газета. – 2006. – 29 июля.

5. О сертификации средств защиты информации: постановление Правительства Российской Федерации от 26.06.1995 г. № 608-ФЗ // Российская газета. – 1995. – 28 июня.

II. Специальная литература:

6. Алиева, М.Ф. Botnet или Зомби-сети / М.Ф. Алиева, Т.Г. Чучминова // Наука. Образование. Молодежь. – 2016. – № 1. – С. 321–323.

7. Атальянц, М.А. Значение способа совершения преступления для квалификации преступлений / М.А. Атальянц // Пробелы в российском законодательстве. – 2009. – № 4. – С. 221–223.

8. Бессонов, С.А. К вопросу о структуре и природе криминалистической характеристики преступлений / С.А. Бессонов // Вестник Поволжского института управления. – 2014. – № 4 (43). – С. 52–57.

9. Бондаренко, Е.С. Эволюция вирусов-шифровальщиков / Е.С. Бондаренко // Контентус. – 2016. – № 8(49). – С. 143–145.

10. Брумштейн, Ю.М. Информационная безопасность сайтов высших учебных заведений: проблемы и решения / Ю.М. Брумштейн // Информационная безопасность регионов. – 2014. – № 1(14). – С. 38–47.

11. Бурданова, В.С. Криминалистическая характеристика преступлений, связанных с незаконным оборотом наркотиков / В.С. Бурданова // Прокурорско-следственный работник. – 1998. – № 3. – С. 7–16.

12. Васильев, А.Н. Проблемы методики расследования отдельных видов преступлений / А.Н. Васильев. – М.: Изд-во МГУ, 1978. – 71 с.

13. Ведерников, Н.Т. Личность преступника в криминалистике и криминологии / Н.Т. Ведерников // Вестник Томского государственного университета. – 2014. – № 384. – С. 148–152.

14. Вехов, В.Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; под ред. Б.П. Смагоринского. – М.: Право и Закон, 1996. – 192 с.

15. Воробьев, В.В. Проблемы применения состава ст. 274 УК РФ / В.В. Воробьев // Вестник КРАГСиУ. Серия «Государство и право». – 2015. – № 20. – С.12–18.

16. Гаврилин, Ю.В. Расследование неправомерного доступа к компьютерной информации: учебное пособие / Ю.В. Гаврилин, А.В. Пушкин, Е.А. Соцков, Н.Г. Шурухнов; под общ. ред. Н.Г. Шурухнова. – Изд. 2-е, перераб. и доп. – М.: ЮИ МВД РФ, Книжный мир, 2004. – 352 с.

17. Гонохова, Д.Ю. Руткиты / Д.Ю. Гонохова // Перспективы развития науки и образования: сборник научных трудов по материалам XI международной научно-практической конференции, г. Москва, (30 ноября 2016 г.); под общ. ред. А.В. Туголукова. – М., 2016. – С. 346–347.

18. Гребеньков, А.А. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей как информационное преступление / А.А. Гребеньков // Актуальные научные исследования в современном мире. – 2016. – № 9. – С. 129–133.

19. Грицына, А.С. Обзор внешних угроз, исходящих от современных киберпреступников / А.С. Грицына // Инновационные процессы в науке и обществе: сборник статей международной научно-практической конференции, г.Москва, (10 июня 2016 г.). – М.: Изд-во ООО «Европейский фонд инновационного развития», 2016. – С. 10–13.

20. Давыдов, В.О. Значение виртуальных следов в расследовании преступлений экстремистского характера / В.О. Давыдов, А.Ю. Головин // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3-2. – С. 254–258.

21. Давыдов, В.О. Методика расследования экстремистских преступлений, совершенных в компьютерных сетях: монография / В.О. Давыдов; под общ. ред. А.Ю. Головина. – М.: Юрлитинформ, 2014. – 184 с.

22. Дедюрина, О.В. Назначение программ-шпионов и методы противодействия им / О.В. Дедюрина, Т.Г. Долгова // Актуальные проблемы авиации и космонавтики. – 2014. – № 10. – С. 363.

23. Добровольский Д.В. Актуальные проблемы борьбы с преступностью (уголовно-правовые и криминологические проблемы): дис. ... канд. юрид. наук: 12.00.08 / Добровольский Дмитрий Владимирович. – М., 2005. – 218 с.

24. Дремлюга, Р.И. Интернет-преступность: монография / Р.И. Дремлюга. – Владивосток: Дальневосточный университет, 2008. – 240 с.

25. Дудников, А.Л. Криминалистическое понятие «способ преступления» / А. Л. Дудников // Проблемы законности. – 2012. – № 120. – С. 1–6.

26. Евдокимов, К.Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: монография / К.Н. Евдокимов. – Иркутск: ИЮИ АГП РФ, 2013. – 267 с.

27. Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: дис. … канд. юрид. наук: 12.00.09 / Зигура Надежда Анатольевна. – Челябинск, 2010. – 234 с.

28. Зуйков, Г.Г. Поиск по признакам способов совершения преступлений: учебное пособие / Г.Г. Зуйков. – М.: НИиРИО ВШ МВД СССР, 1970. – 191 с.

29. Казанцева, С.Я. Информатика и математика для юристов: учебник / под ред. С.Я. Казанцевой, Н.М. Дубининой. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2010. – 560 с.

30. Кирсанов, И.А. Компьютерное уголовное право: проблемы и пути решения / И.А. Кирсанов // Альманах современной науки и образования. – 2012. – № 6. – С. 72–74.

31. Князьков, А.С. Криминалистическая характеристика преступления в контексте его способа и механизма / А.С. Князьков // Вестник Томского Государственного университета. Право. – 2011. – № 1. – С. 51–64.

32. Комиссаров, В.С. Преступления в сфере компьютерной безопасности: понятия и ответственность / В.С. Комиссаров // Юридический мир. – 1998. – № 2. – С. 22–24.

33. Коновалов, С.И. Теоретико-методологические проблемы криминалистики: монография / С.И. Коновалов. – Ростов-на-Дону: РЮИ МВД России, 2001. – 208 с.

34. Коржев, М.А. Криминалистическое значение следов человека / М.А. Коржев // Инновационная наука. – 2015. – №7-2. – С. 74–76.

35. Крестовников, О.А. Механизм и способ преступления в составе расследуемого события / О.А. Крестовников // Юридические записки. – 2013. – № 2. – С. 106–111.

36. Кудряшова, О.А. Криминалистическое значение обстановки совершения преступления / О.А. Кудряшова // Вестник Южно-Уральского государственного университета. – 2011. – № 27. – С. 49–54.

37. Курс криминалистики: В 3 т. Т. 3: Криминалистические средства, приемы и рекомендации / под общ. ред. Р.С. Белкина. – М.: Юристъ, 1997. – 480 с.

38. Лысов, Н.Н. Содержание и значение криминалистической характеристики компьютерных преступлений / Н.Н. Лысов // Проблемы криминалистики и методики ее преподавания: Тезисы выступлений участников семинара-совещания преподавателей криминалистики. – М., 1994. – 108 с.

39. Малыковцев, М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.08 / Малыковцев Михаил Михайлович. – М., 2007. – 186 с.

40. Маслакова, Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук: 12.00.08 / Маслакова Елена Александровна. – Орел, 2008. – 198 с.

41. Милюс, А.И. К вопросу о криминалистической характеристике краж нефти и нефтепродуктов / А.И. Милюс // Вестник Кемеровского государственного университета. – 2014. – № 2. – С. 273–276.

42. Новик, В.В. Криминалистические аспекты доказывания по уголовным делам / В.В. Новик. – М.: Litres, 2017. – 635 с.

43. Образцов, В.А. Теоретические основы раскрытия преступлений, связанных с ненадлежащим исполнением профессиональных функций в сфере производства / В.А. Образцов. – Иркутск, 1985. – 109 с.

44. Олиндер, Н.В. Время и место совершения преступления как элемент криминалистической характеристики преступлений, совершенных с использованием электронных платежных средств и систем / Н.В. Олиндер // Вестник Самарского государственного университета. – 2014. – № 11-1. – С. 89–93.

45. Омарова, Э.А. Мошенничество в финансово-кредитной сфере / Э.А. Омарова, Ю.М. Махдиева // Пути повышения финансовой стабильности регионов Северного Кавказа: взгляд молодых ученых: материалы Всероссийской научно-практической конференции студентов, аспирантов и молодых преподавателей. ФГБОУ ВО «Дагестанский государственный университет», г. Махачкала, (20-22 октября 2016 г.) / под общ. ред. Ю.М. Махдиевой. – Махачкала, 2016. – С. 366–367.

46. Осипенко, А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография / А.Л. Осипенко. – Омск: Омская академия МВД России, 2009. – 480 с.

47. Поляков, В.В. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации / В.В. Поляков, С.М. Слободян // Известия Томского политехнического университета. – 2007. – № 1. – С. 212–216.

48. Поляков, В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической

характеристики / В.В. Поляков // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114–116.

49. Прохорова, О.В. Информационная безопасность и защита информации: учебное пособие / О.В. Прохорова. – Самара: Изд-во Самарского гос. архитектурно-строительного ун-та (СГАСУ), 2014. – 114 с.

50. Радько, Н.М. Угрозы непосредственного доступа в операционную среду компьютера / Н.М. Радько // Информация и безопасность. – 2007. – № 2. – С. 317–320.

51. Рогозин, В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий / В.Ю. Рогозин // Расследование преступлений: проблемы и пути их решения. – 2015. – № 6. – С. 10.

52. Рошко, А.В. Информационное программно-математическое оружие / А.В. Рошко // Новые технологии в учебном процессе и производстве: материалы XIII межвузовской научно-технической конференции, г. Рязань (27-30 апреля 2015г.). – Рязань: Изд-во ООО «Рязанский Издательско-полиграфический дом «ПервопечатникЪ», 2015. – С. 115–119.

53. Савельева, И.А. Анализ статьи 273 УК РФ. Создание распространение и использование вредоносных компьютерных программ / И.А. Савельева // Наука сегодня: проблемы и перспективы развития: материалы международной научно-практической конференции в 2 частях. Научный центр «Диспут», г. Вологда, (30 ноября 2016г.). – Вологда: Изд-во ООО «Маркер», 2016. – С. 140–141.

54. Самойлов, А.В. Современное состояние учения о криминалистической характеристике преступлений / А.В. Самойлов // Российский следователь. – 2010. – № 22. – С. 5–6.

55. Семенов, Г.В. Криминалистическая характеристика неправомерного доступа к компьютерной информации в системе сотовой

связи / Г.В. Семенов // Юридические записки. Криминалистические средства и методы исследования преступлений. – 2001. – № 10. – С. 184–193.

56. Семыкина, О.И. Противодействие киберпреступности за рубежом / О.И. Семыкина // Журнал зарубежного законодательства и сравнительного правоведения. – 2016. – № 6. – С. 104–113.

57. Скородумова, О.Б. Хакеры / О.Б. Скородумова // Знание. Понимание. Умение. – 2005. – № 4. – С. 159–161.

58. Утребов, Д.Р. Классификация угроз в системах управления базами данных / Д.Р. Утребов, С.В. Белов // Вестник Астраханского Государственного технического университета. – 2008. – № 1. – С. 87–92.

59. Федотов, Н.Н. Форензика – компьютерная криминалистика: учебное пособие / Н.Н. Федотов. – М.: Юридический мир, 2007. – 360 с.

60. Холмогоров, В. PRO Вирусы / В. Холмогоров. – М.: Страта, 2017. – 142 с.

61. Хорев, А.А. Технические каналы утечки информации, обрабатываемой техническими средствами / А.А. Хорев // Специальная техника. – 2004.– № 2. – С. 3–6.

62. Чистов, Д.И. Конституционному реформированию уголовно-правовой политики – кибернетический подход / Д.И. Чистов // Юридический мир. – 2006. – № 10. – С. 10–17.

63. Шарков, А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. … канд. юрид. наук: 12.00.08 / Шарков Александр Евгеньевич. – Ставрополь, 2004. – 156 с.

64. Яблоков, Н.П. Криминалистическая характеристика преступлений и типичные следственные ситуации как важные факторы разработки методики расследования преступлений / Н.П. Яблоков // Вопросы борьбы с преступностью. – 1979. – № 30. – С. 21–26.

III. Электронные ресурсы:

65. Вирус WannaCry [Электронный ресурс]. – Режим доступа: http://ru.d-ws.biz/articles/viruses-wana-decryptor.shtml.

66. Кто такие кракеры [Электронный ресурс]. – Режим доступа :http://it-sektor.ru/kto-takoyi-cracker-/-kraker.html.

67. Модельный закон о киберпреступности [Электронный ресурс]. – Режим доступа: ITUToolkitForCybercrimeLegislation.

68. Понятие «компьютерная информация» с точки зрения ее уголовно-правовой защиты. [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/ponyatie-kompyuternaya-informatsiya-s-tochki-zreniya- ugolovno-pravovoy-zaschity.

69. Способы совершения преступлений в сфере компьютерной информации [Электронный ресурс]. – Режим доступа: http://bestreferat.su/Gosudarstvo-i-pravo/Sposoby-soversheniya-prestupleniya-v-sfere-kompyuternoy-informacii/.

70. 10 наиболее распространенных методов взлома паролей [Электронный ресурс]. – Режим доступа: http://internetua.com/10-naibolee-rasprostranennih-metodov-vzloma-parolei.

71. Топ-10 методов взломов паролей [Электронный ресурс]. – Режим доступа: http://www.pcidss.ru /articles/39.html.

IV. Судебная и следственная практика:

72. Приговор Харабалинского районного суда Астраханской области по делу Сергеева Я.О. от 21.11.2016 года по уголовному делу № 1-176/2016 // Справочная правовая система «РосПравосудие». – Режим доступа: https://rospravosudie.com.

73. Приговор Кировского районного суда г. Красноярска по делу Любутина А.Л. от 14.12.2016 года по уголовному делу № 1-606/2016 // Справочная правовая система «РосПравосудие». – Режим доступа: https://rospravosudie.com.

74. Приговор Ленинского районного суда г. Нижний Новгород по делу Борисовой Д.В. от 11.06.2016 года по уголовному делу № 1-365/2016 // Справочная правовая система «Судпрактика». – Режим доступа: http://sud-praktika.ru.

75. Приговор Лефортовского районного суда г. Москвы по делу Анимисова А.В. от 13.01.2015 года по уголовному делу № 1-6/2015 // Справочная правовая система «Судебные и нормативные акты РФ». – Режим доступа: http://sudact.ru.

76. Приговор Новотроицкого городского суда Оренбургской области по делу Малькова А.Ю. от 29.08.2011 года по уголовному делу № 1-304/2011 // Справочная правовая система «РосПравосудие». – Режим доступа: https://rospravosudie.com.

77. Уголовное дело № 15003100 // Архив Лесосибирского городского суда Красноярского края. 2007 год.

78. Уголовное дело № 20051000 // Архив Советского районного суда г. Красноярска. 2013 год.

79. Уголовное дело № 24130500 // Архив Красноярского краевого суда. 2015 год.

80. Уголовное дело № 23001500 // Архив Кировского районного суда г. Красноярска. 2015 год.

81. Уголовное дело № 23042100 // Архив Красноярского краевого суда. 2015 год.

82. Уголовное дело № 23057100 // Архив Красноярского краевого суда. 2015 год.

Приложения

Приложение А.

Приговор Лесосибирского городского суда Красноярского края по уголовному делу № 15003100 // Архив Лесосибирского городского суда Красноярского края. 2007 год.

Вещественные доказательства, хранящиеся в камере хранения вещественных доказательств ОВД г.Лесосибирска - уничтожить, поскольку системный блок компьютера, коммутатор являлись предметами, с использованием которых были совершены преступления.

Гражданские иски не заявлены.

Процессуальные издержки по делу взысканию с подсудимого не подлежат в силу требований ст.316 п.10 УПК РФ.

Приговор может быть обжалован в кассационном порядке в Красноярский краевой суд в течение 10 дней после вынесения, с соблюдением требований ст.317 УПК РФ, подачей жалобы через Лесосибирский городской суд. В случае подачи кассационной жалобы осужденный вправе ходатайствовать о своем участии в рассмотрении уголовного дела судом кассационной инстанции, с указанием об этом в кассационной жалобе.

Председательствующий судья Г.В. Браун

При назначении вида и размера наказания, суд учитывает характер и степень общественной опасности совершенных преступлений, обстоятельства дела личность подсудимого.

Синкевич Р.Н. ранее не судим, впервые совершил преступления небольшой тяжести, вину свою признал полностью, раскаялся в содеянном, возместил причиненный ущерб, занимается воспитанием малолетнего ребенка своей жены от первого брака, положительно характеризуется по месту жительства, занят общественно-полезным трудом, что суд признает смягчающими наказание обстоятельствами.

Принимая во внимание обстоятельства по делу, тяжесть совершенных преступлений, личность подсудимого, имущественное положение Синкевича и его семьи, суд считает, что наказание Синкевичу Р.Н. следует назначить в виде штрафа.

Процессуальные издержки по делу взысканию с подсудимого не подлежат в силу требований ст.316 п.10 УПК РФ.

Гражданские иски не заявлены.

На основании изложенного и руководствуясь ст.ст.307-309,316 УПК РФ, суд

ПРИГОВОРИЛ:

Признать Синкевича Руслана Николаевича виновным в совершении преступления, предусмотренного ч.1 ст.165 УК РФ и в совершении трех преступлений, предусмотренных ч.1 ст.272 УК РФ.

Назначить Синкевичу Р.Н. наказания за совершенные преступления:

- по ч.1 ст.165 УК РФ в виде штрафа в размере 10 тысяч рублей,
- за три преступления, предусмотренных ч.1 ст.272 УК РФ штраф в размере 15 тысяч рублей за каждое,

В соответствии с ч.2 ст.69 УК РФ, по совокупности преступлений, путем частичного сложения назначенных наказаний, окончательно Синкевичу Р.Н. назначить наказание в виде штрафа в размере 20 тысяч рублей.

Меру пресечения Синкевичу Р.Н. до вступления приговора в законную силу оставить в виде подписки о невыезде.

Приложение Б.

Справка об исследовании по уголовному делу
№ 24130500 // Архив Красноярского краевого суда. 2015 год.

ООО "[redacted]"
[redacted]

14.11.2015

Справка об исследовании

Эксперт: Н., имеющий высшее техническое образование по специальности «Системы автоматизированного проектирования», стаж работы в области программного обеспечения и баз данных более 8 лет.

Сертификат курса обучения «Проведение исследований и экспертиз по делам, связанным с нарушением авторского права на программы для ЭВМ».

Сертификат курса обучения "Специалист Microsoft по средствам защиты программных продуктов".

Свидетельство о квалификации "Ассоциации по противодействию компьютерным преступлениям" № СВ-2908/2006-1к.

Сертификат курса обучения "Экспертиза контрафактной продукции" № 00020 АНО «СОЮЗЭКСПЕРТИЗА».

Сертификат курса обучения "Отличительные признаки и свойства оригинальной программной продукции ЗАО «1С».

Сертификат о прохождении курса ООО «Аутодеск (Си-Ай-Эс)».

Сертификат о прохождении курса ООО «Адоб Системс» «Специалист Adobe по средствам защиты и лицензирования программных продуктов AdobeSystems».

Сертификат о прохождении курса «CorelCorporation».

На исследование представлено:

1. НЖМД модели [redacted] серийный номер[redacted].

ВОПРОСЫ ИССЛЕДОВАНИЯ:

1. Имеется ли на представленном носителе информации программное обеспечение TeamViewer, предназначенное для удаленного администрирования? Если да то какова дата его установки, какой используется ID-номер?
2. Имеется ли информация о том, когда и с каких IP-адресов или ID-номеров осуществлялось подключение к операционной системе, установленной на НЖМД?

3. Имеется ли информация о логине «matr.in» в какой программе, для чего используется?

4. Имеется ли на НЖМД информация о единвременном удалении большого количества файлов, содержащих фото-избражения, документы, видео-записи?

В ходе исследования установлено:

Объектом исследования является НЖМД модели [redacted] серийный номер [redacted], упакованный в конверт белого цвета, который опечатан исключающим печатью «Для справок» Отдел «К» ГУ МВД России по Красноярскому краю с сопроводительной надписью «НЖДМ, добровольно выданный гр. [redacted]» не имеющие внешних повреждений, который извлечен из конверта и посредством USB-SATA адаптера подключен к стационарной ПЭВМ.

НМЖД разделен на три логических диска «E», «F», «G».

Локальный диск «E» является служебным диском операционной системы. Локальный диск «F» не содержит информации.

В результате сканирования диска программой восстановления удаленной инормации R-Studio, обнаружено, что ранее находившиеся на диске файлы удалены, установить дату удаления не представилось возможным.

На локальном диске «G» установлена операционная система Windows 8, дата установки 12.03.2014, имя основного пользователя операционной системы «[redacted]».

В результате просмотра журналов работы операционной системы, которые расположены в каталоге «g:\Windows\System32\winevt\Logs\», фактов подключения по стандартному протоколу удаленного администрирования не обнаружено, также не обнаружено IP-адресов, сетевых имен и других идентификаторов позволяющих установить факты сетевого подключения к данной ЭВМ.

В ходе просмотра журналов установлено ЭВМ, в которой был установлен осматриваемый НЖМД был включен в период с 10:00 24.11.2015 по 08:40 25.11.2015.

Программноеобеспечение «TeamViewer», расположенное в каталоге «C:\ProgramFiles (x86)\TeamViewer\» (соответствует катологу G:\ProgramFiles (x86)\TeamViewer\ на момент осмотра диска), предназанченное для дистанционного администрирования, было удалено 25.11.2015 в 08:39.

Вкаталоге «G:\Windows\System32\config\RegBack» обнаружена архивная копия реестра операционной системы, которая установлена на данном НЖМД.

После подключения файла реестра в его содержимом обнаружена запись с настройками удаленной программы «TeamViewer».

Версия программы – 10.0.47484

Последний IP-адрес поддержки – [redacted]

Аккаунт владельца – [redacted]

Дата установки – 24.09.2015

ID-пользователя - [redacted]

Вкаталоге «g:\ProgramFiles (x86)\TeamViewer\» ранее была установлена программа «TeamViewer», дата установки 24.02.2014.

В указанном каталоге обнаружен файл «Connections_incoming.txt», в котором содержится запись об успешной сессии дистанционного администрирования 24.11.2015 в период с 23:15 по 23:17.

Согласно данной записи удаленное администрирование осуществлялось пользователем с ID-[redacted] (ID пользователся в программе TeamViewer) и именем компьтера или именем пользователя «[redacted]», «[redacted]» - имя пользователя операционной системы на осматриваемом НЖМД.

Вкаталоге «g:\ProgramFiles (x86)\TeamViewer\Version9» обнаруженфайл «Connections_incoming.txt», в котором содержатся записи о сессиях дистанционного администрирования в период до января 2015 года.

В результате сканирования диска программой восстановления удаленной информации R-Studio в каталоге «g:\ProgramFiles (x86)\TeamViewer\» обнаружены удаленные служебные файлы программы TeamViewer.

В результате восстановления указанных файлов и их просмотра дополнительной информации не получено.

В каталоге «Документы» пользователя «[redacted]» обнаружено, что удалены только каталог с названием «[redacted]», остальные документы находятся на диске, также на рабочем столе пользователя удалены каталоги содержащие аудиозаписи, созданные на телефоне пользователя.

НЖМД отключен от стационарной ПЭВМ.

Выводы

1. Имеется ли на представленном носителе информации программное обеспечение TeamViewer, предназначенное для удаленного администрирования? Если да то какова дата его установки, какой используется ID-номер?

Вкаталоге «g:\ProgramFiles (x86)\TeamViewer» обнаружена удаленная программа TeamViewer, предназанченная для дистанционного администрирования, дата установки 24.02.2014, ID-номер [redacted]

2. Имеется ли информация о том, когда и с каких IP-адресов или ID-номеров осуществлялось подключение к операционной системе, установленной на НЖМД?

Вфайле«Connections_incoming.txt» содержится информация о том, что 24.11.2015 в период с 23:15 по 23:17 осуществлялось удаленное администрирование операционной системы, установленной на исследуемом НЖМД посредством программы TeamViewer пользователем имеющим ID-номер [redacted], которого имя компьютера или имя пользователя записано как «[redacted]»

3. Имеется ли информация о логине «[redacted]» в какой программе, для чего используется?

Логин «[redacted]» использовался при установке программы TeamViewer, а также пользователь с таким логином или именем компьютера осуществлял удаленное управление 24.11.2015 в период с 23:15 по 23:17 посредством данной программы.

4. Имеется ли на НЖМД информация о единвременном удалении большого количества файлов, содержащих фото-избражения, документы, видео-записи?

На логическом диске F,предположительно, было осуществлено форматирование диска, при котором все находящиеся ранее на нем файлы были удалены. Также в личных каталогах пользователя «[redacted]»удалены папки «[redacted]» и директории, в которых содержались аудио-записи, предположительно, созданные при записи телефоном с функцией диктофона.

Примечание: По окончании исследования, представленные носители информации упакованы в первоначальную упаковку. Упаковка опечатана полоской бумаги белого цвета с оттиском печати «НП КПП» сопроводительной надписью и подписью эксперта выполненных красителем черного цвета.

14.11.2015

Приложение В.

Справка об исследовании по уголовному делу № 23001500 // Архив Кировского районного суда г. Красноярска. 2015 год.

ООО [redacted]

09.08.2015

Справка об исследовании

Эксперт:.Н., имеющий высшее техническое образование по специальности «Системы автоматизированного проектирования», стаж работы в области программного обеспечения и баз данных более 8 лет.

Сертификат курса обучения «Проведение исследований и экспертиз по делам, связанным с нарушением авторского права на программы для ЭВМ».

Сертификат курса обучения "Специалист Microsoft по средствам защиты программных продуктов".

Свидетельство о квалификации "Ассоциации по противодействию компьютерным преступлениям" № СВ-2908/2006-1к.

Сертификат курса обучения "Экспертиза контрафактной продукции" №00020 АНО «СОЮЗЭКСПЕРТИЗА».

Сертификат курса обучения "Отличительные признаки и свойства оригинальной программной продукции ЗАО «1С».

Сертификат о прохождении курса ООО «Аутодеск (Си-Ай-Эс)».

Сертификат о прохождении курса ООО «Адоб Системс» «Специалист Adobe по средствам защиты и лицензирования программных продуктов AdobeSystems».

Сертификат о прохождении курса «CorelCorporation».

На исследование представлено:

1. Бумажный пакет опечатанный отрезом бумаги с оттиском печати «Для справок ГУ МВД России по Красноярскому краю», пояснительной надписью «Оптический носитель с файлом install.apk» и подписями участвовавших лиц.

ВОПРОСЫ ИССЛЕДОВАНИЯ:

1. Имеется ли на представленном носителе вредоносное программное обеспечение?

2. Каков механизм работы указанного вредоносного программного обеспечения?

3. Имеются ли сведения об IP-адресах или Интернет-сайтах с которых происходит управление вредоносным программным обеспечением?

В ходе исследования установлено:

При вскрытии пакета обнаружен компакт-диск CD-RIntro№ [redacted]. На компакт-диске обнаружен файл «install.apk» - формат архивных исполняемых файлов-приложений для операционной системы Android.

Архивный файл «install.apk» содержит файлы, указанные в Приложении № 1.

Антивирусным программным обеспечением DrWebCureIt, указанный файл определяется каквредоносное программное обеспечение типа «Android.SmsBot.391.origin».

Для определения функций предоставленного на исследование программного обеспечения используются общедоступные «Интернет-песочницы», расположенные по адресам [redacted] На указанных сайтах осуществляется распаковка архива и запуск исполняемых программ в безопасной среде, эмулирующей операционную систему Android.

Результаты работы данных сервисов указаны в Приложении № 2.

Представленное на исследование программное обеспечение при установке использует следующие функции устройства с ОС Android:

android.permission.SEND_SMS - отправка SMS сообщения;

android.permission.DISABLE_KEYGUARD - отключение блокировки клавиатуры;

android.permission.RECEIVE_BOOT_COMPLETED - запускпризагрузке;

android.permission.INTERNET - полный доступ в Интернет;

android.permission.SYSTEM_ALERT_WINDOW - дисплей оповещения системного уровня;

android.permission.KILL_BACKGROUND_PROCESSES - остановкафоновыхпроцессов;

android.permission.WRITE_SMS - редактирование SMS или MMS сообщений;

android.permission.ACCESS_NETWORK_STATE - просмотрсостоянияcети;

android.permission.WAKE_LOCK – предотвращение режима «сон» телефона;

android.permission.GET_TASKS – просмотр запущенных приложений;

android.permission.CALL_PHONE – осуществление телефонных вызовов;

android.permission.VIBRATE - контроль вибрации;

android.permission.RECEIVE_SMS – получение SMS;

android.permission.READ_PHONE_STATE – считываниесостоянияателефона;

android.permission.WRITE_EXTERNAL_STORAGE - изменение/удалениесодержимого SD-карты)

android.permission.READ_SMS - чтение SMS или MMS-сообщений.

После установки передает на сервер «[redacted]»телефона на котором установлен, абонентский номер, модель операционной системы. Основной вредоносной функцией программы является отправка СМС-сообщений на номера «[redacted]» (платежная система Qiwi), «900» (мобильный банк Сбербанка), «[redacted]» (служебный номер ОАО «Мегафон»). Обращение по протоколу «Http» осуществляется на Интернет-сайт «[redacted]» (IP-адрес [redacted]), который предположительно является командным сервером для данной программы.

Согласно данным whois-сервиса интернет-регистратора ripe.netдоменное имя «developartner.com» зарегистрировано компанией «[redacted]» (адрес:[redacted]), сайт расположен по IP-адресу [redacted], который принадлежит хостинг-компании ООО «[redacted]» (адрес:[redacted]).

Выводы

1. Имеется ли на представленном носителе вредоносное программное обеспечение?

На указанном носителе представлено вредоносное программное обеспечение типа «Android.SmsBot.391.origin», предназначенное для несанкционированного блокирования и модификации компьютерной информации.

2. Каков механизм работы указанного вредоносного программного обеспечения?

После установке на смартфоне под управлением операционной системы Androidono отправляет СМС-сообщения для получения информации о балансе пользователя на лицевом счете оператора связи, электронном кошельке платежной системы Qiwi, банковском счете Сбербанка и отправляет указанные данные и данные о телефоне на удаленный сервер, после чего получает дальнейшие команды, о переводе денежных средств путем отправки СМС-сообщений.

3. Имеются ли сведения об IP-адресах или Интернет-сайтах с которых происходит управление вредоносным программным обеспечением?

Управление вредоносным программным обеспечением осуществляется посредством сайта «[redacted]» (IP-адрес [redacted]).

Примечание: По окончании исследования, представленный носитель информации упакован в первоначальную упаковку. Упаковка опечатана полоской бумаги белого цвета с оттиском печати «НП КПП» сопроводительной надписью и подписью эксперта выполненных красителем черного цвета.

10.08.2015

Приложение Г.

Справка об исследовании по уголовному делу

№ 23042100.Архив Красноярского краевого суда. 2015 год.

ООО "[redacted]"

26.05.2015

Справка об исследовании

Эксперт: Н, имеющий высшее техническое образование по специальности «Системы автоматизированного проектирования», стаж работы в области программного обеспечения и баз данных более 8 лет.

Сертификат курса обучения «Проведение исследований и экспертиз по делам, связанным с нарушением авторского права на программы для ЭВМ».

Сертификат курса обучения "Специалист Microsoft по средствам защиты программных продуктов".

Свидетельство о квалификации "Ассоциации по противодействию компьютерным преступлениям" № СВ-2908/2006-1к.

Сертификат курса обучения "Экспертиза контрафактной продукции" №00020 АНО «СОЮЗЭКСПЕРТИЗА».

Сертификат курса обучения "Отличительные признаки и свойства оригинальной программной продукции ЗАО «1С».

Сертификат о прохождении курса ООО «Аутодеск (Си-Ай-Эс)».

Сертификат о прохождении курса ООО «Адоб Системс» «Специалист Adobe по средствам защиты и лицензирования программных продуктов AdobeSystems».

Сертификат о прохождении курса «CorelCorporation».

На исследование представлено:

2. Компакт-диск DVD+RSony1130531+REC2656.

ВОПРОСЫ ИССЛЕДОВАНИЯ:

5. Имеется ли на представленном носителе информации вредоносное программное обеспечение, заведомо предназначенное для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации?
6. Каков механизм действия указанной программы?
7. Возможно ли восстановить доступ для чтения и редактирования содержимого зашифрованных файлов в оригинальном виде, содержащихся на компакт-диске?

В ходе исследования установлено:

На компакт-диске DVD+RSony 1130531+REC2656 обнаружены:

1. Файлы находящиеся в зашифрованном виде, в название которых добавлены идентификатор «[redacted]» и адрес электронной почты «[redacted]»:

2. Файл скриншота рабочего стола «desk.jpg»:

3. Файл скриншота электронного письма «Письмо.png»

Уважаемые коллеги!

Добрый день.

Настоящим сообщаем Вам, что у вас образовалась дебиторская задолженность,
перед нашей компанией, что подтверждается актом сверки**(во вложении).**
согласно нашему с Вами договору**(во вложении).**
Задолженность необходимо было погасить в течении 10 рабочих дней,
чего не произошло, в случае не подписания акта сверки с оригинальной печатью и подписью Главного бухгалтера .
Мы будем вынуждены написать официальное письмо Генерального директора Вашей компании и обратиться в суд:
Спасибо за понимание!

С Уважением
Главный бухгалтер ООО "Аква"

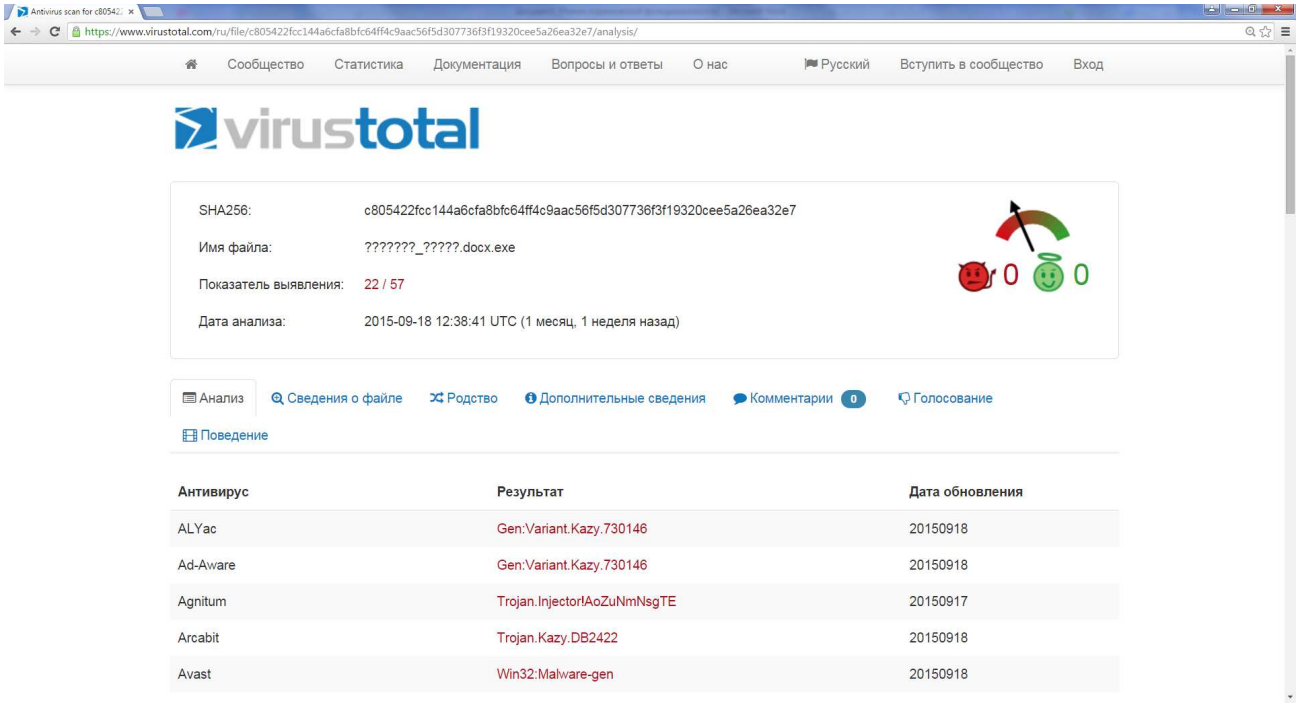
Бочарова Евгения

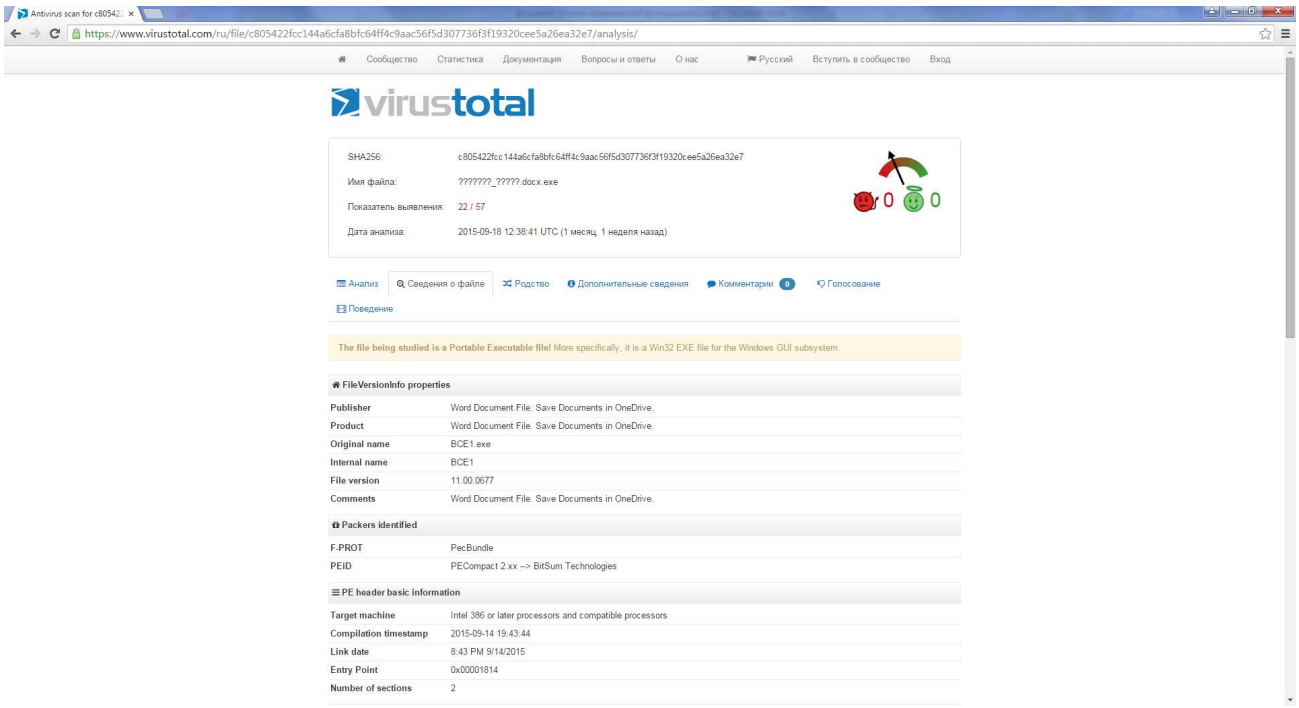
Файлы(2)
Акт_сверки.rar
Договор.rar

4. Архив «Акт_сверки.docx.rar» (пароль для доступа «[redacted]»), содержащий запускаемый файл «Акт_сверки.docx.exe».
5. Каталоги с названиями «Приказы» и «Распоряжения», также содержащие зашифрованные файлы.

В результате анализа файла «Акт_сверки.docx.exe» на Интернет-сервисах, предназначенных для определения алгоритма работы файлов и содержания в них вредоносного программного обеспечения, получена следующая информация:

Virustotal:





Таким образом, данные сервисы идентифицируют указанный файл как вредоносное программное обеспечение типа «Trojan-Ransom.Win32.Crypmod.wjl».

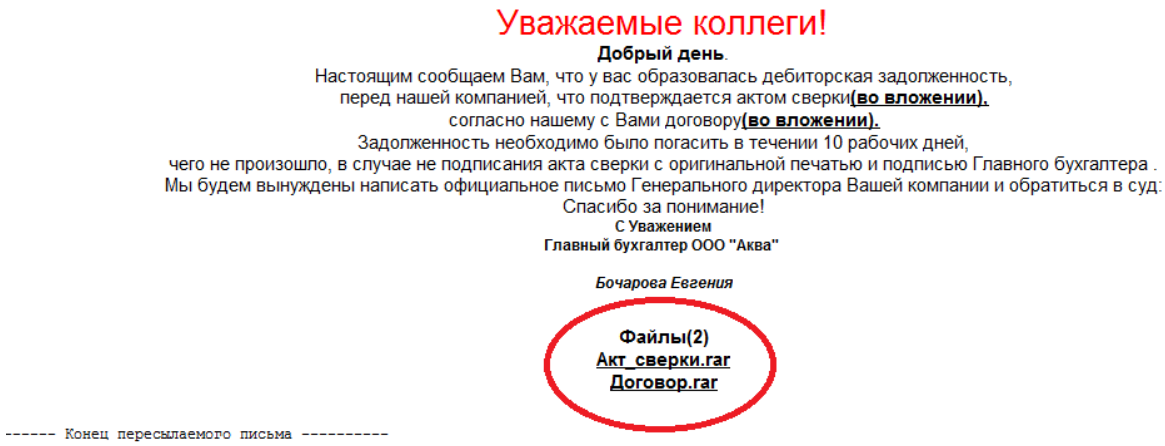
Для определения алгоритма работы указанной программы, файл «Акт_сверки.docx.exe» запущен в программе-песочнице «Sandboxie», позволяющей изолировать область памяти, которая подвергается модификации.

В результате работы программы все файлы с расширениями электронных документов (.doc, .xls и т.д.), содержащиеся в изолированной области памяти оказались зашифрованы, также были изменены названия файлов с добавлением идентификатора и адреса электронной почты:

При этом пользователю не выводились системные или программные сообщения об изменении файлов, т.е. данная модификация файлов осуществлялась несанкционированно, по окончанию работы программы выводится окончательное уведомление пользователю в виде смены рабочего стола пользователя с требованием отправки зашифрованного файла, аналогичного скриншоту в файле «desk.jpg».

Зашифрованные электронные документы, содержащиеся на компакт-диске зашифрованы с использованием неустановленного криптографического алгоритма, при этом получить доступ к содержащейся в них ранее информации невозможно. Их расшифровка, без знания ключа шифрования, известного только лицу осуществившему шифрование, невозможна.

Согласно изображению в файле «Письмо.png», данный файл был получен в результате копирования файла из сети Интернет, при клике пользователя на ссылке указанной в полученном электронном письме:



Уважаемые коллеги!

Добрый день.

Настоящим сообщаем Вам, что у вас образовалась дебиторская задолженность,
перед нашей компанией, что подтверждается актом сверки**(во вложении).**
согласно нашему с Вами договору**(во вложении).**
Задолженность необходимо было погасить в течении 10 рабочих дней,
чего не произошло, в случае не подписания акта сверки с оригинальной печатью и подписью Главного бухгалтера .
Мы будем вынуждены написать официальное письмо Генерального директора Вашей компании и обратиться в суд:
Спасибо за понимание!
С Уважением
Главный бухгалтер ООО "Аква"

Бочарова Евгения

Файлы(2)
Акт_сверки.rar
Договор.rar

------ Конец пересылаемого письма ----------

То есть, файл не был прислан на электронную почту, а прислана была сетевая ссылка для копирования файла, визуально оформленная в виде вложения в письмо.

Выводы

1. Имеется ли на представленном носителе информации вредоносное программное обеспечение, заведомо предназначенное для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации?

На компакт-диске файл «Акт_сверки.docx.rar», содержит вредоносное программное обеспечение, которое определяется антивирусными онлайн-сервисами и антивирусными программами как «Trojan-Ransom.Win32.Crypmod.wjl», которое по алгоритму и результату своей работы, заведомо предназначено для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации

2. Каков механизм действия указанной программы?

Исполняемый файл «Акт_сверки.docx.exe» работает по следующему алгоритму:

1. распространяется посредством электронных писем, в которых содержится ссылка на копирование исполняемого файла с удаленного сервера, находящегося под контролем злоумышленника;
2. запускается по клику пользователя, необходимому для открытия файла;
3. несанкционированно и виузально не определяемо, загружает дополнительные модули необходимые для работы криптографических программ;
4. запускает криптографические программы со сформированным ключем для шифрования;
5. модифицирует криптографическим алгоритмом все электронные документы, фото- и видео-файлы, файлы архивов, файлы баз данных, файлы электронных подписей, при это изменяя их название, добавляя уникальный идентификатор и адрес электронной почты злоумышленника, чем блокирует доступ к информации содердащейся в указанных файлах;
6. отправляет ключ шифрования на командный сервер или адрес электронной почты злоумышленника;
7. удаляет свои исполняемые и служебные файлы, для затруднения идентификации и расшифровки файлов.

3. Возможно ли восстановить доступ для чтения и редактирования содержимого зашифрованных файлов в оригинальном виде, содержащихся на компакт-диске?

Доступ к информации, содержащейся в зашифрованных файлах возможен только при правильной дешифровке исходным алгоритмом криптования и при использовании исходного ключа, который известен только злоумышленнику. Расшифровка антивирусными компаниями или самим владельцем информации без знания данного ключа путем поочередного подбора символов невозможна.

Примечание: По окончании исследования, представленные носители информации упакованы в первоначальную упаковку. Упаковка опечатана полоской бумаги белого цвета с оттиском печати «НП КПП» сопроводительной надписью и подписью эксперта выполненных красителем черного цвета.

26.05.2015

Федеральное государственное автономное
образовательное учреждение
высшего профессионального образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт

Кафедра уголовного процесса и криминалистики

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Д. Назаров
подпись инициалы, фамилия
«14» июня 2017 г.

БАКАЛАВРСКАЯ РАБОТА

_____
код – наименование направления

Способы совершения преступлений в сфере компьютерной информации

Научный руководитель	_____ подпись, дата	доцент, к.ю.н. должность, ученая степень	И.Г. Иванова инициалы, фамилия
Выпускник	_____ подпись, дата		А.С. Нестерова инициалы, фамилия

Красноярск 2017