Содержание:

ВВЕДЕНИЕ

В XX и XXI столетиях произошло развитие наук информатики и кибернетики. Информация стала рассматриваться как одна из составляющих развития материального и духовного мира и восприниматься в качестве нового класса социальных ресурсов. Это ресурс, который, будучи объективной категорией, существует независимо от человека, с одной стороны, но с другой стороны, формируется самим человеком на протяжении истории развития общества, аккумулирует его знания; зависит от деятельности человека и всех форм его ассоциаций; отражает историю и состояние современного мира. Ресурс, обладание, защита и безопасность которого рассматриваются как необходимая составляющая государственного суверенитета. В связи с этим, особое значение приобретают вопросы правового обеспечения информационной безопасности.

Негативным последствием информатизации общества является появление так называемой компьютерной преступности. Особенно остро проблема несанкционированного вмешательства в работу компьютерных систем дала о себе знать в странах с развитой информационной инфраструктурой.

Как известно, современный тренд развития инфо-коммуникационных процессов состоит в обеспечении доступа к любому контенту всех пользователей, независимо от местоположения и используемого устройства. Это неизбежно порождает ряд проблем, связанных с безопасностью. В настоящее время эти проблемы, изначально чисто технические, получают гуманитарное и социальное значение для всех категорий пользователей. Опасным рискам, связанным с реализаций угроз информационного характера, подвержены без исключения все пользователи всех возрастных групп -школьники, студенты, специалисты, руководители организаций. Анализ ситуации многими экспертами по информационной безопасности убедительно показывает, что технологические решения позволяют обеспечить защиту лишь от некоторых опасностей. Многое здесь зависит от человеческого фактора, от участия конкретных пользователей в процессах обмена информацией, от использования ресурсов информационных систем.

Примечательной особенностью компьютерных преступлений является также их транснациональный характер. Уже не имеют большого значения границы между

странами, расстояния, разница в языках общения. Определяющими становятся уровень компьютеризации общества, возможность доступа к компьютерам, соответствующие специальные знания, общие для программистов разных стран.

Проблеме преступлений в сфере компьютерной информации в научной литературе уделено значительное внимание. Вопросы уголовно-правовой оценки преступлений в сфере компьютерной информации рассматривались в работах Ю.М. Батурина, А.М. Жодзишского, А.В. Венгерова, В.Б. Вехова, В.С. Комиссарова В.В. Крылова, В.Д.Курушина, Ю.И. Ляпунова, В.Ю. Максимова, В.А. Минаева, И.В. Никифорова, А.С. Попова, Н.А. Селиванова, А.С. Черных и других. Криминалистические и отдельные криминологические аспекты освещены в исследованиях Д. Айкова, Р.С. Белкина, В.Б. Вехова, П.Б. Гудкова А.Н. Караханьяна, В.В. Крылова, В.А. Мещерякова, Г.Н. Мухина, Н.С. Полевого, С.Г. Спириной, Н.Г. Шурухнова и других ученых.

Цель данной работы – проанализировать технологий совершения компьютерных преступлений.

Для достижения поставленной цели необходимо решить следующие задачи:

- выделить основные черты компьютерных преступлений;
- описать основные виды компьютерных преступлений;
- рассмотреть средства совершения компьютерных преступлений;
- изложить специфику предупреждения компьютерных преступлений.

Работа состоит из введения, четырех глав, заключения и списка литературы.

ОБЩИЕ ЧЕРТЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Существование компьютерной преступности в России и ее качественное развитие в последние годы остается довольно устойчивым, что обусловлено повсеместным применением современных информационных технологий в банковской, торговой, промышленной, научной, образовательной, культурной и других сферах общественной жизни, а также широким использованием компьютерных баз данных, информационно-телекоммуникационных систем в области управления [18].

В российском уголовном законодательстве разделение киберпреступлений на определенные группы (составы) отражено в ряде глав Уголовного кодекса РФ и в первую очередь в главе 28 УК РФ, именуемой «Преступления в сфере компьютерной информации» (статьи 272 - 274 УК РФ) [1].

В ст. 272 УК РФ уголовное наказание предусмотрено за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. Таким образом, предметом преступления является охраняемая законом компьютерная информация. Указанная информация должна находиться на носителе информации (компьютере, мобильном средстве связи) и/или ее программном обеспечении [20, с. 29].

В ст. 273 главы 28 УК РФ уголовная ответственность предусмотрена за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Такое преступление с объективной стороны проявляется в совершении одного из следующих действий:

- создание компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

- использование таких компьютерных программ или такой компьютерной информации;

- распространение таких компьютерных программ или такой компьютерной информации.

В ст. 274 главы 28 УК РФ уголовная ответственность установлена за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации.

При этом следует учитывать, что неправомерный доступ к охраняемой законом компьютерной информации, создание и распространение вредоносных программ являются стадией приготовления или покушения при совершении других преступлений, в первую очередь корыстных.

Помимо статей 272 - 274 УК РФ, уголовная ответственность за совершение преступлений непосредственно с использованием информационных технологий установлена, в частности, в ст. 159.6 «Мошенничество в сфере компьютерной информации», в ст. 159.3 «Мошенничество с использованием платежных карт» и

др. [20, с. 30].

Согласно данным ГИАЦ МВД РФ за последние годы в России было зарегистрировано следующее количество преступлений в сфере компьютерной информации, предусмотренных, статьями 272, 273 и 274 УК РФ (Таблица 1) [4].

Как мы видим из приведенных статистических данных, среди преступлений в сфере компьютерной информации преобладают неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) [1].

Таблица 1 - количество преступлений в сфере компьютерной информации

Год/статья	Ст. 272	Ст. 273	Ст. 274 УК РФ
2010	6132	1010	0
2011	2005	693	0
2012	1930	889	1
2013	1799	764	0

Таблица составлена по данным сайта ГИАЦ МВД РФ [4].

Несмотря на общее снижение количества зарегистрированных преступлений рассматриваемого вида, в данной сфере наблюдается качественная трансформация содержания и сущности компьютерной преступности, что выражается в приобретении ею все более экономического и политического характера. При этом вред, причиняемый российскому обществу преступлениями в сфере компьютерной информации, носит колоссальный характер.

В свою очередь американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 г. в 1 млрд долл., а в 2012 г. - в 1,48 млрд долл. При этом общий ущерб от киберпреступности в мире в 2013 г. составил 113 млрд долл. против 1100 млрд долл. в 2012 г. [6, с. 24].

Цифры аналитиков разнятся, что объясняется, по всей видимости, высокой латентностью компьютерных преступлений, а также отсутствием единой методики расчета вреда, причиненного киберпреступниками.

Компьютерные преступления (computer crime) - это преступления, совершенные с использованием компьютерной информации. При этом компьютерная информация является предметом и (или) средством совершения преступления [16, с. 9].

Уголовное наказание за совершение преступлений в сфере компьютерной информации предусмотрено главой 28-ой УК РФ [1]. Преступными являются следующие виды деяний:

1. Неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК).

2. Создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами (ст. 273 УК).

3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК). Как правило, эти преступления совершаются в совокупности с иными общественно опасными деяниями. Это обусловлено тем, что при использовании компьютерной информации в качестве средства совершения другого преступления, она сама становится предметом общественно опасного деяния. Невозможно противоправно воспользоваться компьютерной информацией не нарушив при этом ее правовой защиты, то есть, не совершив хотя бы одного из действий, перечисленных в п. 1 ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации», а именно: уничтожения, модификации, копирования, блокирования, предоставления и распространения.

Чаще всего компьютерная информация используется для совершения следующих преступлений, расположенных по ранжиру:

1) нарушение авторских и смежных прав (ст. 146 УК);

2) мошенничество (ст. 159 УК);

3) подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков (ст. 327 УК);

4) изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов (ст. 187 УК);

5) изготовление или сбыт поддельных денег или ценных бумаг (ст. 186 УК);

6) причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК) - при незаконном использовании чужого логина и пароля доступа к ресурсам сети «Интернет»;

7) уклонение от уплаты налогов с организаций (ст. 199 УК);

8) нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК);

9) незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК);

10) незаконное распространение порнографических материалов (ст. 242 УК);

11) изготовление и оборот материалов с порнографическими изображениями несовершеннолетних (ст. 242-1 УК);

12) незаконное предпринимательство (ст. 171 УК) [10, с. 26].

Хотя действующее в большинстве стран уголовное законодательство является достаточно гибким, чтобы квалифицировать правонарушения этого типа, социальные и технические изменения создают всё новые и новые проблемы. Поэтому некоторые из известных мировой практике компьютерных посягательств не попадают под действие уголовного законодательства и в юридическом смысле не могут считаться преступными. Так, существует точка зрения, что компьютерных преступлений, как преступлений специфических в юридическом смысле, не существует и следует говорить лишь о компьютерных аспектах преступлений.

Вместе с тем, специалисты в данной области исследований пришли к выводу, что к разряду компьютерных следует отнести те преступления, у которых объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер. По этому пути пошло и российское законодательство.

Следует заметить, что с точки зрения уголовного законодательства охраняется компьютерная информация, которая определяется как информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Вместо термина «компьютерная информация» можно использовать и термин «машинная

информация», под которой подразумевается информация, запечатленная на ма шинном носителе, в памяти электронно-вычислительной машины, системе ЭВМ или их сети. В качестве предмета или орудия преступления, согласно законодательству, может выступать компьютерная информация, компьютер, компьютерная система или компьютерная сеть.

При рассмотрении вопросов о классификации компьютерных преступлений и их криминалистической характеристике целесообразно исходить из определения компьютерного преступления в широком смысле слова. В этом случае под компьютерным преступлением следует понимать предусмотренные законом общественно-опасные деяния, совершаемые с использованием средств ком-пьютерной техники. Правомерно также использовать термин «компьютерное преступление» в широком значении как социологическую категорию, а не как понятие уголовного права.

Парадоксальная особенность компьютерных преступлений состоит в том, что трудно найти другой вид преступления, после совершения которого его жертва не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще компьютерного взлома, мало что утаивая от представителей правоохранительных органов. Психологически этот процесс вполне объясним.

Во-первых, жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты своей репутации) существенно превосходят уже причиненный ущерб.

И, во-вторых, преступник приобретает широкую известность в деловых и криминальных кругах, что в дальнейшем позволяет ему с выгодой использовать приобретенный опыт [5, с. 21].

Рассмотрим виды компьютерных преступлений.

ВИДЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Классификация компьютерных преступлений может быть проведена по различным основаниям. Так, например, можно условно подразделить все компьютерные преступления на две большие категории: преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие

компьютеры как необходимые технические средства. При этом не принимаются во внимание так называемые «околокомпьютерные» преступления, связанные с нарушением авторских прав программистов, незаконным бизнесом на вычислительной технике, а также физическим уничтожением компьютеров и т. п. [7, с. 46]

Одна из наиболее общих классификаций была предложена в 1983 г. группой экспертов Организации экономического сотрудничества и развития. В соответствии с ней выделяются следующие криминологические группы компьютерных преступлений:

- экономические преступления;
- преступления против личных прав и частной сферы;
- преступления против государственных и общественных интересов.

Экономические компьютерные преступления, являются наиболее распространенными. Они совершаются по корыстным мотивам и включают в себя компьютерное мошенничество, кражу программ («компьютерное пиратство»), кражу услуг и машинного времени, экономический шпионаж.

Компьютерными преступлениями против личных прав и частной сферы являются незаконный сбор данных о лице, разглашение частной информации (например, банковской или врачебной тайны), незаконное получение информации о расходах и т.д.

Компьютерные преступления против государственных и общественных интересов включают в себя преступления, направленные против государственной и общественной безопасности, угрожающие обороноспособности государства, а также злоупотребления с автоматизированными системами голосования и т.п.

Подходить к классификации компьютерных преступлений наиболее оправданно с позиций составов преступлений, которые могут быть отнесены к разряду компьютерных. Хотя состав компьютерных преступлений в настоящее время четко не определен, можно выделить ряд видов противоправных деяний, которые могут быть в него включены [3].

Перечислим некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров:

- несанкционированный доступ в корыстных целях к информации, хранящейся в компьютере или информационно-вычислительной сети. Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных. Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.), оказываются беззащитны против этого приёма. Самый простой путь его осуществления – получить коды и другие идентифицирующие шифры законных пользователей. Несанкционированный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы одного пользователя остаются открытыми, то другие пользователи могут получить доступ к не принадлежащим им частям ба данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища одной стены. В таком случае он может проникнуть в чужие сейф похитить все, что в них хранится:
- разработка и распространение компьютерных вирусов. Программы-вирусы обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание;
- ввод в программное обеспечение «логических бомб». Это та программы, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему
- халатная небрежность при разработке, создании и эксплуатации программно-вычислительных комплексов компьютерных сетей приведшая к тяжким последствиям. Проблема небрежности в области компьютерной техники сродни вине по неосторожности использовании любого другого вида техники. Особенностью компьютерных систем является то, что абсолютно безошибочных грамм в принципе не бывает. Если проект практически в области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима;
- подделка и фальсификация компьютерной информации. По-видимому, этот вид компьютерной преступности является одним из наиболее

распространенных. Он представляет собой разновидность несанкционированного доступа с той лишь разницей, что пользоваться им может сам разработчик, причем имеющий достаточно высокую квалификацию. Идея преступления состоит в подле выходной информации с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию [9, с. 233].

К фальсификации информации можно отнести также подтасовку результатов выборов, референдумов и т.п. Если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итого протоколы. Естественно, что подделка информации может следовать и другие, в том числе корыстные цели;

- хищение программного обеспечения. Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения программного обеспечения значительно более сложна. Значительная часть программного обеспечения в России распространяется путём кражи и обмена краденым;
- несанкционированное копирование, изменение или уничтожение информации. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны;
- несанкционированный просмотр или хищение информации из банков данных, баз данных и баз знаний. В данном случае под базой данных следует понимать форму представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ [17].

Сегодня практически все исследователи и специалисты признают, что ситуация с киберпреступностью пока имеет тенденцию к ухудшению. Ещё одна опасная тенденция — всё большая связь между киберпреступностью и организованной преступностью. Можно с уверенностью сказать, что Интернет используется преступными группами уже не только как вспомогательное средство, но и как место и основное средство совершения традиционных преступлений — мошенничеств, краж, вымогательств.

СРЕДСТВА СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Преступления в сфере компьютерной информации всегда совершаются с помощью средств компьютерной техники. Понятие этих средства является комплексным, включающим в себя компьютеры в различных вариантах их исполнения (ноутбуки, планшеты, смартфоны, и т.д.), компьютерные технологии (беспроводные Wi-Fi, Bluetooth, 3G, WiMAX и др.), а также компьютерное программное обеспечение, находящееся в открытом, запрещенном или ограниченном обороте и имеющее различное назначение (разрешенные и бесплатно распространяемые программы, например, Opera, Mozilla Firefox, вредоносные программы, например, SpyEye, Zeus, Carberp и т.д.). Следует отметить, что в настоящее время главную роль при совершении компьютерных преступлений выполняет программное обеспечение, а не аппаратные средства, которые сами по себе обычно не представляют опасности.

Как показывает современная практика, в большинстве случаев компьютерные преступления совершаются путем удаленного доступа по телекоммуникационным сетям с помощью обычной компьютерной техники, на которую устанавливается специальное программное обеспечение [13, с. 114]. Это принципиальное обстоятельство имеет следствия, исключительно важные как для расследования, так и для предотвращения компьютерных преступлений. Так, в непосредственных (бессетевых) способах совершения преступлений аппаратные средства, например аппаратные кейлогеры или скиммеры для негласного съема информации, действуют лишь в отношении конкретного компьютерного устройства. Преступники хорошо знают, что при совершении преступления непосредственным образом остаются традиционные (материальные) следы, по которым можно будет их идентифицировать. Использование вредоносного программного обеспечения при удаленном доступе по информационным сетям позволяет осуществить преступление одновременно в отношении многих компьютеров. При таком доступе преступникам не нужно проникать в помещение, в котором находится объект посягательства, при этом остаются не персонифицируемыми их электронно-цифровые следы. Электронно-цифровые следы всегда образуются и модифицируются в результате опосредованного воздействия компьютерных программ. Специфика этих следов проявляется в том, что 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 т.д. Таким образом, в механизме следообразования нет непосредственного следового контакта с преступником, его физическими и иными особенностями, так как компьютерная программа не несет на себе отпечатка конкретного человека, одни и те же электронно-цифровые следы-последствия могут быть образованы кем угодно. Несмотря на эту специфику, основным источником информации о средствах, применяемых в компьютерном преступлении, остаются именно конкретные следы и вся следовая картина в целом [15, с. 162].

В настоящее время для совершения большинства компьютерных преступлений не требуется наличия средств преступления в виде дорогостоящей компьютерной техники. Практически каждый может найти в сети Интернет бесплатные вредоносные программы, включающие в себя необходимый для совершения преступления алгоритм действий. К таким программам могут прикладываться наглядные инструкции по их использованию. Эти обстоятельства в значительной степени способствуют росту числа совершаемых преступлений в сфере компьютерной информации [13]. Более того, помимо количества преступлений, меняется типичный портрет преступника в сторону лиц, не имеющих специального или высшего образования и постоянной работы [12].

Следственные органы, особенно на первоначальном этапе расследования компьютерных преступлений, редко располагают сведениями о средствах, используемых в преступлении. В отсутствие такой информации имеет важную роль для проведения расследования криминалистическая характеристика аналогичных преступлений. Ее практическое значение, проявляющееся в корреляционной взаимосвязи между структурными элементами преступления, дает основания строить следственные версии на основе использования имеющихся неполных данных.

В компьютерных преступлениях выбор средств для их совершения обычно зависит от целого ряда факторов: объекта посягательства, принятого на нем режима охраны, применяемых технических и организационных средств охраны, программно-аппаратной защиты информации. Так как в большинстве случаев поводом для возбуждения уголовных дел являются заявления потерпевших, то следствию становится известен объект посягательства. Его исследование может пролить свет на способ совершения преступления или примененные преступником программно-аппаратные средства [12].

Анализ судебнаследственной практики показывает, что типичные (относительно простые) или, наоборот, высокотехнологичные способы совершения преступлений могут осуществляться характерными для них программно-аппаратными средствами. Возможна также обратная ситуация, когда данные о средствах преступления известны и помогают строить следственные версии о других искомых элементах преступления. Например, конкретные средства совершения преступления могут указывать на применяемый преступниками способ совершения преступления, а также время и место его осуществления.

Средства, которые используются при совершении преступлений в сфере компьютерной информации, достаточно разнообразны. Важно также, что с криминалистических позиций их можно классифицировать по существенно различным критериям: по законности происхождения; по созданию; по техническому содержанию; по технологии использования; по стадии в преступлении и др. Это обусловливает необходимость разработки системы криминалистической классификации. В целях повышения эффективности расследования компьютерных преступлений разнообразные средства их совершения следует классифицировать, учитывая их основные особенности [15, с. 163].

Предназначенные для полного или частичного управления компьютером и доступа к хранимой на нем информации предлагается прежде всего разграничить на две основные группы - законные и незаконные. Законные (разрешенные для использования) средства могут быть свободно распространяемыми, находиться в ограниченном обороте или быть изъятыми из оборота. Некоторые такие программные средства могут входить в состав операционной системы или устанавливаться самими пользователями дополнительного. Ограниченные в гражданско-правовом обороте средства, например, предназначенные для негласно получения информации путем видеоаудиозаписи, могут быть приобретены при наличии соответствующего разрешения. Использование изъятых из оборота специальных средств может быть разрешено органам оперативно-розыскной деятельности или иным государственным органам (например, следственному комитету, прокуратуре, суду, экспертным учреждениям), однако создавать, владеть, пользоваться и распоряжаться такими средствами гражданам запрещено законом, т.е. их использование гражданами является незаконным.

Преступниками может применяться не только широкий перечень готового программноаппаратного обеспечения, в том числе модифицированного, но и собственные уникальные разработки. Это наиболее характерно для

высокотехнологичных способов совершения компьютерных преступлений, при которых используются компьютерные программы, созданные членами преступной группы или посторонними специалистами по заказу преступников. В этом случае речь идет прежде всего о так называемых шеллах (shell), которые позволяют преступнику выполнять ограниченный круг команд по управлению автоматизированным рабочим местом (например, выполнить какое-либо действие командной оболочки операционной системы и т.п.) [16, с. 59].

По техническому содержанию рассматриваемые средства могут быть условно разделены на аппаратные, программные и программно-аппаратные. При незаконном доступе к объекту посягательства использование чисто аппаратных средств мало распространено, так как современные компьютерные устройства обычно обладают каким-либо собственным программным обеспечением. Как показывает судебно-следственная практика, примерами программно-аппаратных устройств выступают скиммеры и кейлогеры.

Скиммеры используют для кражи реквизитов банковских карт. Как правило, скиммер состоит из двух компонентов - устройства для считывания данных хранящейся на магнитной полосе банковской карты и устройства, позволяющего скопировать пин-код. Некоторые скиммеры оснащены инструментами беспроводной связи, с помощью которой злоумышленники получают информацию в реальном времени, а не хранят ее непосредственно на скиммере. Кей-логеры представляют собой устройства, которые позволяют перехватывать данные, вводимые с клавиатуры. Они выполняются в различных вариантах и могут хранить полученную информацию в собственной памяти или быть оснащены средствами беспроводной связи. Программное обеспечение, используемое для незаконного доступа к компьютерной информации, может быть признано вредоносным только судом. Отметим, что четкого определения вредоносного программного обеспечения в ст. 273 УК РФ не дается, что требует отдельного рассмотрения.

При проведении расследовании целесообразно учитывать, что конкретные средства совершения компьютерных преступлений могут использоваться только на определенных стадиях - подготовки к преступлению, непосредственно при его совершении, при сокрытии преступления, при противодействии следствию в условиях оперативно-розыскных мероприятий или следственных действий. Так, на стадии подготовки преступники изучают обстановку объекта посягательства, физический режим его охраны (замки, контроль сотрудниками, видеонаблюдение, сигнализацию), пытаются собрать информацию о действующих устройствах и программах информационной безопасности (системах идентификации и

аутентификации), готовят хранилища для переноса охраняемой информации (flash носители, облачные хранилища и пр.), средства сокрытия и уничтожения следов своей деятельности (например, размагничивание жесткого диска). На этой стадии могут применяться специальные программы, исследующие и оценивающие объект посягательства с точки зрения его защищенности внешним угрозам (например, программы-шпионы типа Zeus). Непосредственно на этапе совершения преступления соответствующие средства направлены на получение преступником возможности управлять автоматизированным рабочим местом потерпевшего. Для получения неправомерного доступа преступники могут использовать программы, предназначенные для администраторов (TeamViewer, Radmin, TightVNC и т.п.), специализированные клиенты сетевых протоколов RDP (Remote Desktop Protocol) или VNC (Virtual Network Computing), имеющие собственный web-интерфейс для администрирования и управления, либо модификации вредоносного программного обеспечения, например Zeus, Carberp и т.п. [14, с. 124].

Опасной разновидностью вредоносного программного обеспечения, позволяющего получить неправомерный доступ к автоматизированному рабочему месту, являются эксплойты, под которыми понимается программный код или его фрагмент, который через ошибки в каком-либо программном обеспечении, работающем на объекте посягательства, приводит к выполнению этим программным обеспечением действия, непредусмотренного разработчиками. При попытке массового заражения рабочих мест через использование web-сервисов применяются инструменты, которые включают в себя наборы эксплойтов, нацеленные на эксплуатацию ошибок в web-браузерах и различного рода расширений к ним (Adobe Flash, ActiveX и т.п.) [13, с. 115].

Сокрытие преступления, отдельных следов-последствий и участия в нем преступника может реализовываться во время совершения преступления и после него. Для этой цели могут применяться различные элементы маскировки, например: программно-аппаратный сбой, противоправные действия иных лиц и многое другое. Отметим, что для сокрытия электронно-цифровых следов может применяться не только вредоносное, но и законное программное обеспечение, например, позволяющее безвозвратно удалять информацию с носителя путем многократной ее перезаписи. Как правило, сокрытие сводится к попытке затруднить определение местонахождения преступников. Подобная цель может достигаться путем использования сервисов, позволяющих осуществить подмену реального IP-адреса на другой. Популярностью у преступников пользуются услуги предоставления доступа к сети, работающей по протоколу VPN. Современные VPN-

сервисы предоставляют доступ к сети путем использования цепочки промежуточных серверов (Double/Triple-VPN), что значительно затрудняет определение реального IP-адреса преступника. В случаях, когда не требуется высокая пропускная способность канала связи, преступник может отдать предпочтение таким технологиям, как Tor, ввиду бесплатного предоставления анонимности при работе в телекоммуникационных сетях [14, с. 125].

Таким образом, исследование средств совершения компьютерных преступлений с позиций криминалистики, их типизация и классификация позволяют установить корреляционные связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

ПРЕДУПРЕЖДЕНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Названные и иные особенности компьютерных преступлений обусловливают потребность и в соответствующих мерах защиты от такого рода посягательств. Настоящие меры возможны, как нам представляется, двух видов: во-первых, меры, которыми располагает субъект, предупредительного воздействия в отношении угрозы информационного посягательства на охраняемые уголовным законом права и свободы личности; во-вторых, меры, предпринимаемые самой личностью. Определение реальных мер обеспечения криминологической безопасности личности в информационной сфере невозможно без учета характеристик самого этого феномена — безопасности.

Всем уже давно известно, что неразглашение внутренней информации совсем неэффективно. Необходимо применять меры, основной составляющей которых является защита компьютеров, принадлежащих компаниям, от несанкционированного копирования и выведения данных.

Необходимо внедрять программы с помощью которых производится мониторинг всех действий, осуществляемых на компьютерах сотрудников фирмы. Необходимо отслеживать любые движения корпоративных данных, их копирование и вывод на внешние носители. Таким образом, службы безопасности компаний имеют

возможность моментально реагировать и пресекать любые несанкционированные действия, связанные с копированием информации [10, с. 69].

Ошибки в работе и выход из строя компьютерных систем могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся наиболее актуальными на сегодняшний день. Известно много мер, направленных на предупреждение преступления. Необходимо наиболее эффективно использовать всевозможные подходы к сохранению конфиденциальной информации с целью сохранения информационной целостности организации.

В настоящее время можно выделить две основные группы мер предупреждения компьютерных преступлений: правовые; организационно-технические.

Правовые. В эту группу мер предупреждения компьютерных преступлений, прежде всего, относят нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере.

Организационно-технические. Основные положения защиты информации по ряду базовых позиций предполагают: предотвращение утечки, хищения, утраты, искажения и подделки информации; предотвращение угроз безопасности личности, общества и государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и системы; обеспечение правового режима функционирования документированной информации как объекта собственности; сохранение государственной тайны и конфиденциальности документированной информации; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

По методам применения тех или иных организационно-технических мер предупреждения компьютерных преступлений специалистами отдельно выделяются три их основные группы 1) организационные; 2)технические; 3) комплексные (сочетающие в себе отдельные методы двух первых групп).

Организационные меры защиты средств компьютерной техники (СКТ) включают в себя совокупность организационных мероприятий: по подбору, проверке и инструктажу персонала, участвующего на всех стадиях информационного процесса; по разработке плана восстановления информационных объектов после выхода их из строя; по организации программно-технического обслуживания СКТ;

по возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных СКТ; по осуществлению режима секретности при функционировании компьютерных систем; по обеспечению режима физической охраны объектов; по материально-техническому обеспечению и т. д.

Технические меры представляют собой применение различных устройств специального назначения: источники бесперебойного питания, устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находится компьютерная техника, устройства комплексной защиты телефонии, устройства пожарной защиты, средства защиты портов компьютера, также для защиты программного обеспечения нужно ввести параметры доступа в компьютер.

Доступ может быть определен как: общий (безусловно предоставляемый каждому пользователю); отказ (безусловный отказ, например, разрешение на удаление порции информации); зависимый от события (управляемый событием), предусматривает блокировку обращения пользователя, например, в определенные интервалы времени или при обращении к компьютерной системе с определенного терминала; зависимый от содержания данных (в этом случае решение о доступе основывается на текущем значении данных, например, некоторому пользователю запрещено читать те или иные данные); зависимый от состояния (динамического состояния компьютерной системы), осуществляется в зависимости от текущего состояния компьютерной системы, управляющих программ и системы защиты, например, может быть запрещен доступ к файлу, если носитель машинной информации не находится в состоянии «только чтение» либо пока не будет открыт логический диск, содержащий этот файл; частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз - таким образом, предотвращается возможность динамического управления событиями); по имени или другим признакам
пользователя (например, пользователю должно быть более 18 лет); зависимый от полномочий (предусматривает обращение пользователя к данным в зависимости от режима: только чтение, только выполнение и т. д.) [11, с. 56]

Залог успеха предотвращения компьютерной преступности заключается в реализации всех перечисленных выше мер и методов защиты информации и программных средств. Все данные меры позволят решить проблему незаконного доступа и помешают злоумышленнику завладеть чужими конфиденциальными реквизитам.

ЗАКЛЮЧЕНИЕ

В заключении подведем итоги. Компьютерная преступность (преступление с использованием компьютера) - представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует.

Информационные и телекоммуникационные технологии - это новые орудия труда, использование которых определило необходимость правовой оценки различных ситуаций и разработку организационно-правовых механизмов предотвращения и профилактики общественно опасного поведения в данной области.

Преступления, связанные с различными информационными процессами, хищение информации буквально в течение десятилетия превратились из зарубежной и даже книжной «экзотики» в реальную угрозу для всех членов общества. Необходимо также учитывать, что Россия в течение крайне малого исторического промежутка времени перенесла ряд практически революционных изменений во всех сферах жизнедеятельности, в том числе и в сфере государственного устройства, которые, впрочем, продолжаются и сейчас.

Невозможно не принимать во внимание тот факт, что Россия вступила в эпоху существования информационного общества и сама становится информационным обществом. Наряду с традиционными материальными благами национальное богатство, богатство государства и отдельных людей стала составлять информация, в том числе связанная с высокими технологиями. Ценность информации, которой обладают отдельные юридические или физические лица, сравнима, а иногда и превосходит ценность принадлежащих им материальных благ (назовем для примера основных производителей компьютерных программ).

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы информационно-телекоммуникационных сетей, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов,

иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям и даже, как бы невероятно это ни звучало, с убийством.

В нынешних условиях особую актуальность приобретает необходимость обеспечения информационной безопасности государства во всех направлениях обеспечения национальных интересов Российской Федерации.

Решение проблем грамотного правового регулирования усложняющихся и возникающих новых криминализированных общественных отношений возможно только на основе всестороннего анализа складывающейся ситуации в сфере борьбы с киберпреступностью, адекватно-комплексного подхода к определению путей их решения. Без проведения такой работы предпринимаемые законотворческие шаги, даже самые активные, будут и в дальнейшем способствовать включению в уголовное законодательство норм (отдельных новых статей), применение которых на практике не будет востребовано. К тому же их количество не перерастет в качество и, следовательно, не обеспечит создание реального правового механизма по активному противодействию киберпреступности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 01.05.2016) // Собрание законодательства РФ. – 1996. – № 25. – ст. 2954.
2. Борчева Н.А. Компьютерные преступления в России: Коммент. к Уголовному кодексу РФ / Н. А. Борчева. - М.: ИНФРА-М, 2011. – 120 с.
3. Воробьёв В.В. О предмете преступления, его месте в составе преступления и особенностях в компьютерных преступлениях / В.В. Воробьев // Символ науки. 2015. №6. URL: http://cyberleninka.ru/article/n/o-predmete-prestupleniya-ego-meste-v-sostave-prestupleniya-i-osobennostyah-v-kompyuternyh-prestupleniyah Дата обращения: 19.05.2016
4. Данные ГИАЦ МВД РФ о состоянии преступности в России // Министерство внутренних дел Российской Федерации URL: http://mvd.ru/presscenter/statistics/reports/ Дата обращения: 18.05.2016.
5. Дворецкий М.Ю. Преступления в сфере компьютерной информации: Научно-практический комментарий к гл. 28 Уголовного кодекса РФ / М.Ю. Дворецкий.

М., 2010. – 60 с.
6. Евдокимов К.Н. Актуальные вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации / К.Н. Евдокимов // Российский следователь. - 2015. - № 10. - С. 24 – 29.
7. Евдокимов К.Н. Политические факторы компьютерной преступности в России / К.Н. Евдокимов // Информационное право. - 2015. - № 1. - С. 41 - 47.
8. Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере: монография / А.К. Жарова. - М.: Янус-К, 2016. - 248 с.
9. Иванов В.Ф. Медиабезопасность в информационном обществе / В.Ф. Иванов // Вестник ЧелГУ. - 2013. - №21 (312). – С. 233-243.
10. Крылов В.В. Информационные компьютерные преступления: Учеб. и практ. пособие /В.В. Крылов. М., 2012. – 160 с.
11. Лопатин Д.В Анализ информационно-коммуникационных угроз для пользователей / Д.В. Лопатин // Вестник Тамбовского университета. Серия: Естественные и технические науки. - 2012. - №5. – С. 55-59.
12. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» (утв. Генпрокуратурой России) URL: http://genproc.gov.ru Дата обращения 18.05.2016.
13. 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.
14. Поляков В.В. Характеристика высокотехнологичных способов совершения преступлений в сфере компьютерной информации: матер. ежег. Всерос. науч.-практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета «Уголовнопроцессуальные и криминалистические чтения на Алтае» / В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2012. - Вып. 11-12. - С. 123-126.
15. Поляков В.Л. Средства совершения компьютерных преступлений / В.Л. Поляков // Доклады ТУСУР. - 2014. - №2 (32). – 162-165.
16. Проблемы предупреждения преступности в сфере высоких технологий: Сб. науч. ст. / Отв. ред. А.Н. Тарбагаев. Красноярск РУМЦ ЮО, 2010. - 95 с.
17. Российская Федерация: 21-й век. Юридическая безопасность страны и ее граждан в правовом государстве (По материалам научно-практической конференции) // Государство и право. 2009. - № 10. - С. 95.

18. Степанов-Егиянц В.Г. Субъективная сторона компьютерных преступлений / В.Г. Степанов-Егиянц // Бизнес в законе. - 2013. - №2. URL: http://cyberleninka.ru/article/n/subektivnaya-storona-kompyuternyh-prestupleniy Дата обращения: 19.05.2016.
19. Третьяк М. Правила квалификации компьютерного мошенничества и преступлений, предусмотренных гл. 28 УК РФ // Уголовное право. 2014. N 4. С. 69 - 74.
20. Чекунов И.Г. Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества / И.Г. Чекунов // Российский следователь. - 2015. - № 17. - С. 29 - 33.