МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

 **«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Кафедра бухгалтерского учета, аудита и автоматизированной**

**обработки данных**

**РЕФЕРАТ**

**КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ**

Работу выполнила И.С.Озерцова

 (подпись, дата)

Факультет экономический курс 5

Специальность/направление Экономическая безопасность (Экономико-правовое обеспечение экономической безопасности)

Научный руководитель

Доц., канд.экон.наук, доц. Т.Г.Белозерова

 (подпись, дата)

Краснодар 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ ..3

1 Понятие и виды компьютерных преступлений ..5

 1.1 Понятие компьютерных преступлений ..5

 1.2 Виды компьютерных преступлений ..6

2 Компьютерные преступления: ответственность и предупреждение 12

2.1 Ответственность за компьютерные преступления 12

2.2 Предупреждение компьютерных преступлений ..16

ЗАКЛЮЧЕНИЕ ..25

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ ..26

ВВЕДЕНИЕ

В современном мире одной из наиважнейших проблем является проблема развития компьютерной преступности. Научно-техническая революция конца 20-го века привела к широкому использованию информационных технологий и зависимости общества от распространяемой информации через средства глобальной сети Интернет [8].

Актуальность рассматриваемой проблемы в том, что компьютерная преступность становится одним из наиболее опасных видов преступных посягательств. Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных, и, прежде всего, вычислительных систем.

Изучение проблем расследования преступлений в сфере компьютерной информации выступает одной из острейших задач современной криминалистической науки. Несмотря на то, что в последние годы в криминалистической литературе уделяется повышенное внимание методике расследования компьютерных преступлений, в этой области еще остается ряд нерешенных и дискуссионных вопросов

Целью работы - является раскрытие понятия компьютерной преступности, выявление мер контроля над компьютерной преступностью, направленности действий комплекса факторов, снижающих ее эффективность. А также выработка всесторонней стратегии по профилактике и борьбе с компьютерной преступностью, и формулирование предложений повышения эффективности контроля над компьютерной преступностью.

Для достижения поставленной цели следует решить ряд задач:

1. Рассмотреть понятие компьютерных преступлений.
2. Изучить виды компьютерных преступлений.
3. Ознакомиться с ответственностью за компьютерные преступления.
4. Узнать как предупредить компьютерные преступления.

 Объект исследования составляет правовой аспект уголовной ответственности за компьютерную преступность.

 Предметом исследования является компьютерная преступность как современная криминологическая проблема.

 В настоящем исследовании были использованы следующие методы: анализ научных концепций, синтез научных знаний на основе обобщения фактических данных, логический метод.

 Структура работы обусловлена ее целью и задачами, содержанием, взаимосвязью рассмотренных в работе проблем и соответствует логике проведенного исследования. Она состоит из введения, двух основных глав, заключения. В конце работы приведен список литературы, использованный при ее написании, включающий 17 источников.

 1 Понятие и виды компьютерных преступлений

 1.1 Понятие компьютерных преступлений

 Компьютерное преступление — противозаконная деятельность, связанная с информационными ресурсами, при которой компьютер выступает либо как объект совершения преступления, любо как субъект непосредственного воздействия [18].

 Главная особенность компьютерных преступлений – это сложность в установлении состава преступления и решении вопроса о возбуждении уголовного дела. Компьютерная информация способна достаточно быстро изменять свою форму, копироваться и пересылаться на любые расстояния. Следствием этого являются трудности с определением первоисточника и субъекта совершения преступления.

 Преступники в области информационных технологий – это не только высококвалифицированные специалисты в области компьютерной техники и программирования. Зачастую субъектами компьютерных преступлений становятся обычные пользователи ПК, которые в силу недостаточного знания техники или желания бесплатно воспользоваться какой-либо программой, совершают незаконные действия, сами того не подозревая. По статистике из каждой тысячи киберпреступлений, только семь совершаются профессионалами, которые характеризуются многократностью применения противоправных действий с целью достижения корыстных целей, а также непременным сокрытием состава преступления [119].

 Информация как криминалистический объект имеет ряд специфических свойств: высокая динамичность, постоянное функционирование, возможность дистанционной работы и, безусловно,- возможность быстрого изменения и безвозвратного удаления большого объема данных. Последняя особенность является ключевой в понимании сущности компьютерных преступлений. Ведь, получив доступ к информации, киберпреступник может использовать все известные ему средства для манипулирования поведением объекта преступления [56].

 Особого внимания заслуживает сеть Интернет как средство распространения компьютерных преступлений. Очевидно, что возможности сети Интернет безграничны. Каждый может прочитать интересную статью, посмотреть фильм, послушать музыку, скачать необходимую программу или же посидеть в социальных сетях. Общество становится зависимым от сети Интернет и попросту не представляет свою жизнь без него. Этим охотно пользуются компьютерные преступники, внедряя всевозможные мошеннические программы в объекты, пользующиеся особой популярностью.

 Огромную опасность представляют собой преступления, совершаемые через сеть Интернет в сфере государственных организаций, правительственных учреждений, экономики и операций на бирже, а также операций с денежными средствами обычных граждан.

 Использование услуг банков через сеть Интернет таит в себе огромный риск: возможность безвозмездного перевода финансов на счет злоумышленника. Именно поэтому следует особенно внимательно относиться к безопасности используемых программных обеспечений и использовать только проверенные сайты и программы, при этом периодически бороться с компьютерными атаками и предотвращать возможность их возникновения [97].

 1.2 Виды компьютерных преступлений

Компьютерные преступления – это преступления, связанные с незаконной эксплуатацией компьютерных и коммуникационных технологий для преступной деятельности. И в то время как эволюционирующие технологии подаются как благо для человечества, разрушительно направленный человеческий интеллект может превратить эти технологии в проклятие [16].

Для более детального понимания составим рисунок видов компьютерных преступлений.

Виды компьютерных преступлений

 Взлом

 Фишинг

 Компьютерные вирусы

 Электронный спам

 Киберпреследование

К Кража личных данных

 Кибервымогательство

 Кибервойны

Рисунок 1 «Виды компьютерных преступлений»

Рассмотрим подробнее каждый вид и его отличительные особенности.

Взлом.

Получение несанкционированного доступа к данным, через компьютерные системы называется взломом. Также взломом называется несанкционированное отключение безопасности компьютерной системы с целью получения несанкционированного доступа к хранящейся на ней информации. Несанкционированное раскрытие паролей с намерением получить несанкционированный доступ к частной организации или пользователю является одним из самых широко известных компьютерных преступлений. Другим весьма опасным компьютерным преступлением, является использование данных IP-адресов, чтобы взломать компьютер и совершить операции под вымышленным именем, при этом оставаясь анонимным при совершении преступления [16].

Фишинг.

Фишинг - это попытка завладеть конфиденциальной информацией, такой как имена пользователей, пароли и данные кредитной карты, которая выглядит как источник, заслуживающий доверия. Фишинг осуществляется через электронную почту или путем заманивания пользователя вводить личную информацию через поддельные веб-сайты. Преступники часто используют веб-сайты, которые имеют внешний вид некоторых популярных веб-сайтов, которые позволяют пользователям чувствовать себя безопасно и вводить там свои данные [18].

Компьютерные вирусы.

Компьютерные вирусы - это компьютерные программы, которые могут размножаться и нанести вред компьютерным системам по сети без ведома пользователей системы. Распространяются вирусы на другие компьютеры через сетевые файловые системы, сети, Интернет, или посредством съемных устройств, таких как USB-накопители и компакт-диски. Компьютерные вирусы-это формы вредоносных кодов, написанных с целью нанесения вреда компьютерной системе и уничтожения информации. Написание компьютерных вирусов - это преступная деятельность которая может привести к сбою компьютерных систем, тем самым уничтожая огромное количество важных данных [25].

Киберпреследование.

Использование коммуникационных технологий, главным образом Интернета, с целью преследования лиц, известно, как киберпреследование. Ложные обвинения, угрозы, и повреждение данных и оборудования подпадают под класс деятельности киберпреследования. Это преследование часто осуществляются злоумышленниками посредством чатов, интернет-форумов и веб-сайтов социальных сетей для сбора информации о пользователях и изводят своих жертв на основе собранной информации. Непристойные письма, оскорбительные телефонные звонки, и другие такие серьезные последствия киберпреследования сделали его компьютерным преступлением [30].

Кража личных данных.

Это одна из самых серьезных фальсификаций, когда происходит хищение денег и получение других благ через использование фальшивого удостоверения. Это действие, когда злоумышленник притворяясь кем-то другим, использует чужую личность как свою собственную. Финансовые хищения личных данных предполагает использование фальшивого удостоверения для получения товаров и услуг и коммерческие кражи идентичности является использование чужого названия фирмы или кредитной карты в коммерческих целях. Клонирование личности - это использование информации другого пользователя выдавая себя за ложного пользователя [34].

Кибервымогательство.

Когда хакеры угрожают или вредят веб-сайту, серверу или компьютерной системе с помощью отказа в обслуживании или других атак на уязвимую систему с целью шантажа, называется кибервымогательством. Многие корпоративные веб-сайты и сети регулярно подвергаются таким атакам. Правоохранительные органы получают около 20 случаев каждый месяц, и многие другие остаются незарегистрированными [4].

Кибервойны.

Кибервойна определяется как действие государства по проникновению в компьютеры или сети другого государства, с целью нанесения ущерба или разрушения. Она может быть в виде кибер-шпионажа или для получения критически важных секретов для обеспечения безопасности страны. Мотивы получения конфиденциальной информации могут быть политическими, военными, или экономическими. Нарушения транспортных или коммуникационных систем в государстве, незаконная эксплуатация компьютеров или спутниковых технологий - это тоже форма кибервойны. Кибератаки могут быть использованы для создания помех финансовым операциям в стране, тем самым ставя под угрозу ее экономику. Многие страны включают защиту от кибервойн в их военную стратегию [9].

Электронный спам.

Это относится к использованию электронных систем обмена сообщениями для отправки нежелательных сообщений пользователям. Вредоносные веб-сайты отправляют повторные сообщения нескольким пользователям, через электронную почту, мессенджеры, новостные группы, форумы, блоги и др. Сообщения могут содержать вредоносное ПО в виде исполняемых файлов или скриптов, или при нажатии на письма, может направить пользователя на подозрительные сайты [4].

Компьютер, или, скорее, Интернет может быть использован для выполнения незаконной практики, такой как торговля наркотиками. Интернет коммуникационные системы, такие как электронная почта используются для отправки зашифрованных сообщений, связанных с оборотом наркотиков. Доставка лекарственных средств и платежи осуществляются через интернет. С помощью интернета, не требуя очного общения, люди могут найти его как удобный способ продажи или покупки лекарств онлайн. Киберзапугивание делается с использование социальных сетей и других веб-сайтов, чтобы запугивать пользователей, в частности детей и подростков. Это может быть связано с распространением ложной информации о чем-либо, или оскорбление кого-то нарочно, чтобы создать ненависть или негативные чувства о нем среди людей. Это может включать отправку сообщений непотребного содержания, унижающие сообщения, нецензурные изображения, видео и др. Взлом сетей с намерением отключения безопасности или остановка экономических систем является уголовным преступлением. Коммуникационные системы могут быть выведены из строя, сети осуществляющие финансовые операции могут быть атакованы, или компьютерные системы, которые хранят важные данные могут быть повреждены. Эти мероприятия используют компьютерные системы как средства для правонарушений. Они являются частью информационной войны [16].

2 Компьютерные преступления: ответственность и предупреждение

2.1 Ответственность за компьютерные преступления

Ситуация, сложившаяся в сфере информационных технологий, потребовала принятия норм уголовного права, которые предусматривали бы ответственность за совершение преступлений в сфере компьютерной информации.

Это и нашло воплощение в новом Уголовном кодексе РФ. Глава 28 "Преступления в сфере компьютерной информации" содержит три статьи: "Неправомерный доступ к компьютерной информации" (ст.272), "Создание, использование и распространение вредоносных программ для ЭВМ" (ст.273), "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети" (ст.274).

Статья 272 защищает компьютерную информацию любых предприятий, учреждений, организаций и частных лиц. Диспозиция соответствующей нормы заключается в неправомерном доступе к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Неправомерным является доступ, противоречащий действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регулирующим отношения по доступу лиц (группы лиц) к информации. Кроме того, неправомерным будет доступ, если лицо незаконно использовало технические средства для проникновения в ЭВМ и (или) ее сеть, например введение чужого пароля либо снятие необходимого пароля, модификация программы и пр.

Понятие "охраняемая законом компьютерная информация" весьма расплывчато и охватывает практически всю информацию на машинном носителе. Охраняется она достаточно широким кругом законодательных актов: Конституцией Российской Федерации, Гражданским кодексом РФ, законами Российской Федерации "О государственной тайне", "О правовой охране программ для электронных вычислительных машин и баз данных", "Об информации, информатизации и защите информации", "О рекламе","О банках и банковской деятельности".

И если информация не является объектом охраны одного из этих актов, то, как правило, она становится объектом охраны другого. Неохраняемой же информации практически нет.

Необходимое условие наступления уголовной ответственности по ст.272 УК РФ: неправомерный доступ должен влечь за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Необходимо, конечно, отличать уголовное преступление от дисциплинарного проступка. Например, не будут являться преступлением действия работника, нарушившего установленный приказом по предприятию порядок пользования компьютером вне каких-либо корыстных целей.

Диспозиция ч.2 ст.272 УК РФ устанавливает, что предусмотренное ч.1 деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, влечет за собой повышенную ответственность.

Субъект преступления по ст.272 УК РФ - вменяемое физическое лицо, достигшее 16-летнего возраста.

С субъективной стороны преступление характеризуется наличием прямого умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и желание их наступления) или косвенного умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и сознательное допущение их наступления либо безразличное отношение к наступлению последствий).

Не признается преступлением доступ к информации без намерения совершить общественно опасное деяние (техническая помощь пользователю не допущенным к ЭВМ работником, выполнение работы за другое лицо с целью ускорения производственного процесса, непроизвольный доступ к информации вследствие ошибки непосредственного пользователя и т.п.).

Предмет преступления - компьютерная информация. Объект - общественные отношения, связанные с ее безопасностью. Объективная сторона - действие, направленное на неправомерный доступ к компьютерной информации.

Норма права, закрепленная ст.273 УК РФ, направлена на защиту ЭВМ, информации, имущественных интересов пользователя от так называемых компьютерных "вирусов".

Диспозиция ст.273 УК РФ состоит, в частности, в создании программ ЭВМ или внесении изменений в существующие программы, заведомо (здесь: направленно, умышленно) приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы. ЭВМ или их сети, а равно использование либо распространение этих программ или машинных носителей с такими программами.

Состав данного преступления (ч.1 ст.273 УК РФ) формальный (т.е. для того чтобы преступление считалось оконченным, достаточно самого факта "действия", независимо от наступления последствий). Хотя определенные негативные последствия: уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ или их сети - при совершении указанных действий заведомо неизбежны.

Под уничтожением информации понимается лишение сведений, данных и пр. соответствующей материальной формы. Например, преступлением будут являться действия лица, посредством вредоносной программы уничтожившие (стершие и т.п.) информацию, содержавшуюся на магнитном носителе, даже если она имеется на другом носителе, в иной компьютерной сети.

Под блокированием понимается лишение возможности правомерного пользователя реализовать информацию ЭВМ по назначению.

При определении терминов "модификация", "копирование" необходимо использовать понятия, установленные Законом Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных".

Предусмотрено, что ответственность наступает лишь при несанкционированном наступлении негативных последствий, поскольку уничтожение, блокирование и пр. могут проводиться и в разрешительном порядке в тех или иных целях.

Предмет и объект этого преступления - компьютерная информация и (или) компьютерное оборудование; общественные отношения, связанные с безопасностью информации. Объективная сторона - действие, направленное на создание, использование и распространение вирусных программ.

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

Субъективная сторона этого преступления - прямой умысел. Во второй части этой статьи предусмотрена ответственность за те же деяния, повлекшие за собой по неосторожности тяжкие последствия.

При этом "тяжкие последствия" - оценочная категория, которая подлежит квалификации судом. Согласно п.8 постановления Пленума Верховного Суда Российской Федерации от 29 апреля 1996 г. N 1 суд, признавая подсудимого виновным в совершении преступления по признакам, относящимся к оценочным категориям (тяжкие или особо тяжкие последствия, крупный или значительный ущерб, существенный вред, ответственное должностное положение подсудимого и др.), не должен ограничиваться ссылкой на соответствующий признак, а обязан привести в описательной части приговора обстоятельства, послужившие основанием для вывода о наличии в содеянном указанного признака.

Последствия могут быть признаны тяжкими в случае, например, причинения особо крупного материального ущерба, аварий, искажения информации, составляющей государственную тайну.

Нормы, предусмотренные ст.274 УК РФ, устанавливают ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Часть 1 ст.274 УК РФ предусматривает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Условием ее наступления является причинение деянием существенного вреда.

Объективная сторона - прямой умысел. Ответственность по ч.2 ст.274 УК РФ наступает в случае причинения тем же деянием по неосторожности тяжких последствий.

Очевидно, что введение уголовной ответственности за компьютерные преступления - необходимое, но недостаточное условие для эффективной борьбы с ними.

Наряду с уголовно-правовой, гражданско-правовой и административно-правовой охраной программного обеспечения ЭВМ существенным элементом в искоренении такого рода правонарушений стало бы создание специальных подразделений (в рамках правоохранительных органов) по борьбе с компьютерной преступностью, в частности хищениями, совершаемыми путем несанкционированного доступа в компьютерные сети и базы данных.

2.2 Предупреждение компьютерных преступлений

Почти все виды компьютерных преступлений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать различные профилактические меры. В данном случае профилактические меры следует понимать как деятельность, направленную на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению. В нашей стране разработкой методов и средств предупреждения компьютерных преступлений занимается криминалистическая наука. Это наука о закономерностях движения уголовно-релевантной информации при совершении и расследовании преступлений и основанных на них методах раскрытия, расследования и предупреждения преступлений[64].

В настоящее время можно выделить две основных группы мер предупреждения компьютерных преступлений.

1. Правовые

В эту группу мер предупреждения компьютерных преступлений прежде всего относят нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере. Если обратиться к истории, то мы увидим, что первый нормативно- правовой акт такого типа был принят американскими штатами Флорида и Аризона в 1978 году. Этот закон назывался «Computer crime act of 1978». Затем почти во всех штатах Америки были приняты аналогичные законодательства. Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения компьютерных преступлений. Что же касается нашей страны, то первым шагом в этом направлении можно считать Федеральный Закон «О правовой охране программ для ЭВМ и баз данных» от 23 сентября 1992 года. Аналогичные законы в зарубежных странах были приняты на 5-10 лет раньше. 20 и 25 января 1995 года Федеральным Собранием были приняты 2 закона соответственно: «О связи» и «Об информации, информатизации и защите информации». Эти правовые акты явились прогрессивным шагом в развитии данного направления, они:

1. Дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны

2. Устанавливают и закрепляют права и обязанности собственника на эти объекты

3. Определяют правовой режим функционирования средств информационных технологий

4. Определяют категории доступа определенных субъектов к конкретным видам информации

5. Устанавливают категории секретности данных и информации

6. Дают определение и границы правового применения термина «конфиденциальная информация»

Аналогичные законы действуют в западных странах уже более 20 лет.

Решающим законодательным аккордом в этой области можно считать принятие в июне 1996 года Уголовного кодекса РФ, устанавливающего уголовную ответственность за компьютерные преступления. Информация в нем – объект уголовно-правовой охраны.

2. Организационно-технические меры предупреждения компьютерных преступлений.

Организационно-технические меры предупреждения компьютерных преступлений, применяемые в развитых зарубежных странах.

В настоящее время руководство профилактикой компьютерных преступлений в этих странах осуществляется по следующим направлениям:

1) соответствие управленческих процедур требованиям компьютерной безопасности;

2) разработка вопросов технической защиты компьютерных залов и компьютерного оборудования;

3) разработка стандартов обработки данных и стандартов компьютерной безопасности;

4) осуществление кадровой политики с целью обеспечения компьютерной безопасности;

Например, национальным бюро стандартов США были разработаны базовые требования безопасности, предъявляемые к компьютерным сетям. В их числе:

— пригодность — гарантия того, что сеть пригодна для обеспечения санкционированного доступа;

— контролируемая доступность — гарантия, что сеть обеспечит доступ только санкционированному пользователю для решения санкционированных задач;

— неприкосновенность — защита данных от несанкционированного их изменения и уничтожения;

— конфиденциалынсть — защита данных от несанкционированного раскрытия;

— безопасность передачи данных — гарантия того, что идентификация пользователей, качество передаваемых данных, время и продолжительность передачи данных обеспечены.

На основе данных требований были созданы соответствующие механизмы технического контроля, отвечающие следующим критериям:

1) целостность — базовая надежность, гарантирующая, что механизм работает как должно;

2) возможность проверки — способность записывать информацию, которая может иметь значение в раскрытии и расследовании попыток посягательства на средства компыотерной техники и других событий, относящихся к вопросам безопасности системы.

В результате практической реализации этих мер стало возможно:

­—контролировать физический доступ к средствам компьютерной техники (СКТ);

—контролировать электромагнитное излучение аппаратных СКТ;

— наблюдать за возможной угрозой СКТ и фиксировать каждую такую попытку (методом мониторинга).

Как видно из вышеприведенного, цели и основные положения защиты информации в зарубежных странах по ряду базовых позиций совпадают с российскими и предполагают:

а) предотвращение утечки, хищения, утраты, искажения и подделки информации;

б) предотвращение угроз безопасности личности, общества и государства;

п) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;

г) обеспечение правового режима функционирования документированной информации как объекта собственности;

д) сохранение государственной тайны и конфиденциальности документированной информации;

е) 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 СКТ включают в себя совокупность организационных мероприятий по подбору проверке и инструктажу персонала, участвующего на всех стадиях ин формационного процесса; разработке плана восстановления информационных объектов после выхода их из строя; организации программно-технического обслуживания СКТ; возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных СКТ; осуществлению режима секретности при функционировании компьютерных систем; обеспечению режима физической охраны объектов; материально-техническому обеспечению и т. д. и т. п. Организационные мероприятия, по мнению многих специалистов, занимающихся вопросами безопасности компьютерных систем, являются важным и одним из эффективных средств защиты информации, одновременно являясь фундаментом, на котором строится в дальнейшем вся система защиты[85].

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями способствующими совершению компьютерных преступлений в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать указанную в п. 1 ЭВМ в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее белопасности в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности, в т. ч. находящейся в форме машинной информации;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

В функциональные обязанности указанных лиц прежде всего должны входить следующие позиции осуществления организационных мер обеспечения безопасности СКТ:

1) обеспечение поддержки со стороны руководства конкретной организации требований защиты СКТ;

2) разработка комплексного плана защиты информации;

3) определение приоритетных направлений защиты информации в соответствии со спецификой деятельности организации;

4) составление общей сметы расходов финансирования охранных мероприятий в соответствии с разработанным планом и угверждение ее в качестве приложения к плану руководством организации;

5) определение ответственности сотрудников организации за безопасность информации в пределах установленной им компетенции путем заключения соответствующих договоров между сотрудником и администрацией;

6) разработка, внедрение и контроль за исполнеиием раз личного рода инструкций, правил и приказов, регламентирующих формы допуска, уровни секретности информации, кои-кретных  лиц,  допущенных к работе с секретными (конфиденциальными) данными и т. п.;

7) разработка эффективных мер борьбы с нарушителями защиты СКТ.

При этом, как показывает практика, наиболее надежным средством повышения эффективности мер безопасности СКТ является обучение и ознакомление работающего персонала с применяемыми в конкретной организации организационно-техническими мерами защиты[125].

Технические меры представляют собой применение различных устройств специального назначения:

1. Источники бесперебойного питания.

2. Устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находится компьютерная техника.

3. Устройства комплексной защиты телефонии.

4. Устройства пожарной защиты.

5. 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.)

1. Зависимый от предыстории обращения

2. По разрешению (по паролю)

Что же касается антивирусных программ, то ученые сходятся в том, что в настоящее время существует достаточное их количество, чтобы обезвредить практически любой вирус. Антивирусные программы обеспечивают защиту компьютера от вирусов на 97%. Три же процента это подтверждение того, что не бывает абсолютно надежных систем. Вообще если соблюдать простые правила (создавать архивы нужных программ, не устанавливать на компьютер носители информации сомнительного происхождения, периодически проверять компьютер на предмет появления вирусов и т.д.) можно избежать лишних проблем[5,8].

От разработок в области компьютерной безопасности зависит очень многое. В конечном итоге это должно привести к образованию индустрии средств безопасности компьютерных систем и технологий.

ЗАКЛЮЧЕНИЕ

Компьютер стал любимым детищем человека. Уровень развития страны во многом определяется по уровню компьютеризации. С вычислительной техникой человечество связывало надежды на резкий скачок в интеллектуальной и духовной областях, информатике, сервисе, обороноспособности и многое другое, что может сделать нашу жизнь беззаботнее, но к сожалению, далеко не всем надеждам удалось осуществиться. Наряду с несомненными благами компьютеризация еще более нарушила нашу безопасность. Количество ошибок, связанных с неправильным использованием вычислительной техники, с переоценкой ее надежности и защищенности, постоянно растет. В ПК и в вычислительных сетях сосредотачивается информация, исключительное пользование которой принадлежит определенным лицам или группам лиц, действующем в порядке личной инициативы или в соответствии с должностными обязанностями. Такая информация должна быть защищена от всех видов постороннего вмешательства. К тому же в вычислительных сетях должны принимать меры по защите вычислительных ресурсов сети от их несанкционированного использования, т.е. доступа к сети лиц, не имеющих на это права. Физическая защита более надежна в отношении компьютеров и узлов связи, но оказывается уязвимой для каналов передачи данных большой протяженности. Защита сетей приобретает все более важное значение, однако, не все считают, что это наилучшее решение проблемы защиты. Эту проблему следует рассматривать глобально. Необходимо защищать информацию на всем пути ее движения от отправителя до получателя.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ.

2. Федеральный закон "О противодействии коррупции" от 25.12.2008 N 273-ФЗ.

3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ

4.  Федеральный закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года №24-ФЗ.

5. Закон Российской Федерации "Об авторском и смежных правах" от 9 июля 1993 года №5351-1.

6. Закон Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" от 23 сентября 1992 года №3523-1.

7. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. - М., 2016. 3 с.

8. Борзенков Г.Н., Комиссаров В.С. Уголовное право Российской Федерации. - М.: Олимп, 2015. - 8 с.

9. Ведеев Д.В. Защита данных в компьютерных сетях. - М., 2016. – 4 с.

10. Волеводз А. Международная взаимопомощь при расследовании компьютерных преступлений (анализ международно-правовых документов) // Вопросы правоведения. Межвузовский сборник научных трудов. № 4. - Ереван: Изд-во Ереван, 2015. - С.11-26.

11. Воротников В.Л О правовой защите компьютерной информации / В.Л. Воротников // Администратор суда. - № 2. - 2017. - С.14-16.

12. Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н Евдокимов. - № 1 (59). - 2015. - С.21-31.

13. Егорышев А. С. Расследование и предупреждение неправомерного доступа к компьютерной информации. - М.: РГБ, 2014. - 148с.

14. Ефремова М.А. К вопросу о понятии компьютерной информации // Российская юстиция. - 2015. - №7. - С.50-52.

15. Жуков Ю.И., Приманкин А.И., Щербаков О.В. Информационная безопасность и аппаратно-программная надежность компьютерных средств органов внутренних дел / Ю.И. Жуков // Вестник МВД России. 2015. - №3. - С.75-81.

16. Зверева Е.А. Информация как объект имущественных гражданских прав / Е.А. Зверева // Право и экономика. -2014. - № 9. - С.28-33.

17. Иванов В.П. Защита от электронного шпионажа / В.П. Иванов // Сети и системы связи. - 2015. - №3. - С.110-111.