Содержание:

Введение

В современном мире, в эпоху интернета – компьютерная преступность приобрела новый статус и стала частью общественной жизни. С каждым годом технологии компьютерных преступлений развиваются, что негативно сказывается на бизнесе в каждой стране. Под негативом понимаются убытки, которые терпит бизнес при совершении компьютерных преступлений, которые исчисляются в огромных суммах денег.

Однако, компьютерные преступления — это не только кража денег методом взлома компьютерной системы любой организации, а также кража программ, секретной информации и оборудования с целью получения информации. Поэтому, из-за множества разновидностей и способов совершения преступлений увеличивается и охват различных сфер бизнеса, в которых возможно совершить то или иное компьютерное преступление. Следовательно, можно сделать вывод, что на данный момент компьютерная преступность это одна из главных проблем любой развитой страны, а также если учесть, что компьютерные преступления присутствуют в большинстве стран, то данную проблему можно охарактеризовать как глобальную.

Целью данной курсовой работы является «Характеристика понятия «Компьютерные преступления» и изучение принципа совершения компьютерных преступлений».

Задачами курсовой работы будут являться:

1. Изучение уголовных наказаний за компьютерные преступления;
2. Определение способов и методов совершения компьютерных преступлений;
3. Определение методов защиты информации.

Глава 1. Тенденции компьютерной преступности

1.1. Компьютерные преступления

Если прочесть Уголовный кодекс Российской Федерации или любой другой страны, то мы увидим, что ни в одном из разделов Уголовного кодекса нет главы «компьютерные преступления», как и нет понятия данного преступления, а есть лишь некоторые статьи. Это связанно с тем, что сама информация не является объектом преступления. Поэтому в юриспруденции, компьютерных преступлений не существует.

В общем понятии компьютерное преступление – это несанкционированное получение доступа к информации, хранящейся на компьютере методом взлома информационной системы. Однако, компьютерные преступления — это не только взлом, а также кража программ, секретной информации и оборудования с целью получения информации.

Люди, которые совершают данное преступление называются хакерами. Все хакеры в первую очередь высококлассные специалисты. Благодаря интернету они могут объединяться в группы из разных городов, регионов и стран, тем самым увеличивая шанс достижения необходимого результата по взлому компьютерных систем.

1.2. Компьютерная преступность в России

В развитых странах компьютерная преступность является одной из первостепенных проблем. Тройка стран – лидеров по убыткам это США, Франция и Германия. США ежегодно несет убытки около 5 млрд долларов из-за хакерских атак, во Франции потери меньше – около 1 млрд франков, в Германии около 4 млрд марок ежегодно.

В России в 2017 году аналитиками НАФИ[1] было проведено исследование, в котором подсчитали потери, которые терпит бизнес в России. Потери составили 116 млрд руб. Дополнительно, аналитика НАФИ провели опрос 500 сотрудников на руководящих должностях в 8 федеральных округах России на тему «С какими информационными угрозами приходилось сталкиваться вашей компании за последний год?». Статистика ответов приведена на рисунке 1.

Статистическая погрешность данного опроса не превышает 4,4%.

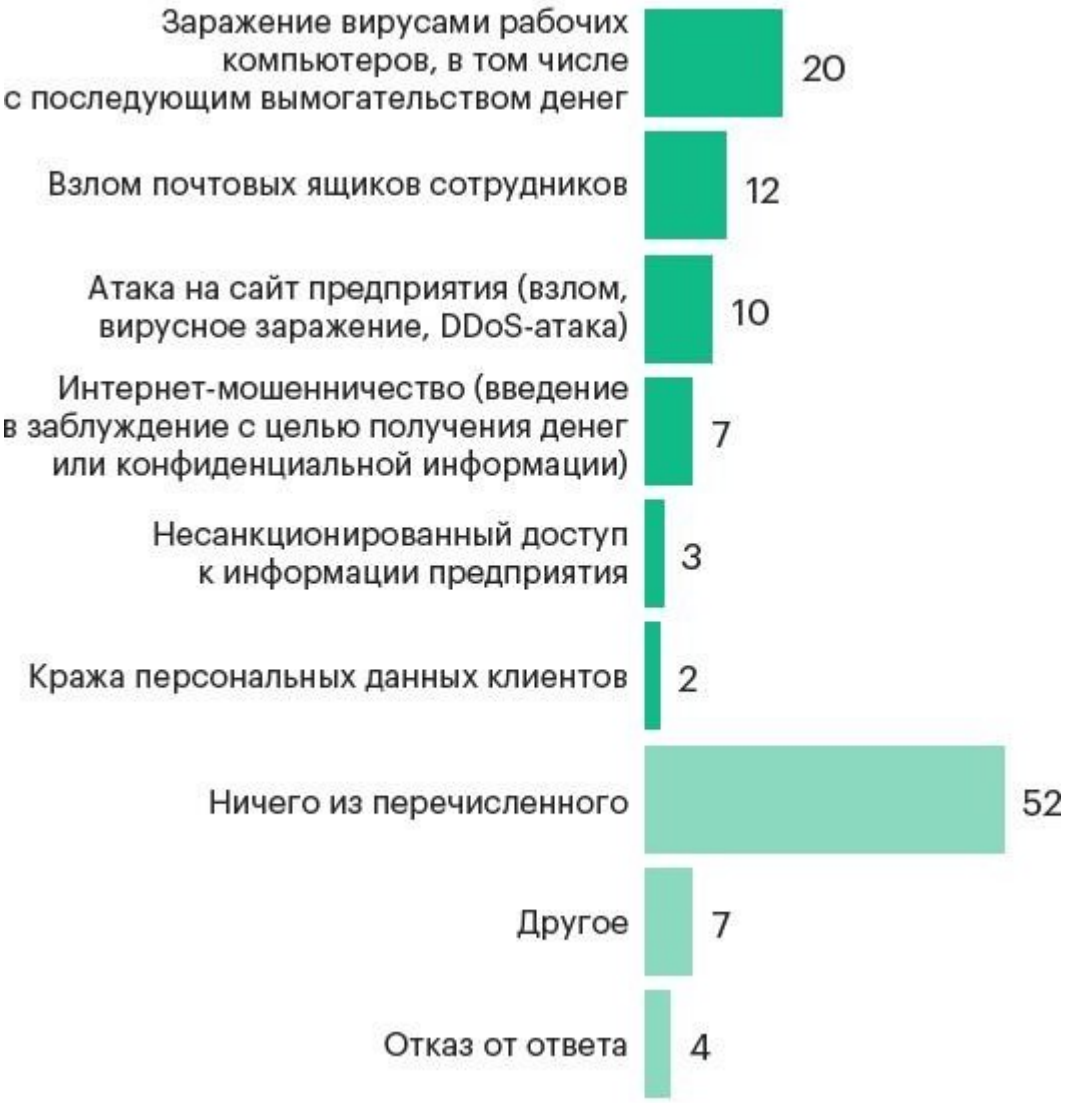


Рисунок 1. Итоги ответов опрошенных сотрудников

Поскольку Россия никогда не была в списке государств, где уровень компьютерной преступности был высок, то в российском законодательстве не предусматривались наказания или ответственность за компьютерные преступления. Изменения стали происходить лишь после громких преступлений, с последующим заведением уголовных дел. Одним из данных преступлений связано с Волжским автомобильным заводом, в котором один из программистов внес изменения в технологический процесс, что повлекло за собой огромные финансовые потери.

1.3. Уголовная ответственность в России

Одним из важных изменений в российском законодательстве стало введение нового Уголовного кодекса в 1997 году, в который внесли следующие статьи:

1) Статья 227 УК РФ «Неправомерный доступ к компьютерной информации»;

2) Статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»;

3) Статья 274 УК РФ «Нарушение правил эксплуатации компьютеров, компьютерных систем и сетей»;

Исходя из этих статей стоит отметить, что незаконное проникновение в компьютерную систему без причинения каких-либо неблагоприятных последствий не будет являться преступлением. Поэтому, уголовная ответственность наступает лишь тогда, когда информация уничтожена, заблокирована или скопирована.

К примеру, проникновение в чужую квартиру против воли владельца является уголовным преступлением, независимо был ли причинён вред квартире или владельцу, в то время как проникновение в чужую систему не будет являться преступлением.

Так, исходя из данных главного информационного центра МВД России в 1997 г. компьютерные преступления составляли всего 0,02% от общего числа преступлений. Тогда как общее количество компьютерных преступлений в 2018 году превысило сотню, а суммарный размер ущерба —20 млрд рублей.

Однако, это далеко не совсем точная статистика, так как Российским правоохранительным органам известна лишь часть компьютерных преступлений (не более 5—10%). Их раскрываемость также не превышает 1—5%. Фактором плохой раскрываемости является то, что изъятие информации за частую остается незамеченным, поскольку данные просто копируются, и за это время преступники успевают скрыться. Так же это происходит из-за недостаточной компьютеризации, плохой подготовки сотрудников правоохранительных органов, тем самым правоохранительные органы зачастую даже не догадываются о возможности осуществления некоторых преступлений. Другой же возможной проблемой является борьба за репутацию. Жертвы компьютерной преступности проявляют нежелание сообщать правоохранительным органам о хищении информации, так как опасаясь распространения информации о ненадежной системе безопасности, что может спровоцировать отток финансов и последующее банкротство.

-

1.4. Уголовная ответственность за границей

1. Законодательство США

Как известно, информационные компании зародились в США. Поэтому именно в США в 1977 году был разработан и введен первый законопроект, который устанавливал уголовное наказание за совершение компьютерных преступлений. А в 1984 году на основании данного законопроекта был принят закон, который также устанавливал уголовное наказание за мошенничество с использованием компьютера.

- ○ 1. Законодательство в Великобритании

Первый законопроект, касающийся компьютерных преступлений в Великобритании, был принят в 1990 году, который гласит, что преступлением является неправомерный доступ к любой программе или данным, находящиеся в компьютере.

Так же в 2000 году происходит расширение закона о терроризме и начинает касаться киберпространства. В данном законе установлено, что действия, которые вмешиваются или нарушают работу какой - либо электронной системы являются террористическими.

- ○ 1. Законодательство Германии

В немецком уголовном кодексе для понятия компьютерных используется специальный термин - Daten, который описан в статье 202 уголовного кодекса.

Так же в статье 303 уголовного кодекса прописаны множество компьютерных преступлений (DNS атаки разработка вредоносного ПО), за совершение которых следует уголовное название.

В большинстве других стран также существуют законы, статьи уголовного кодекса о компьютерных преступлениях, но они менее проработаны чем у их предшественников.

- 1. Интернет – готовая платформа для компьютерных преступлений
  Уникальность сети Internet заключается в том, что она не находится во владении какого-то физического лица, частной компании, государственного ведомства или отдельной страны. Поэтому практически

во всех её отраслях отсутствует регулирование, цензура и другие способы контроля информации. Благодаря данному отсутствию регулирования открываются практически неограниченные возможности доступа к любой информации, которые используют преступники в свою пользу и выгоду. Сеть Internet можно рассматривать не только как инструмент совершения компьютерных преступлений, но и как среда для ведения разнообразной преступной деятельности.

При использовании сети Internet в качестве среды для преступной деятельности является сама возможность обмена украденной информацией.

Так же существует еще одна привлекательная возможность – это информационно – психологическое воздействие на пользователей. Что это значит? А значит это, что с помощью сети Internet один человек может воздействовать на психику и сознание другого человека, тем самым меня его поведение, оказывая влияние на восприятие реальной действительности. Данная цель достигается с помощью распространения своих доктрин и учений, которые способствуют в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира.

Однако наибольший интерес сеть Internet представляет именно как орудие для совершения информационных преступлений. Обычно эти преступления связаны с незаконным копированием и продажей программ.

В современном мире, информация – это очень ценный и дорогой товар, особенно, если эта информация из банковской сферы, которая заключает в себе данные о вкладах, финансовом положении клиентов и самого банка, кредитах.

И так как субъекты банка не могут осуществлять свою работу без информационного обмена между собой, то зачастую для осуществления данного обмена используется сеть Internet, тем самым давая возможность получения преступниками доступа к секретной информации об объектах своей преступной деятельности.

Еще одна сфера компьютерных преступлений через Internet, появилась с возникновением электронных банковских расчётов. Имеется множество способов её хищения, но все они основываются на модификации информации, отображающей электронную наличность – это информация, хранится на личных счетах клиентов, которая в дальнейшем переписывается на другие счета, и используется злоумышленникам.

Глава 2 Взлом компьютерных систем и меры защиты от взлома

2.1. Способы совершения компьютерных преступлений

Способов совершения компьютерных преступлений на данный момент существует великое множество, но далеко не все актуальны на данный момент – некоторые устарели, другие требует большого опыта от хакера, а другие просто не подходят для достижения цели хакера. Поэтому к выбору способа совершения преступления, злоумышленники подходят очень серьезно.

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия преступления.

Выделяют следующие способы совершения компьютерных преступлений:

1. Похищение компьютерной техники;
2. Перехват информации;
3. Несанкционированный доступ к информации;
4. Манипуляция данными и управляющими командами;
5. Компьютерный саботаж;
6. Комплексные методы.

Похищением компьютерной техники преступником это традиционный способ преступления, где действием преступника является похищение чужой техники.

К перехвату информации является получение данных и машинной информации с использования различных методов перехвата. К методам перехвата относятся:

1. Активный перехват;
2. Пассивный перехват;
3. Аудиоперехват;
4. Видеоперехват;
5. Просмотр мусора.

Активный перехват осуществляется при помощи подключения к телекоммуникационному оборудованию компьютера, например, к телефонному проводу канала связи.

Пассивный перехват основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации.

Аудио перехват более распространенный способ и имеет две разновидности. Первая является в установке подслушивающего устройства в средства обработки информации, а вторая в установке микрофона на инженерно-технические конструкции за пределами охраняемого помещения (стены, оконные рамы, двери и т.п.).

Видео перехват осуществляется путем использования различной видеооптической техники.

Просмотр “мусора” является достаточно необычный способ перехвата информации. Преступник использует технологические отходы информационного процесса, оставленные пользователем после работы с компьютерной техникой (удаленная с жестких дисков компьютера).

К несанкционированному доступу относят методы и действия преступника, при помощи которых он незаконно получается доступ к информации.

При несанкционированном доступе используют следующие методы:

1. Подбор паролей;
2. Подмена пользователя;
3. Замена пользователя;
4. Неспешный выбор;
5. Брешь;
6. Люк;
7. Асинхронная атака;

8. Моделирование;
9. Мистификация.

Для манипуляции данных и управляющими командами применяют действия с использованием методов манипуляции данными и управляющими командами компьютерной техники. В эту группу относят следующие способы манипуляции данных:

1. Написание программы «Троянский конь»;
2. Написание программы «Компьютерный вирус»;
3. Компьютерное мошенничество;
4. Незаконное копирование программ с преодолением программных средств.

Компьютерный саботаж несет в себе с аппаратным и программным обеспечением. Данные действия приводят к выводу из работы компьютерные системы. Наиболее значительные компьютерные преступления совершаются посредством порчи программного обеспечения.

Комплексные методы включают в себя различные комбинации рассмотренных выше способов совершения компьютерных преступлений.

2.2. Методы взлома компьютерных систем

На первый взгляд взломать компьютерную систему это не легкое занятие. Но за частый удачный результат зависит от опыта хакера, уровня защиты компьютерной системы, а также выбор метода взлома той или иной компьютерной системы.

В общем понятии программное обеспечение любой компьютерной системы состоит из следующих компонентов: операционной системы (ОС)[2], сетевого программного обеспечения (СПО)[3] и системы управления базами данных (СУБД)[4]. Значит попытки взлома защиты компьютерных систем можно разделить на следующие группы:

1. Атаки на уровне операционной системы;
2. Атаки на уровне сетевого программного обеспечения;
3. Атаки на уровне систем управления базами данных.
    - 1. Атаки на уровне систем управления базами данных

Проще всего обойти защиту СУБД, так как СУБД имеют строго определённую внутреннюю структуру. В СУБД имеются четыре основных операции — поиск, вставка, удаление и замена элемента. Другие операции определяются как дополнительные и используются по мере необходимости. Поэтому благодаря строгой структуре и четко определенных операций защита СУБД и является более облегченной задачей. Наиболее часто хакеры предпочитают взламывать защиту на уровне операционной системы и таким образом получать доступ к файлам СУБД. Однако если в СУБД слабая защитная система, или СУБД, которая содержит ошибки в политике безопасности, которые были допущены администратором СУБД, то увеличивается шанс взлома защиты хакерами на уровне СУБД.

- ○ 1. Атаки на уровне операционной системы

Как взломать, так и защитить ОС является более трудной задачей, так как внутренняя структура ОС сложна и требует достаточно больших знаний для создания качественной защиты, а также требует соблюдение адекватной политики безопасности.

Существует мнение людей, деятельность которых несвязанная со взломом компьютерных систем, что успешные атаки на ОС осуществляются только с помощью сложнейших средств, разработанных на последних достижениях науки и техники, а хакер должен обладать большим опытом высочайшей квалификации. Но это не совсем.

Никто не спорит, что хакер должен быть в курсе всех новинок в области компьютерной техники, да и высокая квалификация не будет являться лишней. Но задача хакера состоит не в том, чтобы взломать самую продвинутую компьютерную систему, а суметь найти слабое место в конкретной системе защиты. При взломе, самые простые методы взлома на первый взгляд могут оказаться и ничуть не хуже самых современных и сложных методов, так как чем проще алгоритм взлома, тем больше вероятность завершение взлома без сбоев и ошибок.

Удачное выполнение алгоритма хакерской атаки зависит от архитектуры и конфигурации операционной системы, которую хакер собирается взломать.

Но несмотря на все разработанные меры защиты ОС, хакеры находят бреши в них, разрабатывают новые методы атак, применяют новые алгоритмы взлома и применяют весь свой опыт, чтобы достичь желаемой цели. Поэтому, существуют атаки, которым может быть подвергнута любая ОС независимо от уровня ее защиты:

1. Кража пароля;
2. Подглядывание за пользователем при вводе пароля, дающий право на работу с операционной системой;
3. Получение пароля из файла, в котором этот пароль был сохранен пользователем;
4. Кража внешнего информационного носителя, на котором хранится пароль (это могут быть дискет, флешка с электронным ключом);
5. Перебор всех возможных вариантов пароля;
6. Сканирование жестких дисков компьютера, для поиска файлов системы, в которых возможен сохранен пароль от операционной системы или любой другой программы;
7. Сборка мусора (восстановление файлов, которые пользователь ранее удалил);
8. Превышение полномочий;
9. Запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы (драйвера, сервиса, демона и т. д.);
10. Замена загружаемой библиотеки, используемой системными программами;
11. Захват ресурсов;
12. Атака запросами;
13. Использование ошибок в программном обеспечении или администрировании.

Каждый перечисленный метод атак имеет как свои плюсы, так и минусы. За частую, чтобы взломать ОС или получить доступ к ней, опытные хакеры применяют несколько методов атак, пока не достигнут положительного результата.

- ○ 1. Атаки на уровне сетевого программного обеспечения

Данный метод атаки является одним из излюбленных и распространенным среди хакеров, так как СПО является самым уязвимым компонентом любой операционной системы, так как канал связи, по которому осуществляется передача сообщения, чаще всего не защищен. Любой пользователь, который имеет доступ к этому каналу может перехватывать сообщения и отправлять свои собственные. Следовательно, на уровне СПО возможны следующие хакерские атаки:

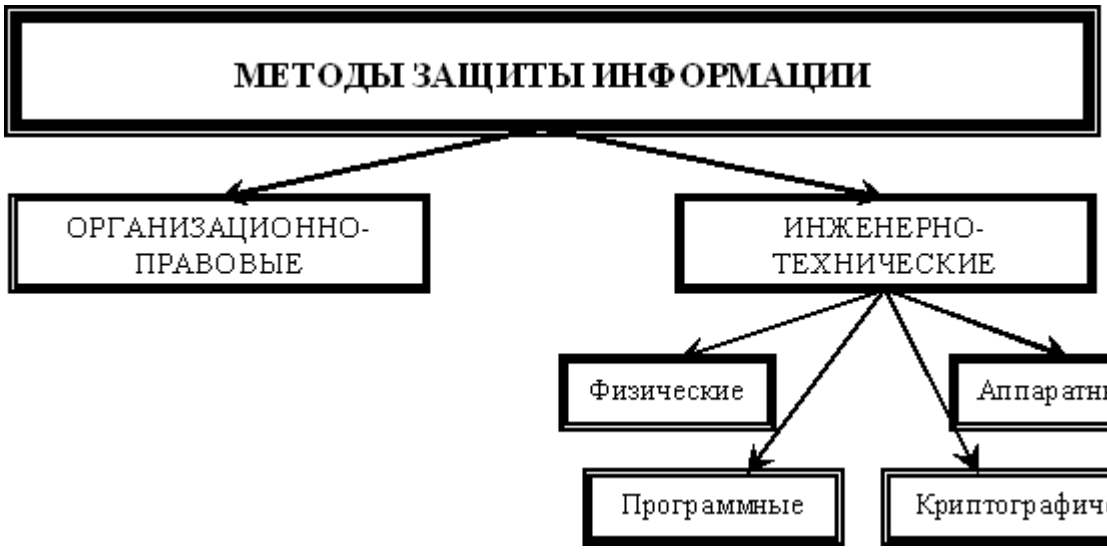
1. Прослушивание сегмента локальной сети;
2. Перехват сообщений на маршрутизаторе;
3. Создание ложного маршрутизатора;
4. Навязывание сообщений;
5. Отказ в обслуживании.

Так как данная атака осуществляется из-за открытости сетевого соединения, разумно предположить, что для предотвращения таких атак необходимо максимально защитить каналы связи, что приведет к затруднению обмена информацией для тех, кто не является легальным пользователем.

Ниже приведены способы такой защиты:

1. Максимальное ограничение размеров компьютерной сети (чем больше сеть, тем труднее ее защитить);
2. Изоляция сети от внешнего мира (это ограничение физического доступа к компьютерной сети извне);
3. Шифрование сетевых сообщений (устранение угрозы перехвата сообщений);
4. Электронная цифровая подпись сетевых сообщений;
5. Использование брандмауэров в качестве дополнительной защиты.
    1. Методы защиты информации от незаконного взлома

Компьютерные преступления подразделяются на множество видов. Это может быть несанкционированный доступ к информации, ввод в программное обеспечение различных ошибок и специальных файлов, которые срабатывают при выполнении того или иного действия пользователя, а то и вовсе частично или



Методы защиты информации подразделяют на следующие группы:

Рисунок 2. Классификация методов защиты информации в компьютерных

2.3. Методы и средства организационно-правовой защиты информации

Методами и средствами организационной защиты информации являются организационно-технические и организационно-правовые мероприятия, которые проводятся в ходе создания и эксплуатации компьютерной сети. Например, данные мероприятия проводятся при строительстве или ремонте помещений, в которых будет находиться компьютерная техника, проектировании системы, монтаже и наладке ее технических и программных средств.

Основным процессом организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, в которых четко определены уровни регулирования доступа к информации со стороны потребителей.

- ○ 1. Методы и средства инженерно-технической защиты информации

Инженерно-техническая защита (ИТЗ)[5] – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

По своему назначению средства ИТЗ подразделяются на следующие группы:

1. Физические средства, которые включают в себя средства и сооружения, препятствующие физическому проникновению (доступу) злоумышленников. Благодаря этому удается ограничить доступ к материальным носителям конфиденциальной информации, а также помогает осуществить защиту персонала, материальных средств, финансов;
2. Аппаратные средства – это приборы, устройства, приспособления и другие технические решения, которые используются для защиты информации. На практике в деятельности предприятия применяется самая разная аппаратура, такая как: телефонный аппарат, различные автоматизированные системы, обеспечивающие производственную деятельность. Основной задачей данных средств является обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа;
3. Программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбор, накопление, хранение,

обработка и передача) данных;
4. Криптографические средства – это специальные математические и алгоритмические средства защиты информации, которые применяют различные методы шифрования при передаче данной информации по системам и сетям связи.

Заключение

Подведя итоги можно сказать, что компьютерная преступность была и остается быть актуальной проблемой. Это постоянный развивающийся вид преступлений. С каждым годом количество компьютерных преступлений увеличивается, а это значит, что способы и методы совершения преступлений с каждым разом становятся все усовершенствованные, а методы защиты остаются на уровень ниже. Поэтому никакие решения, будь то аппаратные или программные, или любые другие не гарантируют полную и надежную безопасность информации от несанкционированного доступа. Но несмотря на это, благодаря комплексному подходу к вопросу безопасности, удаётся свести все рискни на минимум.

Также стоит отметить, что несмотря на все убытки, которые может принести компьютерная преступность, параллельно она и несет в себе прибыль тем, кто борется с этой проблемой. Например, с появлением большого количества вирусов и различных вредоносных программ, увеличился спрос на антивирусную продукцию, а это значит, что у разработчиков антивирусных программ, антишпионов и т.д. с увеличением спроса увеличился и их доход.

В завершении можно также сказать, что в законодательстве большинстве стран плохо, а то и вовсе не проработаны законы, статьи Уголовного кодекса о компьютерных преступлениях, что дает преступникам еще больше безнаказанно совершать свои преступные действия, тем самым развивая и распространяя свои вид преступной деятельности.

Список использованных источников

Источники

1. Доктрина информационной безопасности Российской Федерации: от 09.10.2000 № Пр-1895: (утвержден В.В. Путиным). – Электрон. Дан. – Режим

доступа: http://www.agentura.ru/library/doctrina/
2. Уголовный Кодекс Российской Федерации: от 13.06.1996 N 63- ФЗ: (принят ГД ФС РФ 24.05.1996). – Электрон. Дан. - № 28. – Ст. 273. – Режим доступа: http://www.consultant.ru/popular/ukrf/
3. Уголовный кодекс Германии: от 15.05.1871 – Электрон. Дан. – Ст. 202. – Режим доступа: https://www.litres.ru/n-s-rachkova/ugolovnyy-kodeks-federativnoy respubliki-germanii/chitat-onlayn/
4. Уголовный кодекс Германии: от 15.05.1871 – Электрон. Дан. – Ст. 303. – Режим доступа: www.litres.ru/n-s-rachkova/ugolovnyy-kodeks-federativnoy respubliki-germanii/chitat-onlayn/
5. Уголовный кодекс США: от 1926 г. Режим доступа: https://ru.wikipedia.org/wiki/Кодекс_Соединённых_Штатов_Америки

Литература

1. Кловский Д.Д. Теория передачи сигналов. – М.: Связь, 1984.
2. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. М.: Наука, 2006.
3. Акулов О.А., Медведев Н.В Информатика базовый курс. М.: Омега-Л, 2005.
4. Wikipedia.ru. [Электронный ресурс]: Свободная энциклопедия. – Электрон. дан. – М., Режим доступа: http://ru.wikipedia.org

rbc.ru. [Электронный ресурс]: Газета. Режим доступа: https://www.rbc.ru/newspaper/2017/12/20/5a38f3749a794710aa15581b

1. НАФИ – национальное агентство финансовых исследователей ↑

2. ОС – операционная система ↑

3. СПО – сетевое программное обеспечение ↑

4. СУБД – система управления базами данных ↑

5. ИТЗ – инженерно – техническая защита ↑