Содержание:

ВВЕДЕНИЕ

Главной угрозой для информационной безопасности предприятий является утечка информации, которая является конфиденциальной. Утечка информации представляет собой неправомерное разглашение конфиденциальной информации за пределы предприятия, которой данная информация принадлежит.

Вне зависимости от того, каким образом осуществляется утечка информации и добывается конфиденциальная информация, данное действие в любом случае является незаконным и противоправным.

Утечка информации всегда происходит в случае наличия следующих условий:

- если есть злоумышленник, которому данная конфиденциальная информация необходима.

- если есть подходящие условия для обеспечения добычи конфиденциальной информации.

К факторам, которые способствуют потере конфиденциальной информации и вывод ее за пределы предприятия – собственника, можно отнести следующие обстоятельства:

Это могут быть недостаточные знания работников предприятия, правил защиты конфиденциальной информации, а также халатное отношение к данной сфере деятельности, или же непонимание режима сохранения коммерческой тайны.

Использование технических средств, которые не прошли аттестацию.

Текучесть кадров, в том числе и тех, кто владеет коммерческой тайной, плохие условия труда, грубое отношение со стороны руководства.

Поэтому анализировать причины возникновения угроз информационной безопасности на предприятии необходимо, так как только так оно может их предотвратить.

Вышесказанное и определяет актуальность выбранной темы курсовой работы для исследования «Виды и состав угроз информационной безопасности».

Цель исследования состоит в определении видов угроз информационной безопасности, а также в исследовании мероприятий, которые смогут обеспечить информационную безопасность.

Для достижения цели необходимо решение следующих **задач:**

1) Рассмотреть содержание понятия угрозы информационной безопасности.

2) Оценить борьбу с причинами угроз информационной безопасности.

3) Провести анализ видов и состава угроз информационной безопасности.

4) Рассмотреть методы защиты предприятия от утечки информации.

Объектом исследования является угроза информационной безопасности. **Предметом** исследования является исследование мероприятий, которые будут способствовать снижению данных угроз информационной безопасности предприятия.

Работа состоит из введения, двух глав («Характеристика видов угроз информационной безопасности», «Исследование мероприятий по обеспечению информационной безопасности»), заключения и библиографии.

ГЛАВА 1. Характеристика видов угроз информационной безопасности

1.1 Содержание понятия угрозы информационной безопасности

Угроза информационной безопасности представляет собой потенциальную возможность определенным образом нарушить информационную безопасность.

Если рассматривать вопрос защиты информации, которая является конфиденциальной, то понятие угрозы информационной безопасности можно трактовать несколько иным определением.

В данном случае угроза информационной безопасности представляет собой потенциальную возможность несанкционированного или случайного воздействия на информацию, которое приводит к ее утрате, искажению, модификации и т.д. [1]

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, – злоумышленником. Потенциальные злоумышленники называются источниками угрозы[2].

Однако угроза никогда не существует сама по себе. Угроза выступает следствием наличия слабых звеньев в системе защиты информационных систем. Это может быть, к примеру, наличие доступа к конфиденциальной информации посторонних лиц. Также к угрозе в данном случае можно отнести возникновение ошибки в программном оборудовании.

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на информационную систему.

Когда же говорится об ошибках, возникших в информационной системе, то уязвимое место или опасное окно сохраняется до тех пор, пока программное обеспечение не будет восстановлено, и не будут ликвидированы последствия такого данной ошибки в программном обеспечении.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда – недель), поскольку за это время должны произойти следующие события:

– должно стать известно о средствах использования пробела в защите;

– должны быть выпущены мероприятия по ликвидации данных ошибок;

– мероприятия по ликвидации данных ошибок должны быть установлены в защищаемой информационной системе[3].

Однако, не все угрозы информационной безопасности можно отнести к следствиям какой-либо ошибки или злого умысла. Некоторые угрозы существуют, исходя из природы информационных систем. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания[4].

Далее рассмотрим самые распространенные угрозы, которые могут возникнуть у современных информационных систем. Знание, пусть и минимальное, о потенциальных угрозах информационной безопасности необходимо, так как они помогут выбрать оптимальные методы их предотвращения. Также очень важно знать об угрозах информационной безопасности, так как это поможет избежать перерасхода средств, нерационального расходования финансов. Также самым худшим вариантом может быть концентрация ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Понятие «угроза» для разных предприятий может трактоваться совершенно по-разному. Например, для предприятий открытого типа, не существует угрозы, так как вся информация находится в широком доступе. Но таких предприятий крайне мало, поэтому в большинстве случаев нелегальный доступ представляется серьезной опасностью[5].

Таким образом, можно отметить, что понятие угрозы для конкретного предприятия зависит о того, какой ущерб может быть причинен данному предприятию, и в каком размере.

Далее рассмотрим классификацию угроз информационной безопасности.

Угрозы можно классифицировать по нескольким критериям:

1) по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

2) по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

3) по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);

4) по расположению источника угроз (внутри/вне рассматриваемой ИС) [6].

Рассмотрим данную классификацию в виде рисунка 1.

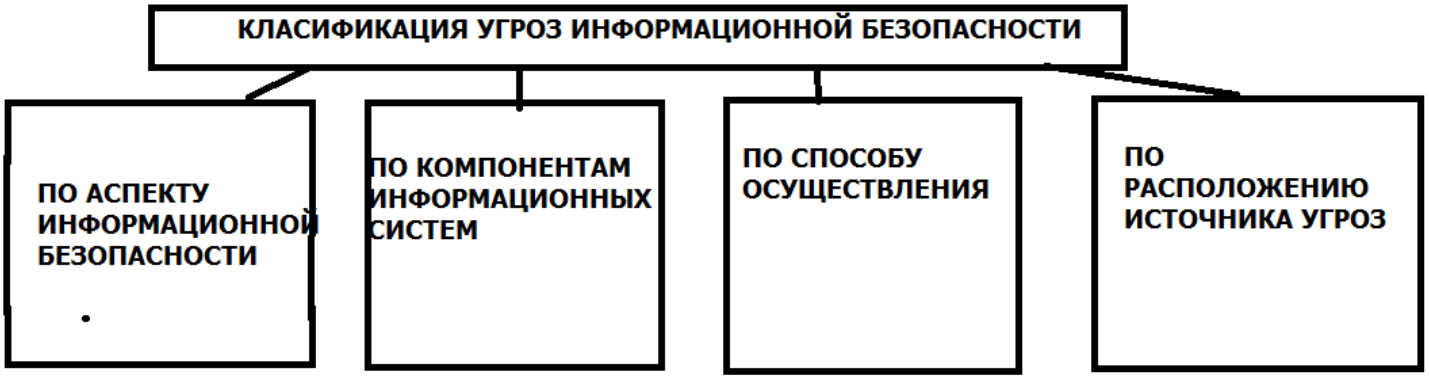

Рисунок 1. Классификация угроз информационной безопасности

Таким образом, в заключении данного раздела «Содержание понятия угрозы информационной безопасности» можно прийти к следующим выводам:

- угроза информационной безопасности представляет собой потенциальную возможность несанкционированного или случайного воздействия на информацию, которое приводит к ее утрате, искажению, модификации и т.д.

- угроза информационной безопасности никогда не существует обособленно, сама по себе. Угроза выступает следствием наличия слабых звеньев в системе защиты информационных систем.

- не все угрозы информационной безопасности можно отнести к следствиям какой-либо ошибки или злого умысла. Некоторые угрозы существуют, исходя из природы информационных систем.

- понятие «угроза» для разных предприятий может трактоваться совершенно по-разному. Например, для предприятий открытого типа, не существует угрозы, так как вся информация находится в широком доступе. Но таких предприятий крайне мало, поэтому в большинстве случаев нелегальный доступ представляется серьезной опасностью.

1.2 Анализ видов и состава угроз информационной безопасности

Существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка уничтожение. На основании данных видов и состава угроз информационной безопасности и будет построен

данный раздел курсовой работы.

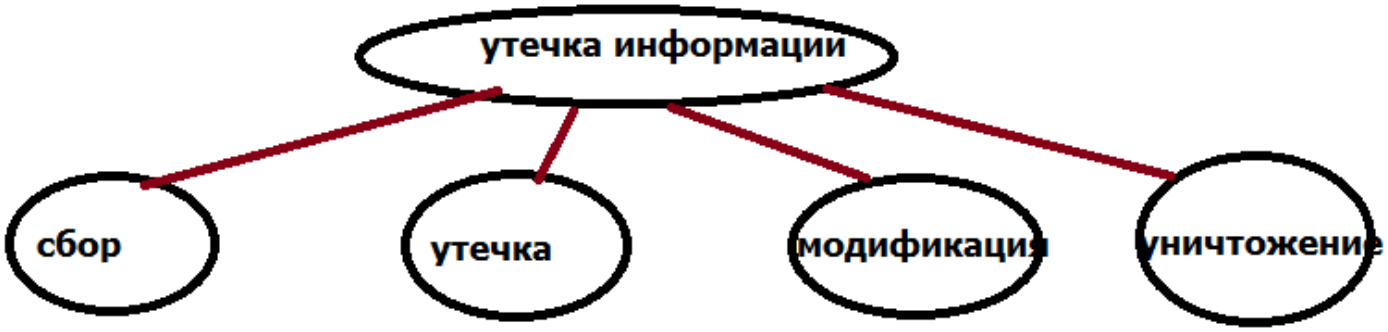

Рисунок 2. Виды угроз информационной безопасности

У угрозы информационной безопасности всегда есть источники. Рассмотрим их.

Источники информационной безопасности можно разделить на внутренние и внешние источники. К источникам внутренних угроз можно отнести следующие:

- сотрудники или персонал предприятия.

- программное обеспечение предприятия.

- программные средства предприятия.

Внутренние угрозы могут проявляться в следующих формах: ошибки пользователей и системных администраторов; нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации; ошибки в работе программного обеспечения; отказы и сбои в работе компьютерного оборудования.

К источникам внешних угроз можно отнести следующие:

1. Компьютерные вирусы и вредоносные программы;

2. Организации и отдельные лица;

3. Стихийные бедствия.

Внешние угрозы могут проявляться в следующих видах и формах. Компьютер может быть заражен вредоносной программой или различными вирусами. Также у злоумышленника мог появиться несанкционированный доступ к информации, которая считается конфиденциальной. Внешней угрозой также называется проверка и добывание информации о предприятии конкурирующей фирмой.

Значительным внешним источником угроз могут быть стихийные бедствия, такие как пожар, наводнение, аварии и другие катастрофические события[7].

Угрозы информационной безопасности также делятся на умышленные и неумышленные угрозы.

Исследования показывают, что более 50% вторжений в информационную безопасность предприятия – это дело рук сотрудников данного предприятия. Причины могут быть самыми различными, от банальной халатности до злого умысла. Наиболее часто информационным атакам подвергаются организации медицинской и финансовой направленности.

Как показывает практика, наиболее инцидентами являются: прослушивание телефонных переговоров и просмотр электронной почты, проникновения в информационные системы, подделка обратного адреса, чтобы замести следы и отвести подозрение на непричастных лиц. Следует отметить, что подобные злые умыслы совершаются чаще всего либо обиженными сотрудниками предприятия, либо конкурентами.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации: информационные, программные, физические, радиоэлектронные организационно-правовые[8].

К информационным угрозам относятся: несанкционированный доступ к информационным ресурсам; незаконное копирование данных в информационных системах; хищение информации из библиотек, архивов, банков и баз данных; нарушение технологии обработки информации; противозаконный сбор и использование информации; использование информационного оружия.

В состав программных угроз относят: использование ошибок и слабых мест в ПО; компьютерные вирусы и вредоносные программы; установка «закладных» устройств; К физическим угрозам относятся: уничтожение или разрушение средств обработки информации и связи; хищение носителей информации; хищение программных или аппаратных ключей и средств криптографической защиты данных; воздействие на персонал[9].

К радиоэлектронным угрозам относятся: внедрение электронных устройств перехвата информации в технические средства и помещения; перехват, расшифровка, подмена и уничтожение информации в каналах связи.

В состав организационно- правовых угроз можно отнести следующие угрозы: это закупка информационных технологий, которая заведомо является устаревшей или недоработанной. Также в данную группу входят нарушение требований и предписаний законодательных и нормативных актов.

Анализ всех видов угроз, которые присутствуют на предприятии, а также их выявление является одной из важнейших задач и функций системы безопасности предприятия. Более того, вся система защиты конфиденциальной информации должна быть основана на анализе всех угроз, которые могут возникнуть у данного предприятия. Рассмотрим пример. Если сотрудник, который владеет конфиденциальной информацией предприятия, имеет доступ в Интернет, то число угроз информационной безопасности резко возрастает. Поэтому и методы защиты данной информации должны быть усилены значительным образом[10].

История развития информационных систем показывает, что новые уязвимые места появляются постоянно. С такой же регулярностью, но с небольшим отставанием, появляются и средства защиты. В большинстве своем средства защиты появляются в ответ на возникающие угрозы, так, например, постоянно появляются исправления к программному обеспечению фирмы Microsoft, устраняющие очередные его уязвимые места и др. [11]

Конечно, такой подход не является абсолютно эффективным, скорее наоборот, неэффективным. Этому есть причина: существует промежуток времени, когда угрозы выявлена и устраняется. Именно в данный промежуток времени злоумышленник может нанести непоправимый ущерб, от которого предприятие понесет как моральные, так и материальные последствия[12].

В этой связи более приемлемым является другой способ - способ упреждающей защиты, заключающийся в разработке механизмов защиты от возможных, предполагаемых и потенциальных угроз.

Как ранее было отмечено, не все ошибки являются преднамеренными и умышленными. Существуют такие ошибки, которые были совершены случайно, и, тем не менее, повлекли за собой возникновение угрозы информационной безопасности.

Рассмотрим признаки классификации угроз информационной безопасности.

1) Признак по составляющим элементам информационной безопасности, против которых направлены угрозы.

2) Признак по компонентам информационных систем, на которые угрозы нацелены.

3) Признак по характеру воздействия.

4) Признак по расположению источника угроз (внутри или вне рассматриваемой информационной системы) [13].

Прежде чем начинать анализировать угрозы информационной безопасности предприятия, необходимо сперва выявить составляющие элементы системы информационной безопасности, которые с большей вероятностью могут быть подвержены атаке со стороны информационных угроз.

Далее рассмотрим, какие могут быть угрозы информационной безопасности по характеру воздействия.

Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

Причинами случайных воздействий при эксплуатации могут быть:

1) Различные аварии в случае стихийных бедствий или других форс-мажорных обстоятельств. Это называются природные и техногенные воздействия.

2) Сбой в работе аппаратуры и оборудования.

3) Ошибки в работе программного обеспечения.

4) Ошибки, совершаемые персоналом, либо по халатности, либо по злому умыслу.

5) Сбои и помехи в работе линий связи в связи с влиянием воздействий внешних условий.

Преднамеренные воздействия - это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник.

Действия нарушителя диктуются различными мотивами, самыми распространенными из которых являются следующие: любопытство, обида на руководство предприятия, то есть уязвленное самолюбие и хакерская атака.

Угрозы, классифицируемые по расположению источника угроз, бывают внутренние и внешние. Внешние угрозы обусловлены применением вычислительных сетей и создание на их основе информационных систем. Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно[14].

Особого внимания заслуживает канал несанкционированного доступа к информации. Ведь именно несанкционированный доступ порождает практически все угрозы информационной безопасности предприятия. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки[15].

Каналы несанкционированного доступа к информации классифицируются по компонентам автоматизированных информационных систем:

1) Посредством вмешательства человека. Несанкционированный доступ информации через человека может быть осуществлен следующим образом:

- через хищение носителей информации. Сюда относят хищение не только документов на бумажных носителях, но и USB накопители данных, слив информации через электронную почту, социальные сети, SKYPE и прочие.

- через чтение информации с экрана компьютера или клавиатуры.

- чтение информации, которая была уже распечатана на бумажный носитель.

2) Посредством программы. Это может осуществляться следующим образом:

- посредством перехвата паролей.

- посредством расшифровки зашифрованной информации.

- посредством копирования информации с носителя. Следует отметить, что на сегодняшний день накопителями информации являются не только флеш карты, но и смартфоны, плееры и прочие накопители информации.

3) Посредством аппаратуры.

- через подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;

- через перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т. д. [16]

Далее рассмотрим основные источники угроз. В настоящее время основными источниками угроз для информации на компьютере пользователя является интернет и электронная почта. Огромное количество вредоносных программ, в число которых входят вирусы, троянские программы, черви, могут «пробраться» на компьютер, пока пользователь читает статью в интернете, занимается поиском информации, открывая множество веб-сайтов, скачивает и устанавливает программное обеспечение на компьютер, читает почтовое сообщение. Вредоносные программы распространяются с молниеносной скоростью и за доли секунды могут нанести такой вред, восстановление после которого может дорого обойтись. Речь здесь идет не только о повреждении данных, но и о несанкционированном доступе к системе, нарушении ее целостности, краже информации. Не стоит забывать и о еще одном важном источнике «неприятностей» - спаме. Нежелательная почтовая корреспонденция может нанести гораздо больший вред, чем некоторые вредоносные программы. Не являясь источником прямой угрозы, спам приводит к потерям рабочего времени и наносит значительные финансовые потери, которые увеличиваются в сотни, тысячи раз, если это касается корпоративной компьютерной сети. Каждый пользователь, широко использующий современные информационные ресурсы, должен знать, что ему угрожает, и какие последствия может за собой повлечь то или иное вредоносное воздействие[17].

Таким образом, в заключении раздела «Анализ видов и состава угроз информационной безопасности» можно прийти к следующим выводам:

- источники информационной безопасности можно разделить на внутренние и внешние источники. К источникам внутренних угроз можно отнести следующие: - сотрудники или персонал предприятия, программное обеспечение предприятия, программные средства предприятия. Ко внешним источникам угроз информационной безопасности можно отнести вирусы, программы – шпионы, и прочие вредоносные угрозы, которые возникают со стороны Интернет.

Выводы по главе 1.

В ходе первой главы данной курсовой работы «Характеристика видов угроз информационной безопасности» были сделаны следующие выводы:

- угроза информационной безопасности представляет собой потенциальную возможность несанкционированного или случайного воздействия на информацию, которое приводит к ее утрате, искажению, модификации и т.д.

- угроза информационной безопасности никогда не существует обособленно, сама по себе. Угроза выступает следствием наличия слабых звеньев в системе защиты информационных систем.

- не все угрозы информационной безопасности можно отнести к следствиям какой-либо ошибки или злого умысла. Некоторые угрозы существуют, исходя из природы информационных систем.

- понятие «угроза» для разных предприятий может трактоваться совершенно по-разному. Например, для предприятий открытого типа, не существует угрозы, так как вся информация находится в широком доступе. Но таких предприятий крайне мало, поэтому в большинстве случаев нелегальный доступ представляется серьезной опасностью.

- источники информационной безопасности можно разделить на внутренние и внешние источники. К источникам внутренних угроз можно отнести следующие: - сотрудники или персонал предприятия, программное обеспечение предприятия, программные средства предприятия. Ко внешним источникам угроз информационной безопасности можно отнести вирусы, программы – шпионы, и прочие вредоносные угрозы, которые возникают со стороны Интернет.

ГЛАВА 2. Исследование мероприятий по обеспечению информационной безопасности

2.1 Борьба с причинами угроз информационной безопасности

Статистика, которая касается утечки информации в России, неутешительна. Россия уже два года подряд занимает второе место в мире по числу утечек. При этом уже

несколько лет наблюдается их стабильный рост. В частности, в 2014 году количество российских утечек данных выросло на 25%. За этот же период объем скомпрометированных данных увеличился более чем в 2,5 раза, в результате за год в России утекло более 8 миллионов записей о персональных данных россиян, которые представляют собой самую привлекательную категорию конфиденциальной информации для злоумышленников. Утечки персональных данных составляют 90% всех инцидентов подобного рода[18].

Цифры исследований довольно внушающие, поэтому задача борьбы с утечкой информации на сегодняшний день стоит весьма остро и болезненно.

Следует привести еще одни цифры исследований, согласно которым, в России 75% утечек информации происходят случайным образом, чаще всего из-за халатности сотрудников. Лишь 15% утечек являются преднамеренными. И только 10% утечек всей информации произошли из-за преднамеренной деятельности руководителей предприятия[19].

Разрабатывая мероприятия по борьбе с утечкой информации, стоит определить, по каким же каналам осуществляется данная утечка информации. Специалисты утверждают, что большая часть утечек информации происходит либо через Интернет, либо через бумажные носители. И эти каналы любому предприятию под силу контролировать.

Эксперты в области исследования данной тематики утверждают, что большинство сотрудников передают конфиденциальную информацию через электронную почту, либо распечатывают ее на бумагу и потом уже уносят с собой.

Менее популярными, но все же реальными каналами утечек являются также USB-носители информации и мобильные устройства, которые сегодня используют практически все сотрудники компаний, независимо от их должности и служебного положения.

Особую опасность представляет так называемый канал утечки информации, как «канал неопределен». Опасность состоит в том, что неизвестно от кого, и в каком направлении ждать подвоха. Это может случиться в любую минуту, через неизвестный канал, и слиться может любая информация, даже которая раньше была максимально защищенной.

По состоянию на 2015 год в России нет закона, требующего раскрывать данные об утечках ни перед клиентами, ни перед СМИ. Поэтому при возникновении утечки

необходимо в первую очередь проанализировать, как утеря данных может повлиять на деятельность организации, и принять превентивные меры, а также внедрить соответствующие системы безопасности, которые помогут закрыть обнаруженный канал утечек[20].

Поскольку основная причина утечек – действия инсайдеров, защита от утечек подразумевает установку средств защиты от внутренних угроз. Для этого применяются системы класса DLP (Data Leakage Prevention) [21].

Также современные информационные технологии предлагают следующие решения: специальное программное обеспечение, которое блокирует отправку электронной переписки, то есть делает ее невозможной, ограничивает работу с флеш накопителем информации. Эффективным методом является программное обеспечение, которое полностью контролирует действия пользователей компьютеров.

Второй тип систем представляет собой специальное ПО или оборудование для шлюзов, которое анализирует весь трафик, выходящий за пределы компании. После тщательной настройки, такие системы позволяют обнаружить передачу конфиденциальной информации в момент отправки данных, пресечь факт нарушения и выявить виновных.

Все перечисленные средства защиты дополняют системы разграничения прав доступа и шифрования данных. Такие решения не позволят пользователю обращаться к данным, которые не нужны ему в работе, а также обеспечивают защиту данных от перехвата при передаче по открытому интернету, а также не позволяют прочитать конфиденциальную информацию в случае утери мобильного устройства или USB-накопителя. Главное, чтобы используемые системы располагали нужным сертификатом ФСТЭК и соответствовали требованиям по определенному классу защиты, если ваша компания является оператором персональных данных.

Стоимость защиты от утечек данных будет сильно зависеть от выбранной стратегии, количества защищаемых рабочих станций и мобильных устройств, мощности установленных средств фильтрации трафика на шлюзе, наличия дополнительных элементов, таких как защита данных в облачных хранилищах или контроль запуска приложений. Например, если приобретать только решения для защиты от копирования через USB-порт, стоимость защиты будет составлять несколько тысяч рублей на один ПК, а стоимость комплексных систем объявляется

поставщиками только по запросу[22].

Было выяснено, что основная угроза – это внутренняя угроза. Специалисты по обеспечению информационной безопасности утверждают, что именно внутренней угрозе и ее ликвидации относят 80% всех усилий данных специалистов.

Внутренним злоумышленником, или инсайдером, может стать практически любой сотрудник, имеющий доступ к конфиденциальной информации компании. Мотивация действий инсайдера не всегда очевидна, что влечёт за собой значительные трудности в его идентификации. Недавно уволенный сотрудник, затаивший обиду на работодателя; нечистый на руку работник, желающий подзаработать на продаже данных; современный Герострат; специально внедрённый агент конкурента или преступной группы – вот лишь несколько архетипов инсайдера.

Самая большая ошибка, которую предприятие может допустить в части обеспечения информационной безопасности - это недооценивание масштабов данной проблемы. Статистика неукоснительна и неутешительно. 20% утекшей конфиденциальной информации. В конечном счете, ведет если не к краху, но и к значительным финансовым потерям[23].

Особенно частой, но до сих пор наиболее уязвимой жертвой инсайдеров становятся финансовые учреждения, причём любого размера – со штатом от сотни до нескольких тысяч работников. Это вызвано желанием осуществить мошенничество по отношению к финансовым интересам лиц. Несмотря на то, что в большинстве случаев компании стараются скрыть или существенно занизить реальные цифры ущерба от действий инсайдеров, даже официально оглашаемые суммы убытков поистине впечатляют[24].

Непредумышленное причинение вреда конфиденциальным данным компании, их утечка или потеря – вещь куда более частая и прозаическая, чем вред, наносимый инсайдерами. Безалаберность персонала и отсутствие должного технического обеспечения информационной безопасности может стать причиной прямой утечки корпоративных секретов. Такая халатность несёт не только серьёзные убытки бюджету и репутации компании, но и может вызывать широкий общественный диссонанс. Вырвавшись на волю, секретная информация становится достоянием не узкого круга злоумышленников, а всего информационного пространства – утечку обсуждают в интернете, на телевидении, в прессе. Вспомним громкий скандал с публикацией SMS-сообщений крупнейшего

российского оператора сотовой связи «Мегафон». Из-за невнимательности технического персонала, смс-сообщения были проиндексированы интернет-поисковиками, в сеть попала переписка абонентов, содержащая информацию как личного, так и делового характера. Совсем недавний случай: публикация личных данных клиентов Пенсионного фонда России. Ошибка представителей одного из региональных представительств фонда привела к индексации персональной информации 600 человек – имена, регистрационные номера, подробные суммы накоплений клиентов ПФР мог прочитать любой пользователь интернета[25].

Таким образом, в заключении раздела «Борьба с причинами угроз информационной безопасности» можно сделать следующие выводы:

- угрозы информационной безопасности на предприятии не являются чем-то мифическим и далеким. Это вполне реальная проблема, которая стоит перед предприятием достаточно остро.

- угрозы бывают внешние и внутренние, нельзя недооценивать ни те, ни другие причины и источники утечки корпоративной информации.

- утечка корпоративной информации может произойти как в результате злого умысла, так и в результате банальной халатности и безответственности сотрудника данного предприятия.

- при выборе системы защиты и обеспечения информационной безопасности необходимо руководствоваться степенью надежности данной системы и исключить влияние максимального количества внешних и внутренних угроз.

- необходимо постоянно осуществлять мониторинг потока информации на предприятии, отслеживать внимательным образом трафик данных.

2.2 Методы защиты предприятия от утечки информации

Каждое предприятие в своей деятельности должно разрабатывать методы по борьбе с угрозами информационной безопасности, методы, которые позволят защититься от утечки информации. Более того, некоторые методы при их правильном применении могут повысить степень защиты корпоративной сети без крупных финансовых вложений[26].

Рассмотрим основные методы борьбы с утечкой информации:

1) Осуществление более тщательного контроля действий персонала, как ни странно особенно за низкооплачиваемыми сотрудниками, за уборщиком или за охранником. Ведь именно они могут быть подосланы конкурентами с целью остаться незамеченными.

2) Проверка тактическим и корректным образом послужного списка сотрудника, который устраивается на работу на данное предприятие. Данная проверка может избавить от многих проблем предприятия с данным сотрудником в будущем.

3) Ознакомление нанимаемого сотрудника с документами, описывающими политику компании в области информационной безопасности, и получение от него соответствующей расписки[27].

4) Изменение содержимого всех экранов для входа в систему таким образом, чтобы они отражали политику компании в области защиты данных (эта мера настоятельно рекомендуется Министерством юстиции США).

5) Повышение степени физической защиты информации. Речь идет о бумагосжигателях или о машинах, которые кромсают бумагу на мельчайшие детали, из которых уже ничего нельзя выяснить.

6) Необходимо заблокировать все дисководы гибких дисков у тех пользователей, которые имеют доступ в Интернет. Это не только позволит снизить уровень хищения информаций в электронной форме, но и минимизирует процесс заражения вирусами.

7) Признание за сотрудниками определенных прав при работе с компьютерами, например организация досок объявлений, соблюдение конфиденциальности электронной почты, разрешение использовать определенные компьютерные игры. Сотрудники компании должны быть союзниками, а не противниками администратора системы в борьбе за безопасность данных[28].

До тех пор, пока Интернет не был распространен, обеспечить уровень информационной безопасности было достаточно легко и просто. Но с появлением глобальной сети, полностью на 100% обеспечить информационную безопасность практически невозможно.

В наши дни эффективным может считаться только защитное средство, работающее в симметричном режиме. Два десятилетия все пользовались моделями защиты

данных при их передаче в одном направлении. Теперь надо приспосабливать эти модели к работе с хитросплетениями двунаправленного трафика. Поэтому давайте проанализируем некоторые аспекты защиты данных, которая должна быть организована таким образом, чтобы не мешать работе сети. В компании, как правило, работают разные сотрудники, у них разные запросы в отношении доступа к данным, а кроме того, к сети обращаются и деловые партнеры компании, интересы которых могут также иметь определенную специфику. Необходимо решить, каким образом пользователи смогут обращаться к конкретным ресурсам - как в пределах организации, так и вне ее. Восприятие сети ее администратором приобретает все более серьезное значение по мере развития самого понятия сети; кроме того, совершенно новое значение приобретают виртуальные частные сети. Все связаны между собой тем или иным способом, и надо обеспечить правильное управление этими линиями связи[29].

Два критически важных правила обеспечения информационной безопасности таковы.

1) Корректная достоверная идентификация и аутентификация пользователей. Если не владеешь информацией, с кем имеешь дело, то чрезвычайно трудно управлять информационной системой.

2) Установка таких правил управления доступом в симметричном режиме, которые отражали бы политику корпорации и позволяли выявить, кто запрашивает доступ к информации.

Таким образом, в заключении раздела «Методы защиты предприятия от утечки информации» можно прийти к следующим выводам:

- проведение более тщательной проверки деятельности персонала.

- аккуратный анализ послужного списка сотрудника, который устраивается на работу на данное предприятие. Данная проверка может избавить от многих проблем предприятия с данным сотрудником в будущем.

- ознакомление нанимаемого сотрудника с документами, описывающими режим коммерческой тайны на предприятии, а также получение документального обязательства сотрудника о неразглашении коммерческой тайны предприятия.

- повышение степени физической защиты информации посредством ее удаления за ненадобностью.

- блокировать все дисководы гибких дисков у тех пользователей, которые имеют доступ в Интернет. Это не только позволит снизить уровень хищения информаций в электронной форме, но и минимизирует процесс заражения вирусами.

Также следует отметить, что Интернет значительным образом повысил уровень угроз информационной безопасности.

Выводы по главе 2.

Во второй главе данной курсовой работы «Исследование мероприятий по обеспечению информационной безопасности» можно сделать следующие выводы:

- угрозы информационной безопасности на предприятии не являются чем-то мифическим и далеким. Это вполне реальная проблема, которая стоит перед предприятием достаточно остро.

- угрозы бывают внешние и внутренние, нельзя недооценивать ни те, ни другие причины и источники утечки корпоративной информации.

- утечка корпоративной информации может произойти как в результате злого умысла, так и в результате банальной халатности и безответственности сотрудника данного предприятия.

- при выборе системы защиты и обеспечения информационной безопасности необходимо руководствоваться степенью надежности данной системы и исключить влияние максимального количества внешних и внутренних угроз.

- необходимо постоянно осуществлять мониторинг потока информации на предприятии, отслеживать внимательным образом трафик данных.

- проведение более тщательной проверки деятельности персонала.

- аккуратный анализ послужного списка сотрудника, который устраивается на работу на данное предприятие. Данная проверка может избавить от многих проблем предприятия с данным сотрудником в будущем.

- ознакомление нанимаемого сотрудника с документами, описывающими режим коммерческой тайны на предприятии, а также получение документального обязательства сотрудника о неразглашении коммерческой тайны предприятия.

- повышение степени физической защиты информации посредством ее удаления за ненадобностью.

- блокировать все дисководы гибких дисков у тех пользователей, которые имеют доступ в Интернет. Это не только позволит снизить уровень хищения информаций в электронной форме, но и минимизирует процесс заражения вирусами.

Также следует отметить, что Интернет значительным образом повысил уровень угроз информационной безопасности.

ЗАКЛЮЧЕНИЕ

Чтобы подвести какие-то итоги данной курсовой работы, стоит отметить следующие моменты:

Во второй главе курсовой работы «Исследование мероприятий по обеспечению информационной безопасности» можно сделать следующие выводы:

- угрозы информационной безопасности на предприятии не являются чем-то мифическим и далеким. Это более чем реальная проблема, которая стоит перед предприятием достаточно остро.

- угрозы бывают внешние и внутренние, нельзя недооценивать ни те, ни другие причины и источники утечки корпоративной информации.

- при выборе системы защиты и обеспечения информационной безопасности необходимо руководствоваться степенью надежности данной системы и исключить влияние максимального количества внешних и внутренних угроз.

- утечка корпоративной информации может произойти как в результате злого умысла, так и в результате банальной халатности и безответственности сотрудника данного предприятия.

- необходимо постоянно осуществлять мониторинг потока информации на предприятии, отслеживать внимательным образом трафик данных.

- проведение более тщательной проверки деятельности персонала.

- аккуратный анализ послужного списка сотрудника, который устраивается на работу на данное предприятие. Данная проверка может избавить от многих проблем предприятия с данным сотрудником в будущем.

- ознакомление нанимаемого сотрудника с документами, описывающими режим коммерческой тайны на предприятии, а также получение документального обязательства сотрудника о неразглашении коммерческой тайны предприятия.

- повышение степени физической защиты информации посредством ее удаления за ненадобностью.

- блокировать все дисководы гибких дисков у тех пользователей, которые имеют доступ в Интернет. Это не только позволит снизить уровень хищения информаций в электронной форме, но и минимизирует процесс заражения вирусами.

Также следует отметить, что Интернет значительным образом повысил уровень угроз информационной безопасности.

В ходе первой главы данной курсовой работы «Характеристика видов угроз информационной безопасности» были сделаны следующие выводы:

- угроза информационной безопасности представляет собой потенциальную возможность несанкционированного или случайного воздействия на информацию, которое приводит к ее утрате, искажению, модификации и т.д.

- угроза информационной безопасности никогда не существует обособленно, сама по себе. Угроза выступает следствием наличия слабых звеньев в системе защиты информационных систем.

- не все угрозы информационной безопасности можно отнести к следствиям какой-либо ошибки или злого умысла. Некоторые угрозы существуют, исходя из природы информационных систем.

- понятие «угроза» для разных предприятий может трактоваться совершенно по-разному. Например, для предприятий открытого типа, не существует угрозы, так как вся информация находится в широком доступе. Но таких предприятий крайне мало, поэтому в большинстве случаев нелегальный доступ представляется серьезной опасностью.

- источники информационной безопасности можно разделить на внутренние и внешние источники. К источникам внутренних угроз можно отнести следующие: - сотрудники или персонал предприятия, программное обеспечение предприятия, программные средства предприятия. Ко внешним источникам угроз информационной безопасности можно отнести вирусы, программы – шпионы, и прочие вредоносные угрозы, которые возникают со стороны Интернет.

Таким образом, предприятие должно постоянно быть на страже своих информационных интересов, которые составляют коммерческую тайну предприятия. Ведь именно информационные технологии на сегодняшний день определяют степень успеха предприятия. Поэтому их необходимо тщательно оберегать.

БИБЛИОГРАФИЯ

1. «Гражданский кодекс Российской Федерации» от 30 ноября 1994 года N 51-ФЗ.

2. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017).

3. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ.

4. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

5. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.

6. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

7. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.

8. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.

9. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

10. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

11. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с.

12. Утечка информации - [онлайн] URL: http://detective-ua.com/vitik-inform/

13. На сайте Пенсионного фонда произошла утечка данных граждан- онлайн] URL: http://stopmalware.kz/showthread.php?t=2181

ПРИЛОЖЕНИЕ 1

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с. ↑

2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с. ↑

3. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с. ↑

4. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с. ↑

5. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с. ↑

6. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с. ↑

7. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с. ↑

8. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с. ↑

9. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с. ↑

10. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с. ↑

11. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с. ↑

12. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с. ↑

13. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с. ↑

14. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с. ↑

15. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с. ↑

16. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с. ↑

17. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с. ↑

18. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с. ↑

19. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с. ↑

20. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с. ↑

21. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с. ↑

22. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с. ↑

23. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с. ↑

24. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с. ↑

25. На сайте Пенсионного фонда произошла утечка данных граждан- онлайн] URL: http://stopmalware.kz/showthread.php?t=2181 ↑

26. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с. ↑

27. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с. ↑

28. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с. ↑

29. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с. ↑