Утечка информации это - несанкционированный процесс перехода информации от источника к злоумышленнику. На данное время одной из основ безопасности информационных систем является конфиденциальность. Существует огромное количество средств и методов получения конфиденциальной информации. Я считаю, что на данный момент защита любой информации является одним из основополагающих факторов предприятия о котором оно должно заботится в первую очередь.

Для устранения утечки информации необходимо в первую очередь знать пути её утечки. В случае предприятий создаются отделы безопасности задачей которых состоит обезопасить все пути утечек информации.

[2]Особенностями утечки информации в отличии от утечки продукции

1.утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю.

2.цена информации при ее утечке уменьшается за счет тиражирования

3.факт утечки информации, как правило, обнаруживается спустя некоторое время, по последствиям, когда меры по обеспечению ее безопасности принимать могут оказаться неэффективным

Причин утечки информации несколько. На это влияет ряд факторов и обстоятельства в процессе деятельности предприятия (организации) и создают предпосылки для утечки информации. К таким факторам и обстоятельствам могут, например, относиться:

[3]1.недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;

2.использование неаттестованных технических средств обработки конфиденциальной информации;

3.слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;

4.текучесть кадров, в том числе владеющих сведениями конфиденциального характера.

[4]Выделяют следующие группы основных технических каналов утечки информации: электромагнитные; электрические; оптические; акустические.

1. К электромагнитным каналам утечки информации относят каналы возникающие за счет побочных электромагнитных излучений технического оборудования. Основой данных каналов является электрическое поле, создаваемое оборудованием. Специальные широкополосные приемники позволяют «считывать» электромагнитные излучения а затем восстанавливать и отображать содержащуюся в них информацию .

2. Электрические каналы утечки информации*.*

возникают за счет наводок электромагнитного излучения технических средств, утечек информационных сигналов в цепях заземления и питания. обработки информации и побочных электромагнитных полях работающих компьютеров производят наводки на близко расположенные коммутационные линии вспомогательных средств и систем, к которым можно отнести: охранно-пожарную сигнализацию, телефонные провода, сети электропитания, металлические трубопроводы. В этом случае возможен съем информации путем подключения специальной аппаратуры к коммуникационным линиям за пределами контролируемой территории.

3. Оптические каналы утечки информации.

Несанкционированное получение оптической информации осуществляется путем наблюдения за объектом, наиболее частый метод это фото- или видеосъемка. На данный момент существует много средств незаметной фото и виде сьёмки. Размеры самых маленьких экземпляров фото и видео сьёмки достигают 5 сантиметров что позволяет встраивать их во многие бытовые или офисные принадлежности.

*4. [5]*Акустические каналы утечки информации*.*

Наиболее распространенным способом несанкционированного доступа к информации является перехват речи и переговоров. Акустические каналы также разделяются внутри себя на 6 типов:

1) Электроакустический канал утечки информации.

Звонковая цепь проводного телефона обладает «микрофонным эффектом». Подвижные части микрофона трубки под действием звуковых волн создают минимальные колебания и соответственно минимальные электромагнитные амплитуды, что приводит к появлению в нем электрического тока. Это позволяет провести соответствующую обработку сигнала в цепи и выделить из него звуковую составляющую.

2) Виброакустический канал утечки информации реализуется путем использования электронных стетоскопов. Они снимают результаты колебания окружающих предметов. При воздействии звуковых волн на окружающие объекты (наиболее частый пример это окна). Эти волны воздействуют на чувствительный элемент датчика возбуждения и преобразуются в электрический сигнал, который в дальнейшем преобразуется в электронную запись.

3) Оптико-электронный канал утечки информации.

Довольно сложный и трудоемкий способ получения аудио информации т.к. устроен он так что данная система состоит из источника луча и приемника отражения. Передатчик формирует луч и направляет в определенную точку оконного стекла помещения при этом передатчик должен находится в относительной близости от окна. Отраженный луч модулируется речевым или акустическим сигналом, который возникает в помещении и затем принимается приемником и расшифровывается. Процессу съема информации предшествует определенная работа по наводке и настройке техники, а также он зависим от метеорологических обстоятельств

4) Проводной канал утечки акустической (речевой) информации.

В этом случае для снятия акустической информации могут использоваться проводные микрофоны, которые при помощи мембран улавливают возбуждения воздуха и преобразуют их в электронный сигнал, передаваемый затем по линии связи. Суть работы данной системы в обычном сокрытии микрофона в помещении или в элементах одежды подставных лиц. Является довольно простым, но в то же время не самым эффективным методом т.к.

В данном эссе были рассмотрены большинство технических каналов утечки информации. И большая часть их них может быть исключена обычной защитой территории, наблюдательностью и осторожностью сотрудников. Почти все утечки секретных данных планируются и в них вовлечены сотрудники подкупом или обычной невнимательностью. Так же не стоит забывать о том что утечка информации важна лишь тем кто в ней заинтересован и обычно это конкуренты.

Начинать защиту любой организации необходимо с анализа конкурентов, их методов и историю их действий. Предотвратить утечку проще чем устранить её последствия.

Список литературы:

1. Информационная безопасность и защита информации :учебник М.А. Бурова, А.С. Овсянников 2012
2. Основы инженерно-технической защиты информации: учебник Торокин А. А. 2015 – 114 стр
3. Специальная техника правоохранительной деятельности С.С. Вологодский институт права и экономики 145ст 2007г
4. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с
5. Хорев А.А. "Защита информации от утечки по техническим каналам"часть1 Технические каналы утечки информации" www.analitika.info

1. Защита информации от утечки по техническим каналам ↑

2. Основы инженерно-технической защиты информации ↑

3. Информационная безопасность и защита информации ↑

4. Технические каналы утечки информации ↑

5. Специальная техника правоохранительной деятельности ↑