**Практическая работа № 16**

**Моделирование технической разведки по исходным данным для объекта информатизации**

**Цель работы:** Приобрести практические навыки в определении степени защищенности объекта *информатизации* путем моделирования возможных действий технических разведок. Научиться определять потенциальные и реальные каналы утечки информации.

**Самостоятельная часть работы**

1.Просмотр помещения со стороны улицы, ввиду того, что помещение находится на 4 этаже, не возможен. Так как возможен просмотр помещения извне, со стороны жилого дома (который находится на расстоянии 30 метров, что очень близко) с помощью оптических приборов, существует потенциальный канал утечки видовой информации, если не закрыты шторы.

2.Так как возможно прослушивание помещения, со стороны улицы и жилого дома, через открытые окна и форточки с помощью направленных микрофонов, существует потенциальный канал утечки акустический информации.

Однако, если организационными мероприятиями введено обязательное закрытие окон и форточек во время проведения совещаний, реального акустического *канала утечки информации* нет.

Рекомендуется постоянно проверять телефоны, ПЭВМ и другую технику на предмет прослушки или видеосъемки.

В качестве дополнительной меры можно установить кондиционер или приобрести генератор белого шума и включать его во время проведения совещаний.

1. Так же возможна утечка информации возможна даже в дневное время, прослушка сторонними посетителями, а также сотрудниками, которые не имеют право на получение данной информации. Есть вероятность что дежурный может быть заказан специально для сбора информации о компании. Возможен перехват информации, просочившийся в линию электропитания, заземления с ПЭВМ. Возможен перехват информации, просочившийся в линию электропитания, заземления с телевизора.

Так как возможен съем информации о ведущихся в помещении разговорах с оконных стекол, за счет их вибрации, при использовании лазерного микрофона, при расположении поста перехвата в жилом доме, существует еще один потенциальный канал утечки акустической информации.

В данном случае с помощью одних организационных мероприятий устранить канал утечки не представляется возможным. Однако реальное существование канала утечки может быть констатировано лишь после проведения инструментальных измерений.

По результатам инструментальной проверки будет определяться необходимость проведение защитного мероприятия, например, установка рифленых стекол или зашумление стекол и пространства между ними.

1. Телефон, телевизор и радиотрансляционный приемник могут быть в любое время оборудованы средствами прослушки или видеосъемки, так как доступ в помещение не ограничен ни для сотрудников, ни для посетителей. Если две линии проводной связи имеют протяженный параллельный пробег, то существует вероятность съема информации за счет паразитных связей - между каналом оперативной связи и однопрограммным радиоприемником радиотрансляционной сети.

Если в помещении электросеть (она есть везде), возможные помехи на бытовых приборах при использовании электросети для передачи информации, а также плохое качество передаваемого сигнала при большом количестве работы бытовых приборов, подключена линия телефонного аппарата, то допускается акустоэлектрический канал утечки информации. Акустоэлектрический канал утечки информации в основном используется для перехвата разговоров, ведущихся в помещении.

Для предотвращения утечки информации необходима трансформаторная развязка. Она является препятствием для дальнейшей передачи информации по сети электропитания. Предотвращение утечки информации через системы пожарной и охранной сигнализаций осуществляется отключением датчиков пожарной и охранной сигнализации на период проведения важных мероприятий, содержащих конфиденциальную информацию, или применением датчиков, не требующих специальных мер защиты.

1. Возможен перехват информации стетоскопами, комплексированными радиопередатчиками и передатчиками в ИК-диапазоне через систему вентиляции. При оценке защищенности объектов (помещений) от утечки речевой информации необходимо учитывать возможность их случайного прослушивания как из соседних помещений, так и извне. Поэтому следует обращать внимание на возможность возникновения каналов утечки речевой (или иной акустической информации) через открытые (неплотно закрытые) двери и окна, через воздуховоды систем вентиляции, трещины строительных конструкций и т.п. Также следует проводить оценку возможности ведения разведки с использованием лазерных микрофонов и направленных микрофонов. Подобная оценка производится с учетом возможности размещения на опасных расстояниях постов перехвата. Интерес могут вызывать структурные каналы утечки акустической информации, образующиеся в строительных конструкциях, проходящих через помещения трубах отопления, коробах вентиляции и т.п.

В данном случае с наибольшей вероятностью утечка информации может произойти через трубы отопления, так как там находятся менее охраняемые помещения, через служебные помещения на крышу забраться при должной охране будет невозможно, но поскольку посетители и сотрудники перемещаются по всему зданию в рабочее время, то это представляется возможным.

1. Оценка разведдоступности объекта для агентурного проникновения включает в себя анализ режима работы и охраны объекта с целью моделирования действий по скрытному проникновению на них (неконтролируемому пребыванию) посторонних лиц и режим работы специалистов сторонних организаций – т.е. всю совокупность условий, позволяющих внедрить на объект специальные закладные устройства перехвата информации. Кроме того, необходимо учесть возможность применения злоумышленником контактных микрофонов (стетоскопов), на основе которых конструируются так называемые «беззаносные» устройства негласного съема акустической информации.

Так же стоит внимательно отнестись к приему на работу сотрудников, так как их могут подослать злоумышленники или конкуренты. Дежурный не дает сто процентной защиты от утечки информации, так как он может быть заказан специально для этой цели или у него есть свой план по сбору информации предприятия.

1. Если штатные сотрудники не разграничены, то вероятность утечки информации только повышается, т.к. в наше время очень много случаев, когда в организациях находились подставные сотрудники. Для того, чтобы избежать этой ситуации нужно очень внимательно относится к трудоустройству сотрудников в свою организацию, проверять связи с другими организациями, прошлые места работы, разграничить штат сотрудников, контролировать доступ к служебной информации, не допускать посторонних лиц в служебные помещения.