**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.

**Ход работы:**

**Потенциально возможные каналы утечки информации:**

1. Так как возможен просмотр помещения извне, со стороны жилого дома с помощью оптических приборов, существует потенциальный канал утечки видовой информации.

Однако, если организационными мероприятиями введено обязательное зашторивание окон во время проведения совещаний, работы с документами и т.п., то реального визуально-оптического канала утечки информации нет.

В качестве дополнительных мер можно ввести периодический контроль за соблюдением сотрудниками правила зашторивания, а также поставить тонированные или рифленые стекла.

1. 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.

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

1. 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.

**Возможные действия технических разведок, реальные каналы утечки информации:**

Устройства по типу телефона, телевизора и радиотрансляционного приемника могут быть в любое время оборудованы средствами прослушивания 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.

Для предотвращения утечки информации необходима трансформаторная развязка. 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.

При оценке защищенности объектов от утечки речевой информации необходимо учитывать возможность их случайного прослушивания как из соседних помещений, так и извне. Следует обращать внимание на возможность возникновения каналов утечки речевой через открытые 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.

**Вывод:** Я приобрел практические навыки в определении степени защищенности объекта информатизации путем моделирования возможных действий технических разведок и научился определять потенциальные и реальные каналы утечки информации.