**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 работа:**

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 с помощью оптических приборов, существует потенциальный канал утечки видовой информации.

Однако, если организационными мероприятиями (соответствующим инструктажем ответственных лиц) введено обязательное зашторивание окон вовремя проведением 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.

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

В заключение первого этапа можно предложить установку стекол с рифленой поверхностью и кондиционера. Решение представляется оптимальным, т.к. акустический и визуально оптический каналы устраняются при минимальных финансовых затратах. Также, в дальнейшем, обеспечивается *удобство эксплуатации* объекта и исключается негативный *человеческий фактор*.

При оценке вероятности использования технической разведкой потенциальных каналов утечки информации следует принимать во внимание окружающую обстановку, с точки зрения возможности по организации и ведению технической разведки, а именно:

* скрытное размещение поста перехвата (для прослушивания и просмотра помещения) на улице с интенсивным движением затруднительно, т.к. подозрительные лица, транспортные средства и т.п. привлекают к себе внимание, легко визуально обнаруживаются;
* скрытное размещение поста перехвата (для прослушивания и просмотра помещения, установки лазерного микрофона) в жилом здании, если, например, арендовать квартиру с окнами, расположенными напротив окон защищаемого помещения, вполне реализуемо.

Необходимо, если имеется такая возможность, проверить благонадежность (лояльность) жильцов в квартирах, потенциально пригодных для организации поста перехвата (сдаются ли квартиры, проживают ли в квартирах потенциальные конкуренты, имеются ли лица, бывшие в конфликте с законом и т.п.). Возможности организации постов перехвата на технических этажах и т.п.

В случае получения в ходе проверки положительных данных можно заключить, что защитные мероприятия не требуются вообще. С точки зрения защиты от случайных утечек, например, прослушивания, можно заключить, что улица с интенсивным автомобильным и пешеходным движением создает достаточно сильную акустическую помеху, за которой разговоры случайными прохожими различаться не будут. При необходимости в этом можно убедиться экспериментально.

В случае получения в ходе проверки отрицательных или неоднозначных данных оптимальным остается вариант указанный в заключение первого этапа.

Мои варианты:

1) Так как, есть угроза утечки информации через сотрудников, посетителей, рабочих из других сфер (электрики, рабочие, которые привозят воду и меняют её в кулерах). Утечка информации через носители, микрофоны, прослушки, находящиеся на телах сотрудников, рабочих посетителей, должен организоваться, пост проверки на входе для, посетителей организации.  
  
Пост будет проверять людей на наличие носителей прослушивания или записи информации. В положительном случае запрещенные предметы будут изыматься, а нарушители будут должны покинуть здание организации.

2) Есть угроза похищения данных организации с помощью вирусов. Конкуренты отправляют на почту организации, или же сотруднику письмо с спам-рассылкой, где содержится вирусный файл, с помощью которого крадут данные с компьютеров сотрудников.

Во избежание этого, нужно создать блокирующий протокол, который будет проверять автоматически все письма с почт сотрудников и удалять вредоносные письма.