МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«___» _____ 2017 г.

МОДЕЛИРОВАНИЕ ТЕХНИЧЕСКОЙ РАЗВЕДКИ ПО ИСХОДНЫМ ДАННЫМ ДЛЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Методические рекомендации по выполнению лабораторной работы №11
для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: А.Л. Ханис

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» М.А. Ефремов

Моделирование технической разведки по исходным данным для объекта информатизации [Текст] : методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. – Курск, 2017. – 10 с. – Библиогр.: с. 10.

Содержат сведения по вопросам изучения степени защищенности объекта. Указывается порядок выполнения лабораторной работы, правила оформления отчета.

Методические рекомендации соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать 24.11.17. Формат 60x84 1/16.
Усл.печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 100 экз. Заказ. Бесплатно. 257
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

1. 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 и угрозы несанкционированного доступа.

2. Краткая вводная часть

Для того чтобы построить эффективную систему информационной безопасности, необходимо в первую очередь определить потенциальные и реальные угрозы технического проникновения на защищаемый объект, возможные каналы для несанкционированного доступа и утечки защищаемой информации.

Данная работа базируется на знании возможностей и методов ведения технической разведки (необходимо учитывать также возможность непреднамеренного получения информации, при ее случайной утечке, лицами которым она не предназначена).

Успешная реализация этого этапа позволит, в дальнейшем спланировать и построить эффективную систему защиты объекта, при оптимальных затратах на проведение организационных и технических защитных мероприятий и минимуме неудобств для персонала, при последующей эксплуатации объекта.

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное оборудование технических средств обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т.п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др.

В качестве каналов утечки большой интерес представляют вспомогательные средства, имеющие линии выходящие за пределы

контролируемой зоны. а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При оценке защищенности объектов (помещений) от утечки речевой информации необходимо учитывать возможность их прослушивания как из соседних помещений (если есть такая необходимость) так и извне. В данном случае следует обращать внимание на возможность возникновения каналов утечки речевой (другой акустической информации) через открытые (не плотно 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. В названных случаях оценка производится с учетом возможности размещения на опасных расстояниях постов перехвата. Интерес могут вызывать каналы утечки за счет структурного звука в строительных конструкциях, проходящих через помещения трубах отопления и т.п.

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. Режим работы специалистов сторонних организаций, приобретение, установка и ремонт мебели, оргтехники и т.п. Т.е. всю совокупность условий позволяющих внедрить на объект специальные закладные устройства перехвата информации (микропередатчики, возможность установки миниатюрных микрофонов с подключением к внешним линиям и т.д.). А также определение наиболее эффективных, для использования на разных уровнях проникновения, средств технической разведки.

Большое, а иногда решающее, значение при оценке угрозы может иметь знание наиболее вероятного противника, его финансовых и оперативных возможностей, знание личностных качеств постоянного персонала, временных работников и другая дополнительная информация

3. Пример моделирования действий технической разведки

Примерная характеристика защищаемого объекта (исходные данные)

1. Защищаемое помещение расположено на втором этаже 3-х этажного здания.

Все здание принадлежит одной организации.

Сверху расположены служебные помещения.

Снизу расположены технические помещения (туалет, электрощитовая).

Со стороны стены Б расположена приемная.

Со стороны стены Г расположен общий коридор.

Стороны А и В выходят на улицы с интенсивным пешеходным и транспортным движением.

Окна помещения оборудованы шторами, смотрят на жилой дом расположенный на расстоянии 30 метров.

2. Из мебели в помещении установлены рабочий и журнальный столы, стулья, подставки под: телефоны, ПЭВМ и телевизор.

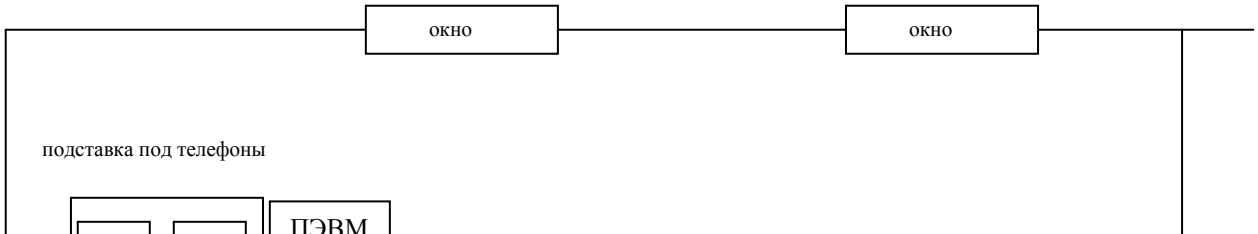
3. Из основных технических средств в помещении установлен телефон внутренней конфиденциальной связи, ПЭВМ включенная в локальную сеть.

4. Из вспомогательных технических средств в помещении установлен телефон ГТС, телевизор, радиотрансляционный приемник. Помещение оборудовано системой пожарной и охранной сигнализации, линии которых выходят на пульт дежурного охранника. Помещение электрифицировано (освещение, питание оборудования).

5. Помещение оборудовано системой вытяжной вентиляции, короб которой проложен вдоль коридора и поднимается на крышу здания. Радиаторы отопления установлены вдоль стены А. Трубы отопления спускаются в подвал.

6. Режим работы учреждения предусматривает свободное передвижение сотрудников и посетителей в рабочее время. В ночное время помещение закрывается на ключ, сдается под охрану дежурному. Системы связи обслуживаются штатным сотрудником. Системы жизнеобеспечения (отопление, канализация) обслуживаются по заявке приходящим сотрудником.

7. Доступ штатных сотрудников к служебной информации не разграничен.



Пример рассуждения при определении степени защищенности объекта от возможных действий технической разведки

В качестве примера приведена оценка разведдоступности помещения со стороны окон. При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допущено использование оговорок типа « если.... то....».

1

Просмотр помещения со стороны улицы, ввиду того, что помещение находится на 2 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 во время проведением совещаний, работы с документами и т.п., то реального визуально оптического канала утечки информации нет.

Исходя из этого условия, в последующем, будет определяться необходимость проведения защитного мероприятия, например, для исключения отрицательного человеческого фактора – постоянно следить за зашториванием окон, можно установить тонированные или рифленые стекла.

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 (соответствующим инструктажем ответственных лиц) введено обязательное закрытие окон и форточек во время проведения совещаний, реального акустического канала утечки информации нет.

Исходя из этого условия, в последующем, будет определяться необходимость проведения защитного мероприятия, например, для исключения отрицательного человеческого фактора - постоянно следить за состоянием окон, можно установить кондиционер.

3. 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.

Впрочем возможны другие варианты, с учетом дизайнерских и прочих решений.

2

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.

4. <u>Самостоятельная часть работы</u>

В самостоятельной части работы предлагается:

- выявить оставшиеся, потенциально возможные каналы утечки информации (с учетом исходных данных, используя, при необходимости оговорки);
- смоделировать возможные действия технических разведок, определить реальные каналы утечки информации;
- доказать целесообразность и предложить проведение тех или иных защитных мероприятий.

Примечание: При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допускается использовать оговорку типа « если.... то....».

5. Оформление результатов

Результаты работы оформляются каждым студентом письменно в форме отчета. Отчет должен содержать обоснованные определения потенциальных и реальных каналов утечки информации и выбора защитных мероприятий. Форма изложения произвольная.