**Лабораторная работа «Разработка модели угроз защищаемого объекта»**

**Цель.** Построение модели угроз безопасности защищаемого объекта информатизации.

**Задачи**

1) Определение перечня угроз безопасности объекта.

2) Анализ каналов утечки информации.

3) Построение модели угроз с учетом каналов утечки.

4) Разработка модели вероятного нарушителя.

**Определение перечня угроз безопасности объекта**

Угроза - потенциальная возможность совершения действий направленных на нарушение безопасности объекта.

Проявление угроз (фактор неопределенности):

– действие нарушителей;

– воздействие стихийных сил;

– сбои в работе средств СФЗ;

– воздействие субъективного фактора.

Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых на объекте и условий расположения и эксплуатации объекта.

Для составления перечня угроз необходимо:

– определить перечень актуальных источников угроз;

– определить перечень актуальных уязвимостей;

– оценить взаимосвязь угроз, источников угроз и уязвимостей;

– определить перечень возможных атак на объект;

– описать возможные последствия реализации угроз.

**Угрозы утечки информации по техническим каналам.**

1) Угрозы утечки речевой (акустической) информации по техническим каналам.

2) Характеристика угроз перехвата видовой (графической) информации ограниченного доступа визуально­оптическими средствами.

3) Угрозы утечки информации ограниченного доступа по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

**Технический канал утечки информации**- совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Утечка информации**- неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней и ее получения разведками.

**Утечка (защищаемой) информации по техническим каналам -**неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Основные элементы описания угроз утечки информации по техническим каналам представлены на рисунке 3.1.



Рисунок 3.1 - Основные элементы угроз утечки информации

**Носитель защищаемой информации** - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Задание 1.** Составить перечень угроз для заданного объекта по образцу таблицы 3.1.

Таблица 3.1 - Перечень угроз

|  |  |  |  |
| --- | --- | --- | --- |
| № угрозы | Источник угрозы | Среда распространения | Носитель информации |
|   |   |   |   |
|   |   |   |   |

Каналы утечки информации по физическим принципам можно классифицировать на следующие группы:

- акустические (включая и акустопреобразовательные);

- визуально-оптические (наблюдение, фотографирование);

- электромагнитные (в том числе магнитные и электрические);

- материально-вещественные (бумага, фото, магнитные носители и т.п.).

При использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

– акустическое излучение информативного речевого сигнала;

– электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам, выходящими за пределы КЗ;

– виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

– несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

– воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;

– побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;

– наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

– радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств;

– радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;

– радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

– прослушивание ведущихся телефонных и радиопереговоров;

– просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

– хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

**Задание 2.** Провести анализ потенциальных каналов утечки на указанном объекте. Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу таблицы 3.2.

Таблица 3.2 - Перечень потенциальных каналов утечки информации

|  |  |
| --- | --- |
| Каналы утечки информации с объекта защиты | Место расположения |
| 1. | Оптический канал | Окно со стороны проспекта | каб. №1 |
| Окно со стороны проспекта | каб. №2 |
| Окно со стороны проспекта | каб. №3 |
| 2. | Радиоэлектронный канал | Стоянка автотранспорта на просп. | указать |
| Система часофикации | указать |
| Телефон | указать |
| Розетки | указать |
| ПЭВМ | указать |
| Воздушная линия электропередачи | указать |
| Система оповещения | указать |
| Система пожарной сигнализации | указать |
| 3. | Акустический канал | Теплопровод подземный | указать |
| Водопровод подземный | указать |
| Стены помещения | указать |
| Батареи | указать |
| Окна контролируемого помещения | указать |
| 4. | Материально-вещественный канал | Документы на бумажных носителях | указать |
| Персонал предприятия | указать |
| Производственные отходы | указать |

Моделирование угроз безопасности информации предусматривает анализ способов её хищения, изменения, уничтожения с целью оценки наносимого ущерба. Моделирование угроз включает моделирование:

– способов физического проникновения;

– технических каналов утечки информации.

Возможные пути проникновения злоумышленника отмечаются на планах, схемах территорий, этажей помещений линиями. Результаты оформить в виде следующей модели, показанной в таблице 3.3.

Таблица 3.3 – Модель угроз защищаемого объекта

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № элемента | Цена информации | Путь проникновения | Оценка реальности | Величина угрозы | Ранг угрозы |

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

 Моделирование технических каналов утечки информации (ТКУИ) является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты. Целесообразно рассматривать каналы в статике и динамике. Статическое состояние характеризует пространственное состояние структурной модели, описывает состав и связи элементов канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве: места расположения источника и приёмника сигналов. Ориентация вектора распространения носителя информации в канале утечки и его протяжённость структурную модель целесообразно представить в табличной форме. Пространственную – в виде графов на планах помещений.

Динамику канала утечки описывает **функциональная и информационная модель.** Функциональная модель характеризует режимы функционирования канала: это может быть интервал времени, в течении которого возможна утечка. Информационная модель содержит характеристики информации, утечка которой возможна по техническому каналу(количество и ценность).

 Указанные модели объединяются и увязываются между собой в рамках комплексной модели канала утечки. В ней указываются интегрированные параметры утечки – источник информации, его вид, ист-к сигнала, среда распространения, протяжённость среды распространения, возможное место размещения приёмника сигнала, информативность канала, величина угрозы. Все выявленные потенциальные каналы утечки и их характеристики заносятся в таблицу 3.4.

Таблица 3.4 – Комплексная модель каналов утечки

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Цена информации | Источник сигнала | Путь утечки | Вид канала | Оценка реальности | Величина угрозы/ранг |
|   |   |   |   |   |   |   |

Оценка угроз информации в результате проникновения злоумышленника к источнику или в результате её утечки по ТКУИ проводится с учётом вероятности реализуемости рассматриваемого пути или канала, а также с учётом цены соответствующего элемента информации. Угроза безопасности информации выражается в величине ущерба при захвате её к злоумышленником, где - цена элемента информации - вероятность угрозы.

**Задание 3.** Построить модель угроз и комплексную модель каналов утечки информации для заданного объекта.

**Под моделью нарушителя** понимается совокупность количественных и качественных характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны и/или его составным частям.

**Составляющие модели нарушителя:**

– категории нарушителя и его возможные тактические методы (внешние, внутренние, внешние в сговоре с внутренними);

– возможные действия нарушителя (применение силы, хищение, дезинформация и т.д.);

– причины и мотивы действий нарушителя (корысть, принуждение и т.д);

– возможности нарушителя (навык, опыт, количество, оснащенность-техника, оружие, транспорт).

**«**Внешний нарушитель» - нарушитель из числа лиц, не имеющих права доступа в охраняемые зоны;

«Внутренний нарушитель» - нарушитель из числа лиц, имеющих право доступа без сопровождения в охраняемые зоны;

«Внешняя угроза» - угроза, исходящая от внешнего нарушителя;

«Внутренняя угроза» - угроза, исходящая от внутреннего нарушителя.

Для описания моделей нарушителей в качестве критериев классификации рассматриваются:

1. Цели и задачи вероятного нарушителя:

- проникновение на охраняемый объект без причинения объекту видимого ущерба;

- причинение ущерба объекту;

- преднамеренное проникновение при отсутствии враждебных намерений;

- случайное проникновение.

2. Степень принадлежности вероятного нарушителя к объекту:

- вероятный нарушитель - сотрудник охраны;

- вероятный нарушитель - сотрудник учреждения;

- вероятный нарушитель - посетитель;

- вероятный нарушитель - постороннее лицо.

3. Степень осведомленности вероятного нарушителя об объекте:

- детальное знание объекта;

- осведомленность о назначении объекта, его внешних признаках и чертах;

- неосведомленный вероятный нарушитель.

4. Степень осведомленности нарушителя о системе охраны объекта:

- полная информация о системе охраны объекта;

- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;

- информация о системе охраны вообще, но не о системе охраны конкретного объекта;

- неосведомленный вероятный нарушитель.

5. Степень профессиональной подготовленности вероятного нарушителя:

- специальная подготовка по преодолению систем охраны;

- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.

6. Степень физической подготовленности вероятного нарушителя:

- специальная физическая подготовка;

- низкая физическая подготовка.

7. Владение вероятным нарушителем способами маскировки.

8. Степень технической оснащенности вероятного нарушителя.

9. Способ проникновения вероятного нарушителя на объект.

На основе изложенных критериев выделяют четыре категории нарушителя:

1) нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель-профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов;

2) нарушитель второй категории - непрофессиональный нарушитель с враждебными намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект;

3) нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;

4) нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

Модели нарушителя по типу бывают: неформализованные, формализованные.

**Неформализованная** модель нарушителя представляет собой словесное описание его, отражает причины и мотивы действий, его возможности, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей, способы реализации исходящих от него угроз, место и характер действия, возможная тактика.

**Формализованная** модель нарушителя представляет собой математическое описание его, которое обычно строится на основе теории игр, когда для создания защитной системы используется матрица угроз/средств защит и матрица вероятностей наступления угроз. Типовая модель нарушителя представлена на рисунке 3.2.



Рисунок 3.2 - Типовая модель нарушителя

**Задание 4.**

1)Провести анализвероятных внешних и внутренних нарушителей.

2) Построить модель вероятного нарушителя (внешнего и внутреннего) на основе моделей угроз и утечки информации.

Варианты объектов защиты

|  |  |
| --- | --- |
| № варианта | Объект информатизации |
| 1 | Бухгалтерия завода железобетонных изделий |
| 2 | Помещения дирекции торгового центра |
| 3 | Медпункт учебного корпуса университета |
| 4 | Деканат факультета университета |
| 5 | Отдел главного конструктора приборного завода |
| 6 | Зал переговоров фирмы по изготовлению лекарственных средств |
| 7 | Следственный отдел прокуратуры |
| 8 | Помещение группы программистов коммерческого банка |
| 9 | Патентный отдел завода |
| 10 | Редакция научного издания |
| 11 | Отдел научно-исследовательского института |
| 12 | Помещения диссертационного совета университета |
| 13 | Рекламное агентство |
| 14 | Отдел кадров завода бурового оборудования |
| 15 | Конструкторское бюро завода оборонной промышленности |

**Контрольные вопросы**

1 Что является исходными данными для проведения оценки и анализа угроз безопасности объектов?

2 Дать определение нарушителя, по каким критериям они классифицируются?

3 Дать определение технического канала утечки информации, назвать типы.

4 Дать определение носителя защищаемой информации, назвать типы.

5 Какие сведения включает пространственная модель каналов утечки?

6 Что такое формализованная и неформализованная модель нарушителя?

7 Перечислите цели и задачи вероятного нарушителя.

8 Какое оборудование относят к виброакустические каналам утечки информации?

9 Дать описание четырех категорий нарушителя.

10 Что представляет собой матрица угроз/средств защит и матрица вероятностей наступления угроз?