### Практическая работа № 3. Анализ источников угроз и путей проникновения нарушителя

**Цель.** Формирование перечня источников угроз и каналов утечки информации на защищаемом объекте.

### Задачи.

1. Дать характеристику объектов воздействия и источников угроз физической безопасности.
2. Проанализировать уязвимости объекта.
3. Дать характеристику каналов утечки информации.
4. Построить схему путей проникновения нарушителя на объект.

**Задание 1. Характеристика объектов воздействия источников угроз физической безопасности.** Самый общий перечень угроз физической безопасности включает:

* + диверсии;
  + терроризм;
  + негативное воздействие на технологические процессы;
  + кража материальных и финансовых ценностей;
  + кража и воздействия на информацию и ее носители;
  + воздействия стихийных сил.

Все эти угрозы направлены на объекты угроз. Составить список объектов, подлежащих защите, оценить вид и масштаба ущерба с помощью вербальных показателей, и занести их в таблицу 7.10.

Таблица 7.10 – Объекты защиты, виды ущерба

|  |  |  |
| --- | --- | --- |
| Объекты защиты | Вид ущерба | Уровень ущерба |
| 1 | 2 | 3 |
| персонал | Физический, моральный,  экономический | высокий |

Продолжение таблицы 7.10

|  |  |  |
| --- | --- | --- |
| 1 | 2 | 3 |
| технологические  процессы | Материальный,  экономический | высокий |
| оборудование | Материальный,  экономический | средний |
| готовая продукция | Материальный,  экономический | высокий |
| интеллектуальная  собственность | Экономический | высокий |
| средства  вычислительной техники | Материальный,  экономический | средний |
| Конфиденциальная информация | Потеря репутации компании,  материальный, экономический | высокий |
| Заполнить по данным  защищаемого объекта | Заполнить по данным  защищаемого объекта | Заполнить по данным  защищаемого объекта |

Проанализировать виды источников угроз, сформировать перечень источников угроз и занести их в таблицу 7.11.

Таблица 7.11 – Виды источников угроз безопасности

|  |  |  |
| --- | --- | --- |
| Вид источника угроз | | Перечень источников угроз |
| Техногенные | внешние | Средства связи, сети электропитания |
| Системы кондиционирования |
| Технические средства обработки  информации |
| Сети инженерных коммуникаций |
| Заполнить по объекту |
| внутренние | Неправильная конфигурация средств  защиты |
| Сбои в работе СКУД |
| Заполнить по объекту |
| Антропогенные | Внешние нарушители | Заполнить по объекту |
| Внутренние нарушители | Заполнить по объекту |
| Стихийные |  | Заполнить по объекту |

### Задание 2. Проанализировать уязвимости объекта.

Анализ уязвимости - совокупность действий, направленных на выявление уязвимых мест физической защиты объекта. Фактор, влияющий на уязвимость (фактор уязвимости) - признак наличия уязвимого места в физической защите.

Уязвимые места - элементы физической защиты, преодолевая которые нарушитель имеет наибольшую вероятность совершения диверсии или хищения ценных ресурсов предприятия. Все уязвимости можно разбить по их принадлежности к определенным подсистемам системы физической защиты. Сформулировать факторы уязвимостей защищаемого объекта по примеру таблицы 7.12.

Таблица 7.12 – Факторы уязвимостей защищаемого объекта

|  |  |
| --- | --- |
| Уязвимости  подсистем | Факторы уязвимости |
| 1 | 2 |
| Уязвимости подсистемы обнаружения | Входы (выходы) в зданиях, сооружениях и помещениях, расположенных во внутренней и особо важной зонах, не оборудованы техническими средствами обнаружения, средствами оптико-электронного наблюдения и управления  доступом. |
| Не обеспечено автоматическое переключение электропитания  ТСФЗ на резервные источники при отключении основной системы. |
| Отсутствует автоматический дистанционный контроль  работоспособности ТСФЗ. |
| Система оптико-электронного наблюдения не имеет  подсистему видеозаписи и ее сохранения. |
| Заполнить |
| Уязвимости подсистемы задержки | Входы (выходы) в зданиях, сооружениях и помещениях, расположенных во внутренней и особо важной зонах, не оборудованы замковыми устройствами, техническими средствами обнаружения, средствами оптико-электронного  наблюдения и управления доступом. |
| Физические барьеры, замедляющие проникновение нарушителя в охраняемую зону, находятся не на всех участках  охраняемой зоны. |
| Проемы, окна, вентиляционные короба, технологические  проходы не обеспечены физическими барьерами. |
| Заполнить |

Продолжение таблицы 7.12

|  |  |
| --- | --- |
| 1 | 2 |
| Уязвимости действий подразделений охраны | Время реагирования подразделений охраны не обеспечивает перехват нарушителя на возможных  маршрутах следования нарушителя. |
| Не соответствуют ведомственным нормативным документам по организации охраны ОИАЭ и порядку несения службы подразделениями охраны следующие характеристики подразделений охраны:   * укомплектованность личным составом, * обеспеченность вооружением, транспортом и средствами связи, * профессиональная подготовка, прохождение периодической аттестации. |
| Заполнить |
| Уязвимости подсистемы организационных мероприятий | Не соответствуют объему и характеру предъявляемых требований следующие организационно-распорядительные документы:   * положение о службе безопасности, * положение о пропускном режиме и разрешительной системе допуска и доступа, * план охраны.   Не установлен порядок выдачи и хранения ключей от охраняемых помещений. |
| Заполнить |

### Задание 3. Дать характеристику каналов утечки 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,

др.).

Провести анализ потенциальных каналов утечки на заданном объекте.

Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу таблицы 7.13.

Таблица 7.13 - Перечень потенциальных каналов утечки информации

|  |  |  |
| --- | --- | --- |
| Каналы утечки информации с объекта защиты | | Место  расположения |
| Оптический канал | Окна со стороны проспекта | каб. №1 |
| Окна, выходящие на улицу | каб. №2 |
| Окна, выходящие во внутренний  двор | каб. №3 |
| 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 |
| Акустический канал | Теплопровод подземный | указать |
| Водопровод подземный | указать |
| Стены помещения | указать |
| Батареи | указать |
| Окна контролируемого помещения | указать |
| Материально- вещественный канал | Документы на бумажных носителях | указать |
| Персонал предприятия | указать |
| Производственные отходы | указать |

**Задание 4. Построить схему путей проникновения нарушителя на объект.** Несанкционированное проникновение на объект осуществляется в основном через окна, двери, балконы; на периметр - через проходную, лазы в заборе и непосредственно через ограду. Проанализировать возможные пути проникновения нарушителя и обозначить их на плане защищаемого объекта. Образец схемы проникновения представлен на рисунке 7.4.



Рисунок 7.4 – Пути проникновения нарушителя на объект

### Контрольные вопросы.

1. Дать определение понятия «источник угроз безопасности». На какие классы подразделяются все источники угроз безопасности?
2. Охарактеризовать антропогенные источники угроз безопасности. Привести перечень возможных внешних и внутренних нарушителей.
3. Дать характеристику внутренних и внешних техногенных источников угроз безопасности.
4. Дать определение понятий «уязвимость физической защиты»,

«фактор уязвимости». Кратко пояснить, как определяются уязвимости физической защиты.

1. Назовите типичные уязвимости подсистемы организационных мероприятий.
2. Дать определение технического канала утечки информации, назвать типы каналов утечки.
3. Какие сведения включает пространственная модель каналов утечки?