**КУРСОВАЯ РАБОТА**

по дисциплине: **«Инженерно-техническая защита информации»**

Тема работы: **«Разработка системы защиты объекта**»

**СОДЕРЖАНИЕ**

Введение………………………………………………………………………….. ...3

1.Моделирование объекта защиты…………………………………………..….. 4

1.1.Описание объекта защиты……………………………………………..….4

1.2.Моделирование объектов защиты………………………………….….… 5

1.3.Моделирование возможных каналов утечки информации………….......9

1.4.Оценка степени угрозы защищаемой информации………………….…12

2.Моделирование мероприятий инженерно-технической защиты

информации объекта защиты……………………………………………….…...17

2.1.Разработка модели скрытия вида деятельности организации

(объекта)……………………………………………………………………….17

2.2.Разработка мероприятий по технической защите информации на объекте защиты…………………………………………………………………….18

2.3.Разработка модели охранной и пожарной сигнализации объекта (помещения)………………………………………………………………………...22

2.4.Расчет зон распространения акустических и электромагнитных

волн с объекта защиты с масштабной привязкой на местности…………...23

2.5.Заполнение шаблона базы данных технических средств защиты информации помещения (объекта)…………………………………………….….27

3.Оценка эффективности и возможностей средств защиты информации……28

3.1.Оценка степени защиты информации на объекте………………………28

3.2.Экономическая оценка стоимости средств защиты информации……..32

Заключение…………………………………………………………………………33

Список использованных источников…………………………………..…………34

**ВВЕДЕНИЕ**

Мы живем в мире информации. Информация - сведения о лицах, фактах, событиях, явлениях и процессов независимо от формы их представления. Владение информацией во все времена давало преимущества той стороне, которая располагала более точной и обширной информацией, тем более, если это касалось информации о своих соперниках.

Проблема защиты информации существовала всегда, но в настоящее время из-за огромного скачка научно-технического прогресса она прибрела особую актуальность. Поэтому задача специалистов по защите информации, заключается в овладении всего спектра приемов и способов защиты информации, научится моделировать и проектировать системы защиты информации.

Целью данной работы является описание и построение наиболее полной модели объекта защиты. Приводится список защищаемой информации, её носители, возможные пути утечки, технические каналы утечки, проводится моделированием угроз безопасности информации.

Курсовая работа включает в себя 3 главы:

- Моделирование объекта защиты;

- Моделирование мероприятий инженерно-технической защиты

информации объекта защиты;

- Оценка эффективности и возможностей средств защиты информации;

Данная работа преследует целью научить нас всесторонне и комплексно анализировать объект защиты с целью выявления наиболее опасных каналов утечки информации и тем самым предупредить возможные потери.

Курсовая работа выполнена на 34 листах, содержит 18 таблиц, 1 рисунок и 6 приложений

1. **МОДЕЛИРОВАНИЕ ОБЪЕКТА ЗАЩИТЫ**
   1. **Описание объекта защиты**

В данной курсовой работе представлен объект защиты – частное предприятие, занимающееся производством медицинских препаратов ООО «Авицена».

Объект защиты расположен на пересечении проспекта Сталинграда и ул. Мира. С северной и северо-восточной стороны от него проходит подземный теплопровод (1). С западной стороны на расстоянии 40 метров расположены служебное здание (2), пункт водоснабжения (К – колодец, 140 суточный дебит воды, м3) (3) и вдоль ул. Мира воздушная линия электропередачи (4).

С юго-западной стороны от объекта на удалении 45 метров находятся торговый павильон (5), служебное здание (6) и главная центральная районная больница, рассчитанная на 300 коек (общее количество больниц в районе – 7 (5000 коек)) (7). На южной стороне от объекта через проспект Сталинграда расположен газон (8), а в юго-восточном направлении находятся подземный водопровод (9) и телефонная станция (7 метров от объекта защиты) (10).

Объект защиты представляет собой двухэтажное здание. Помещение, в котором обрабатывается секретная информация, расположено на втором этаже и разделено на три комнаты и коридор. Материал стен: внешние – железобетонные блоки (толщина блока - 300мм), внутренние - отштукатуренные с двух сторон (толщина - 1,5мм). Остекленение одинарное (3мм). Двери звукоизолирующие тяжелые.

Так же на территории объекта защиты расположены системы: громкоговорящий связи, оповещения, энергоснабжения, часофикации, автоматизированная система управления и телефон.

Наиболее вероятные направления угроз объекту защиты во взаимосвязи с инфраструктурным и коммуникационным обеспечением представлены в приложении 1

* 1. **Моделирование объектов защиты**

Для создания полной модели объекта защиты необходимо для начала определить ту информацию, которую необходимо защищать, поэтому необходимо провести её структурирование.

Структурирование производится путем классификации защищаемой информации в соответствии с функциями, задачами и дальнейшей привязкой элементов информации к их носителям. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Моделирование состоит в анализе на основе пространственных моделей возможных путей распространения информации за пределы контролируемой зоны.

Для выбранного объекта защиты структурная модель защищаемой информации, приведена ниже.

#### Конфиденциальная информация

Об организации

О внутренней деятельности организации

О внешней деятельности организации

* структура предприятия
* личные сведения о сотрудниках фирмы
* финансы

- безопасность предприятия

* качество медикаментов
* характеристики разрабатываемой продукции
* технологии производства

- планы и программы развития

* каналы приобретения и сбыта медицинских препаратов
* партнеры
* конкуренты
* переговоры и соглашения
* заказы и поставки

Рис. 1. Структура конфиденциальной информации

**Граф структура защищаемой информации**

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п\п** | **Наименование источника информации** | **Гриф конфиденциальности** | **Источник информации** | **Место нахождения источника информации** |
| **1** | **2** | **3** | **4** | **5** |
| 1.1.1 | Структура предприятия | ДСП | Контракты, документы на бумажных носителях | Сейф с секретными документами, каб. №2 |
| 1.1.2 | Личные сведения о сотрудниках фирмы | ДСП | Документы на бумажных носителях | Сейф с секретными документами, каб. №2 |
| 1.1.3 | Финансы | ДСП | Документы на бумажных и электронных носителях, БД | Сейф с секретными документами, каб. №2. ПЭВМ каб.№3 |
| 1.1.4 | Безопасность предприятия | ДСП | Документы на бумажных и электронных носителях | Сейф с секретными документами, каб. №2. ПЭВМ каб.№3 |
| 1.2.1 | Качество медикаментов | ДСП | Документы на бумажных носителях | Сейф с секретными документами, каб. №2 |
| 1.2.2 | Характеристики разрабатываемой продукции | ДСП | Документы на электронных носителях | ПЭВМ каб.№3 |
| 1.2.3 | Технологии производства | ДСП | Документы на электронных носителях | ПЭВМ каб.№3 |
| 1.2.4 | Планы и программы развития | ДСП | Документы на электронных носителях. Персонал предприятия | ПЭВМ каб.№3 |
| 1.3.1 | Каналы приобретения и сбыта медицинских препаратов | ДСП | Документы на бумажных и электронных носителях, БД | Сейф с секретными документами, каб. №2. ПЭВМ каб.№3 |
| 1.3. | Партнеры | ДСП | Руководство предприятия, документы на бумажных носителях | Сейф с секретными документами, каб. №2, рабочий стол директора |
|  |  |  |  | Продолжение таблицы |
| 1.3.3 | Конкуренты | ДСП | Руководство предприятия, документы на бумажных носителях | Сейф с секретными документами, каб. №2, рабочий стол директора |
| 1.3.4 | Переговоры и соглашения | ДСП | Документы на бумажных носителях | Сейф с секретными документами, каб. №2, рабочий стол директора |
| 1.3.5 | Заказы и поставки | ДСП | Директор, работники отдела поставок, документы на электронных носителях | Сейф с секретными документами, каб. №2. ПЭВМ каб.№3 |

Как видно из граф структуры в основном это бумажные и электронные документы, а также речевая информация, содержащаяся в беседах сотрудников и телефонных разговорах.

Таким образом, было проведена классификация и структурирование информации в соответствии с функциями, задачами и структурой организации, в результате чего защищаемая информация была представлена в виде отдельных элементов информации.

## Пространственная модель контролируемых зон

**(технический паспорт помещения)**

Пространственная модель представляет подробное описание помещения, инженерных конструкций, коммуникаций и средств связи, характеристику и основные параметры электронных устройств находящихся в этом помещении, а также технических средств безопасности

Пространственная модель объекта – это модель пространственных зон с указанным месторасположением источников защищаемой информации.

**Пространственная модель контролируемых зон**

Таблица 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п.п | **Пространственная характеристика помещения** | **Функциональная, конструктивная и техническая характеристика помещения** | | | |
| 1 | Этаж | 2 | Площадь, м2 | | 56 |
| 2 | Количество окон, тип сигнализации, наличие штор на окнах | 3 окна, жалюзи на окнах, плотные шторы, датчики разбития стекла «Breakglass 2000», F2, Y2, M1:2 | Куда выходят окна | | Проспект Сталинграда |
| 3 | Двери, кол-во, одинарные, двойные | 4 двери звукоизолирующие тяжелые | Куда выходят двери | | Коридор, каб. №3, каб. №2, каб. №1 |
| 4 | Соседние помещения, название, толщина стен | 1.С западной стороны находится Помещение №3. отштукатуренная с двух сторон стена (толщина - 1,5 кирпича)  2. С восточной стороны расположен коридор. отштукатуренная с двух сторон стена (толщина - 1,5 кирпича) | | | |
| 5 | Помещение над потолком, название, толщина перекрытий | Отсутствует | | | |
| 6 | Помещение под полом, название, толщина перекрытий | 1.Складское помещение. Бетонная плита 30 см, изоляционная ткань, паркет | | | |
| 7 | Вентиляционные отверстия, места размещения, размеры отверстий | Отсутствуют | | | |
| 8 | Батареи отопления, типы, куда выходят трубы | Централизованное, восьми секционные, трубы выходят на 1 этаж | | | |
| 9 | Цепи электропитания | Напряжение, (В), количество розеток электропитания, входящих и выходящих кабелей | | 220 В  7 розеток  2 входящих телефонных кабелей, 1 входящий АСУ | |
| 10 | Телефон | Типы, места установки телефонных аппаратов, тип кабеля | | 1. ТА-68, зав. № 0076, Т3, Тк12х0.5  2. ТА-68, зав. № 076, С1:5, Тк12х0.5 | |
|  |  |  | |  | |
| Продолжение таблицы | | | | | |
| 11 | Радиотрансляция | Типы громкоговорителей места установки | | 1. Громкоговоритель «**LBC3087/31», N24** | |
| 12 | Электрические часы | Тип, куда выходит кабель электрических часов | | 1.Часы «Gastar SP 3340 Red», N1:17, выходит к электрическому щиту в коридоре | |
| 13 | Бытовые радиосредства | Радиоприемники, телевизоры, аудио и видеомагнитофоны, их кол-во и типы | | Отсутствуют | |
| 14 | Бытовые электроприборы | Вентиляторы и др., места их размещения | | Отсутствуют | |
| 15 | ПЭВМ | Кол-во, типы. состав, места размещения | | 1.системный блок, зав. № 0076, V1:16;  2. монитор Samsung, зав. № 0716, V1:15;  3.клавиатура, зав. № 276, V1:15. | |
| 16 | Технические средства охраны | Типы и места установки извещателей, зоны действий излучений | | датчики движения:  1. «Контроль-Люкс 360°», 12 м, H1:10; H14;  2. «M-901A»,12 м, V12; D1:19; | |
| 17 | Телевизионные средства наблюдения | Места установки, типы и зоны наблюдения телевизионных трубок | | Видеокамеры:  1. «LCL-217 HS», 176 гр., B26; X1:12.  2.»MTV-63V 3HP», 176 гр., V17, X1:19 | |
| 18 | Пожарная сигнализация | Типы извещателей, схемы соединения и вывода шлейфа | | Пожарные датчики  1. «ИП 212/101-4-A1R», N1:10;  2.«ИП212/101-2», H7, Z7.  3. Извещатель пожарный ручной «ИПР 513-3А», X24 | |
| 19 | Другие средства |  | | Отсутствуют | |

* 1. **Моделирование возможных каналов утечки информации**

Под техническим каналом утечки информации понимают совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

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, отходы и т.п.).

**Классификация возможных каналов утечки информации**

Таблица 3

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

**Граф структура возможных каналов утечки конфиденциальной информации с объекта защиты**

Таблица 4

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Наименование  эл. информации** | | **Гриф информации** | | **Цена**  **информации** | | **Наименование источника информации** | | | **Местонахождение**  **источника информации** |
| **1** | **2** | | **3** | | **4** | | **5** | | | **6** |
| 1. Оптический канал | | | | | | | | | | |
| 1.1 | Обрабатываемая информация | | ДСП | | Не определена | | Секретарь ООО «Авицена» Тихонова И.И. | | | Кабинает №3 |
| 1.2 | Руководитель предприятия | | ДСП | | Не определена | | Директор OOO «Авицена» Молотов Т.Т. | | | В соответствии со служебной необходимостью |
| 1.3 | Уставные документы | | ДСП | | Не определена | | Директор OOO «Авицена» Молотов Т.Т. | | | В соответствии со служебной необходимостью |
| 2. Радиоэлектронный канал | | | | | | | | | | |
| 2.1 | ПЭВМ | | ДСП | | Не определена | | Персональная вычислительная машина  Системный блок NIX № 542637  Клавиатура NEC №83949  Монитор Samsung № 97787667 | | Инженер-электронщик Петров А.А. | |
| 2.2 | АСУ | | ДСП | | Не определена | | Автоматизированная система управления «Искра» №48488 | | Инженер-электронщик Петров А.А. | |
| 2.3 | Сеть 220 V | | ДСП | | Не определена | | Трансформаторная подстанция ул. Садовая | | Инженер- электрик Сидоров В.А. | |
|  |  | |  | |  | |  | |  | |
|  | |  | |  | |  | | Продолжение таблицы | | |
| 2.4 | Телефон | | ДСП | | Не определена | | Секретарь ООО «Авицена» Тихонова И.И.  Директор OOO «Авицена» Молотов Т.Т. | | В соответствии со служебной необходимостью | |
| 3. Акустический канал | | | | | | | | | | |
| 3.1 | Телефоны | | ДСП | | Не определена | | Секретарь ООО «Авицена» Тихонова И.И.  Директор OOO «Авицена» Молотов Т.Т. | | | В соответствии со служебной необходимостью |
| 4. Материально-вещественный канал | | | | | | | | | | |
| 4.1 | Уставные и руководящие документы | | ДСП | | Не определена | | Директор OOO «Авицена» Молотов Т.Т. | | | В соответствии со служебной необходимостью |
| 4.2 | Компоненты производства | | ДСП | | Не определена | | Отходы производства | | | Мусорка |

* 1. **Оценка степени угрозы защищаемой информации**

Моделирование возможных каналов утечки информации ставит целью анализ способов и путей хищения защищаемой информации. Оно включает:

- моделирование технических каналов утечки информации

- моделирование способов физического проникновения злоумышленника к источникам информации.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы.

**Модель получения информации по техническим каналам с объекта зашиты**

Таблица 5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п\п** | Место **установки** | **Позиционное место установки устройств съема информации** | **Тип (индекс)**  **устройства съема информации** | **Вероятная возможность**  **(способ) установки** | **Технический канал утечки информации** |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1. | Просмотр окна со стороны просп. Сталинграда | J1:1 | Лазерная система мониторинга помещения «HKG GD-7800» | Конкуренты | Оптический |
| 2. | Окно со стороны просп. Сталинграда | L1 | Оптический прибор (Бинокль) | Автостоянка по просп. Сталинграда | Оптический |
| 3. | Телефон1 | Т5 | Радиопередатчик «IPSA-2» | Во время установки аппарата | Радиоэлектронный |
| 4. | Телефон2 | С1:7 | «Передатчик ТЛФ» | При плановой проверке | Радиоэлектронный |
| 5. | Кабинет руководителя объекта защиты | В1:11 | Видео- и аудиопередатчик «HKG GD 6110» | Персонал предприятия | Радиоэлектронный |
| 6. | Система часофикации | N1:17 | Микрофон «PK – 795» | Установка часов на стену | Радиоэлектронный |
| 7. | Оконная рама | J1:1 | Микрофон «РК-905» | При проведении уборочных работ | Радиоэлектронный |
| 8. | Розетка 220В | I1:2 | «TN-1 Тройник» | При проведении плановых закупок отделом снабжения | Радиоэлектронный |
| 9. | Стол руководителя предприятия | D1:5 | «ТС-3 маркер» | Подарочный набор руководителю | Акустический |
| 10. | Внешняя стена кабинета №3 | Y1:10 | стетоскоп-микрофон «HKG GD 0016» | Посетителями организации | Акустический |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Продолжение таблицы | | | | | |
| 11. | Окно со стороны просп. Сталинграда | Н1 | «Радиостетоскоп Т-5» | Конкуренты организации | Акустический |
| 12. | Стол руководителя предприятия | Е1:12 | «Кард» | Подарочный набор руководителю | Акустический |

**Тактико-технические характеристики устройств съема информации**

Таблица 6

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п\п** | Место **установки** | **Тип (индекс)**  **устройства съема информации** | **Технические характеристики** |
| 1 | 2 | 3 | 4 |
| 1. | Просмотр окна со стороны просп. Сталинграда | Лазерная система мониторинга помещения «HKG GD-7800» | Напряжение питания -8 х 1,5 В  Мощность–5Вт  Длина волны - 750-840м |
| 2. | Окно со стороны просп. Сталинграда | Оптический прибор (бинокль) |  |
| 3. | Телефон1 | Радиопередатчик «IPSA-2» | Напряжение питания –6В  Диапазон частот - 138-180 МГц  Дальность действия–100-2000 м |
| 4. | Телефон2 | «Передатчик ТЛФ» | Напряжение питания -9В  Диапазон частот - 300 - 3400 Гц |
| 5. | Кабинет руководителя объекта защиты | Видео- и аудиопередатчик «HKG GD 6110» | Напряжение питания -115/230 В  Мощность – 4Вт  Частотный диапазон - УВЧ, ~ 800 МГц |
| 6. | Система часофикации | Микрофон «PK – 795» | Напряжение питания -1.5В  Мощность–0.5 Вт  Радиус действия – 20м |
| 7. | Оконная рама | Микрофон «РК-905» | Напряжение питания -1.5В  Мощность–0.5 Вт  Радиус действия – 20м |
|  |  |  |  |
|  |  |  |  |
| Продолжение таблицы | | | |
| 8. | Розетка 220В | «TN-1 Тройник» | Напряжение питания -220В  Мощность–10мВт  Радиус действия–250 м |
| 9. | Стол руководителя предприятия | «ТС-3 маркер» | Напряжение питания -9В  Мощность–200 мВт  Радиус действия –100м |
| 10. | Внешняя стена кабинета №3 | стетоскоп-микрофон «HKG GD 0016» | Напряжение питания -9В  Усиление - 100 тыс. раз, 86 дБ |
| 11. | Окно со стороны просп. Сталинграда | «Радиостетоскоп Т-5» | Мощность–5 мВт  Радиус действия–150 м |
| 12. | Стол руководителя предприятия | «Кард» | Напряжение питания –собственный аккумулятор  Частота - 135 МГц  Радиус действия–200 м |

**Возможные пути проникновения злоумышленников**

Таблица 7

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ элемента информации** | **Цена информации** | **Путь проникновения злоумышленника** | **Оценки реальности канала** | **Величина угрозы** | **Ранг угрозы** |
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1.1 | Не определена | A1:27-J1:18-P1:16 | Во время обработки информации | 47 | 3 |
| 1.2 | Не определена | A1:27-J1:18-C1:5 | При нарушении службой безопасности требований инструкций | 0.26 | 6 |
| 1.3 | Не определена | A1:27-J1:18-C1:5 | При нарушении службой безопасности требований инструкций | 47 | 2 |
| 2.1 | Не определена | A1:27-J1:18-P1:16 | Во время отправки продукции | 0.07 | 9 |
| 2.2 | Не определена | A1:27-U21-S4 | В неслужебное время | 0.02 | 8 |
| Продолжение таблицы | | | | | |
| 2.3 | Не определена | A1:27-U21-U14  A1:27-J1:18-X1:10  A1:27-J1:18-I1:2  A1:27-J1:18-B1:16-V8 | При нарушении службой безопасности требований инструкций | 113.4 | 1 |
| 2.4 | Не определена | A1:27-U21-S4 | При проведении обслуживания копировально-множительной техники | 40.1 | 4 |
| 3.1 | Не определена | A1:27-J1:18-P1:16 | При нарушении службой безопасности требований инструкций | 7.83 | 5 |
| 4.1 | Не определена | A1:27-J1:18-P1:16 | Во время отправки продукции | 0.26 | 7 |

Возможные пути проникновения злоумышленника на территорию охраняемого помещения представлены в приложениях 2 и 3.

1. **МОДЕЛИРОВАНИЕ МЕРОПРИЯТИЙ ИНЖЕНЕРНО – ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ЗАЩИТЫ**
   1. **Разработка модели скрытия вида деятельности организации (объекта)**

**План организационно технических мероприятий по активному скрытию объекта защиты**

Таблица 8

|  |  |  |
| --- | --- | --- |
| **№**  **п\п** | **Демаскирующий признак** | **Мероприятия по уменьшению (ослаблению) демаскирующих признаков** |
| **1** | **2** | **3** |
| **I. Организационные мероприятия** | | |
| 1. | Прибытие сотрудников на службу в форменной одежде | 1. Прибытие сотрудников на службу в форменной одежде другого ведомства 2. Проведение совещаний и переподготовки сотрудников других ведомств |
| 2. | Организация отдыха сотрудников | 1. Разнесение по времени перерывов сотрудников разных отделов 2. Организация различных мест отдыха сотрудников разных отделов 3. Регламентация распорядка работы сотрудников |
| 3. | Перемещение сотрудников | 1. Разграничение доступа сотрудников в различные помещения  2. Организация пропускного режима |
| 4. | Готовая продукция | 1. Разграничение доступа сотрудников в склад при вывозе продукции за пределы предприятия |
| 5. | Отходы производства | 1. Сбор и утилизация отходов производства 2. Уничтожение отходов делопроизводства 3. Создание комиссии для уничтожения документов |
| 6. | Готовая продукция | 1. Организация производства медицинских препаратов 2. Выставки и презентации медицинских препаратов 3. Привлечение средств массовой информации для рекламы медицинских препаратов 4. Привлечение средств массовой информации для проведения рекламных акций по приему сотрудников для выпуска медицинских препаратов |
|  | | |
| Продолжение таблицы | | |
| **II. Технические мероприятия** | | |
| 1. | Излучение ПЭВМ | 1. Организация работы системы зашумления 2. Установка в ПЭВМ генераторов зашумления 3. Персонификация доступа в систему 4. Программная защита системы ПЭВМ 5. Плановые (внеплановые) проверки ПЭВМ 6. Спецпроверки помещений 7. Программная защита информации |
| 2. | Телефонная связь | 1. Организация работы внутренней АТС 2. Персонификация сотрудников пользующихся АТС 3. Запись переговоров сотрудников по телефонам 4. Спецпроверки телефонной связи 5. Закрытие каналов связи |
| 3. | Строительные конструкции здания | 1. Нанесение на стекла пленки поглощающей ИК - излучение 2. Установка системы виброакустического зашумления стекол и строительных конструкций при проведении специальных мероприятий 3. Исключение доступа сотрудников в смежные помещения при проведении специальных мероприятий 4. Специальная проверка персонала обслуживающего смежные помещения 5. Определения перечня сотрудников допускаемых для проведения работ в смежных помещениях 6. Спецпроверки помещений |
| 4. | Контрольно-пропускной режим | 1. Организация контрольно-пропускного режима 2. Разграничение зон доступа 3. Персонификация и учет перемещения сотрудников по помещения 4. Создание отдельной службы безопасности выделенных помещений |

* 1. **Разработка мероприятий по технической защите информации на объекте защиты**

Мероприятия по технической защите информации можно условно разделить на три направления: пассив­ные, активные и комбинированные.

Пассивная защита подразумевает обнаружение и локализацию источников и каналов утечки информа­ции.

Активная — создание помех, препятствующих съему информации.

Комбинированная — сочетает в себе использование двух предыдущих направлений и явля­ется наиболее надежной.

Однако пассивная и активная защиты уязвимы в не­котором смысле. Например, при использовании ис­ключительно пассивной защиты приходится проводить круглосуточный мониторинг, так как неизвестно, ког­да включаются средства съема, или теряется возмож­ность использовать оборудование обнаружения при проведении деловой встречи.

Активная защита может заметно ослож­нить жизнь людям, ведущим наблюдение за вами, а вы можете использовать ее вхоло­стую, не зная точно, есть ли наблюдение.

Комбинированная защита позволяет уст­ранить эти недостатки.

**Модель защиты информации от утечки по техническим каналам с объекта зашиты**

Таблица 9

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п\п** | Место установки | **Позиционное место установки устройств съема информации** | **Тип (индекс) устройства съема информации** | **Способ применения** | **Технический канал закрытия утечки информации** |
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1. | Рабочий стол руководителя объекта защиты | С1:5 | Генератор шума «Гром ЗИ – 4» | Постоянно | Радиоэлектронный |
| 2. | ПЭВМ кабинета №3 | V1:13 | Генератор шума  «ГШ-К-1000М» | Постоянно | Радиоэлектронный |
| 3. | Помещение секретного отделения | Т6 | Генератор шума «Купол-W-ДУ» | Постоянно | Радиоэлектронный |
| 4. | Розетка 220 В. Кабинет руководителя объекта защиты | Х1:10 | Генератор шума  «SEL SP-41/C» | По решению руководства | Радиоэлектронный |
| Продолжение таблицы | | | | | |
| 5. | Розетка 220 В. Помещения секретного отделения | U14 | Генератор шума «SI-8001» | Постоянно | Радиоэлектронный |
| 6. | Розетка 220 В. Кабинета №2 | V8 | Генератор шума «SI-8001» | По решению руководства | Радиоэлектронный |
| 7. | Кабинет руководителя объекта защиты | Х1:3 | Генератор зашумления «Волна 4 М» | По решению руководства | Радиоэлектронный |
| 8. | Кабинет руководителя объекта защиты | Х1:6 | Генератор зашумления «SEL SP-21B1» | По решению руководства | Радиоэлектронный |
| 9. | Кабинет руководителя объекта защиты | Х1:9 | Фильтр питания «ФСП-1Ф-7А» | Постоянно | Радиоэлектронный |
| 10. | Окно кабинета руководителя объекта защиты | D1:3 | Виброакустическая система «ВГШ-103» | Постоянно | Акустический |
| 11. | Окно помещения секретного отделения | R2 | Виброакустический генератор шума «ANG-2000» | По решению руководства | Акустический |

**Тактико-технические характеристики средств защиты**

Таблица 10

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п\п** | Место установки | **Тип (индекс) устройства защиты информации** | **Технические характеристики** |
| **1** | **2** | **3** | **4** |
| 1. | Рабочий стол руководителя объекта защиты | Гром ЗИ-4 | Диапазон частот- 20 - 1000 МГц  Питание - сеть 220 В  Напряжение сигнала - в диапазоне частот 100 кГц - 1МГц - 60 дБ |
| 2. | Кабинет руководителя объекта защиты | ГШ-К-1000М | Диапазон частот - 100 кГц - 1000 МГц  Питание - +12 В, от шины компьютера  Уровни излучаемой мощности  шума - 30 - 45 дБ |
| Продолжение таблицы | | | |
| 3. | Помещение секретного отделения | Купол-W-ДУ | Радиус действия - 5 - 10 м  Диапазон рабочих частот - 100 кГц - 1800 МГц  Питание - 220 В  мощность излучения - 15 Вт  Коэффициент качества шума - не хуже 0.6 |
| 4. | Розетка 220 В. Кабинет руководителя объекта защиты | SEL SP-41/C | Ширина спектра помехи - 30 кГц - 30 МГц  Питание - 220 В  Уровень шумового сигнала - 75 - 35 дБ/мкВ |
| 5. | Розетка 220 В. Помещения секретного отделения | SI-8001 | Ширина спектра помехи - 5 кГц - 10 МГц  Потребляемая мощность< 15ВА  Питание - 220 В  Уровень помех - 30 - 80 дБ |
| 6. | Розетка 220 В. Кабинета №2 | SI-8001 | Ширина спектра помехи - 5 кГц - 10 МГц  Питание - 220 В  Уровень помех - 30 - 80 дБ |
| 7. | Кабинет руководителя объекта защиты | Волна 4 М | **Диапазон частот -** 0,5...1000 МГц  **Мощность -** 20 Вт  **Питание -** 220 В  **Амплитуда шумового сигнала -** не менее 3 В |
| 8. | Кабинет руководителя объекта защиты | SEL SP-21B1 | Питание - 12 В  Диапазон частот - 5 МГц...1 ГГц  Уровень сигнала на выходе - 45 дБ  Ток потребления - 350 мА |
| 9. | Кабинет руководителя объекта защиты | ФСП-1Ф-7А | Диапазон рабочих частот - 0,15-1000 МГц  Величина затухания - 60 дБ  Допустимый ток нагрузки -7 А |
| 10. | Окно кабинета руководителя объекта защиты | ВГШ-103 | Диапазон - 40 дБ в диапазоне частот 175 - 5600 Гц  Радиус - 5 м |
| 11. | Окно помещения секретного отделения | ANG-2000 | Ширина спектра помехи - 250 Гц - 5 кГц  Питание - 220 В  Потребляемая мощность - 24 Вт  Выходное напряжение - 1 - 12 В  Сопротивление > 0.5 Ом |

* 1. **Разработка модели охранной и пожарной сигнализации объекта (помещения)**

## Номенклатура средств системы охранной и пожарной сигнализации

Таблица 11

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п.п** | **Наименование** | **Схемное**  **обозначение** | **Позиция** | **Количество** | **Стоимость, руб.** |
| I. Система охранной сигнализации | | | | | |
| 1. | Видеокамера «LCL-217HS» | LCL | B26  X1:12 | 2 | 26 100.00 |
| 2. | Видеокамера «MTV-63V 3HP» | MTV | V17  X1:19 | 2 | 19 720.00 |
| 3. | Датчик движения «Контроль-Люкс 360°» | К-Л | Н1:10  Н14 | 2 | 2 438.00 |
| 4. | Датчик движения «M-901A» | М | V12  D1:19 | 2 | 330.00 |
| 5. | Датчик разбития стекла «Breakglass 2000» | BG | F2  Y2  M1:2 | 3 | 570.00 |
| 6 | Громкоговоритель «**LBC3087/31**» | LBC | N24 | 1 | 1 176.00 |
| 7 | Приемно-контрольный прибор «Астра-781» | A | Х26 | 1 | 2 608.00 |
| 8. | Световой оповещатель «Астра-10 (О12-3)» | Ас | В1:26 | 1 | 112.00 |
| 9. | Звуковой оповещатель «DBS12/24BW» | DB | D1:25 | 1 | 803.00 |
| II. Система пожарной сигнализации | | | | | |
| 1. | Пожарный датчик «ИП 212/101-4-A1R» | ИП-R | N1:10 | 1 | 640.00 |
| 2. | Пожарный датчик «ИП212/101-2» | ИП | H7  Z7 | 2 | 414.00 |
| 3. | Извещатель пожарный ручной «ИПР 513-3А» | ИПР | X24 | 1 | 552.00 |
| I. Система допуска сотрудников | | | | | |
| 1. | Контрольный считыватель «Em Marin» | EM | B1:27 | 1 | 3 893.00 |
| 2. | Электромагнитный замок «Малыш-5 ТМ» | М-5 | A1:26  U19  B1:15  G1:18 | 4 | 5 336.00 |
| **Итого** | | | | | **64 692.00** |

Схематичное расположение приборов охранно-пожарной сигнализации представлено в приложении 4.

* 1. **Расчет зон распространения акустических и электромагнитных волн с объекта защиты с масштабной привязкой на местности**

Затухание акустической волны на границе контролируемой зоны зависит от множества факторов, таких как конструкция помещения, материал стен, тип и количество дверей и окон, наличие звукопоглощающих элементов и т.п.

Расчет распространения акустических волн с объекта защиты проводится для двух точек от уровня сигнала 80 дБ.

**Звукопоглощающие свойства строительных конструкций**

Таблица 12

|  |  |  |
| --- | --- | --- |
| Материал | Толщина | Звукоизоляция на частотах (Гц), 2000 дБ |
| Стена из железобетонных блоков | 300 мм | 69 |
| Отштукатуренная с двух сторон стена | 1,5 кирпича | 61 |
| Одинарное остекление | 3 мм | 31 |
| Дверь звукоизолирующая тяжелая | - | 50 |

Уровень акустического сигнала за ограждением можно оценить по формуле:

, дБ,

где – уровень речевого сигнала в помещении (перед ограждением), дБ;

– площадь ограждения, м2;

– звукоизолирующая способность ограждения, дБ.

Для **точки 1** уровень акустического сигнала будет равен:

- окно =80+6-10lg21-31=41.8

- дверь=80+6-10lg21-50=22.8

- стена внешняя=80+6-10lg21-69=3.8

- стена внутренняя=80+6-10lg21-61=11.8

Для **точки 2** уровень акустического сигнала будет равен:

При S=5.9 м2:

- стена внутренняя=80+6-10lg5.9-61=17.3

- стена внешняя =80+6-10lg5.9-69=9.3

- окно =80+6-10lg5.9-31=47.3

При S=4.4 м2:

- стена внешняя =80+6-10lg4.4-69=10.6

- стена внутренняя=80+6-10lg4.4-61=18.6

- окно =80+6-10lg4.4-31=48.6

- дверь=80+6-10lg4.4-50=29.6

При S=5.4 м2:

- стена внутренняя =80+6-10lg5.4-61=17.7

- стена внешняя =80+6-10lg5.4-69=9.7

- окно =80+6-10lg5.4-31=47.7

При S=4.0 м2:

- стена внутренняя =80+6-10lg4.0-61=19

- стена внешняя =80+6-10lg4.0-69=11

- окно =80+6-10lg4.0-31=49

- дверь=80+6-10lg4.0-50=30

Результаты проведенных вычислений представлены в таблице 13

**Уровни акустического сигнала на строительных конструкциях**

Таблица 13

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п\п** | **Строительная конструкция** | | **Позиционное обозначение** | **Уровень (дБ)** |
| **Точка №1** | | | | |
| 1.1 | Окно | | I1-P1 | 65.1 |
| 1.2 | Дверь | | U19-U23 | 46.1 |
| 1.3 | Стена внешняя | | A2-F2  P2-U2 | 27.1 |
| 1.4 | Стена внутренняя | | A2-A26  A26-U26  U23-U26  U2-U18 | 35.1 |
| **Точка №2** | | | | |
| 2.1 | При S=5.9 м2 | Стена внутренняя | A2-A26  A26-L26 | 32.7 |
| 2.2 | Стена внешняя | A2-F2 | 24.7 |
| 2.3 | Окно | I1-L1 | 62.7 |
| 3.1 | При S=4.4 м2 | Стена внутренняя | U2-U18  U23-U26  M26-U26 | 23.4 |
| 3.2 | Стена внешняя | P2-U2 | 31.4 |
| 3.3 | Окно | M1-P1 | 61.4 |
| 3.4 | Дверь | U19-U23 | 42.4 |
| 4.1 | При S=5.4 м2 | Окно | I1-L1 | 62.3 |
| 4.2 | Стена внутренняя | A2-A25 | 32.3 |
| 4.3 | Стена внешняя | A2-F2 | 24.3 |
| 5.1 | При S=4.0 м2 | Стена внутренняя | U2-U18  U23-U25 | 31 |
| 5.2 | Стена внешняя | P2-U2 | 23 |
| 5.3 | Окно | M1-P1 | 61 |
| 5.4 | Дверь | U19-U23 | 42 |

Для того чтобы рассчитать расстояние распространения акустической волны воспользуемся формулой , дБ, но с условием, что = 0 и  не учитывается.

Для **точки 1**:

- окно 6+10lg S = 65.1дБ;

lg S =5.9;

- дверь 6+10lg S = 46.1дБ;

lg S =4;

- стена внешняя 6+10lg S = 35.1дБ;

lg S =2.9;

- стена внутренняя 6+10lg S =27.1дБ;

lg S =2.1;

Аналогично делаются расчеты для каждого значения полученных в таблице 13.

Степень ослабления электромагнитного излучения зависит от размеров контролируемой зоны и от наличия преград на пути распространения электромагнитной волны.

**Экранирующие свойства элементов здания**

Таблица 14

|  |  |
| --- | --- |
| Тип здания | Ослабление, дБ на частоте |
| 1 ГГц |
| Железобетонное здание с ячейкой арматуры 15х15 см и толщиной 160 мм | 15-17 |

Напряженность электрического поля электромагнитной волны убывает пропорционально расстоянию от источника излучения и определяется формулой:

,

где  – мощность излучения;

*r* – расстояние от источника излучения, м

Далее можно рассчитать распространение электромагнитных волн для следующих приборов:

- «TN-1 Тройник» 250-18=232

- «ТС-3 маркер» 100-18=82

- «Радиостетоскоп Т-5» 150-18=132

- «Кард» 200-18=182

- Микрофон «РК-905» 20-18=2

- Микрофон «PK – 795» 20-18=2

Исходя из выше изложенного можно сделать вывод о том, что уровень как акустической, так и электромагнитной волны выходят за пределы охраняемого помещения, что может повлечь за собой утечку информации по соответствующим каналам. В связи с этим необходимо:

1. Установить систему виброакустического зашумления стекол и строительных конструкций;
2. Экранировать средства кабельных коммуникаций;
3. Использовать подавляющие фильтры в цепях питания и заземления;
4. Нанести на стекла пленку, поглощающую ИК-излучение.

Распространение акустических и электромагнитных волн представлено в приложении 5.

* 1. **Заполнение шаблона базы данных технических средств защиты информации помещения (объекта)**

Список основных и вспомогательных технических средств связи, определенных исходными данными и определенными в результате моделирования в ходе выполнения работы представлен в приложении 6.

1. **ОЦЕНКА ЭФФЕКТИВНОСТИ И ВОЗМОЖНОСТЕЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**
   1. **Оценка степени защиты информации на объекте**

Оценки угроз информации в результате проникновения злоумышленника к источнику или ее утечки по техническому каналу проводятся с учетом вероятности реализуемости рассматриваемого пути или канала, а также цены соответствующего элемента информации.

Для каждой из угроз рассчитывается коэффициент опасности угроз *α*:

 = I **/*F* ,

где  - коэффициент опасности угрозы;

 *Z* – стоимость бита информации (принимается равной 1, поскольку все

угрозы сравниваются между собой);

*I* – объем «похищенной» информации (при реализации угрозы);

* F* – полоса пропускания канала;

*q* – среднеспектральное отношение мощности сигнала к мощности помехи.

Результаты расчетов отображены в таблице 13.

## Ранжирование каналов утечки акустической информации

## Таблица 15

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Код угрозы | Вид угрозы | Δ F  (кГц) | Т(час) | q(дБ) | I(Мб) | b(s)(дол.) | α  Мб  дол. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Sp1 | Вносимая или заранее установленная автономная радиозакладка, в том числе с дистанционным управлением ДУ | 3,5 | 200 | 40 | 4,35х103 | 1000 | 7.83 |
|  |  |  |  |  |  |  |  |
| Продолжение таблицы | | | | | | | |
| Sp2 | Долговременная радиозакладка с сетевым питанием, в том числе с ДУ | 3,5 | 3000 | 40 | 6,3х104 | 500 | 113.4 |
| Sp4 | Контроль стен (стетоскопы) | 3,5 | 3000 | 10 | 1,57х104 | 1000 | 14.1 |
| Sp5 | Контроль труб (стетоскопы) | 2,0 | 1500 | 10 | 4,5х103 | 1000 | 7.1 |
| Sp6 | Использование вносимых диктофонов | 3,5 | 50 | 40 | 1,05х103 | 1500 | 1.89 |
| Sp7 | Направленные микрофоны | 2,0 | 200 | 10 | 6х102 | 2000 | 0,94 |
| Sp9 | Лазерный контроль оконных стекол | 2,5 | 1500 | 20 | 1,1х104 | 100000 | 19,6 |
| Sp11 | Проводные (телефонные) закладки | 3,5 | 3000 | 20 | 3,14х104 | 200 | 40,1 |

### Аналогичным образом формируется (для данного помещения) спектр сигнальных угроз, представленный в таблице 14

Коэффициенты  опасности угроз сигнальной информации оценивается по формуле:

** =**** *I/b*,

где ****– средняя стоимость информации (принята при расчетах равной 1)

*I* – общий объем информации по каналу ее утечки за время анализа *Т* (принято, что *Т* = 1 год);

*b* – стоимость реализации угрозы;

Входящая в формулу величина *I* объема информации принималась равной:

*I* = *103 Мб* – для вариантов хищения информации с жесткого диска ЭВМ;

**, – для вариантов копирования дискет (документов), где *m* – число дискет, а ** 1,44 Мб – емкость дискеты.

Для вариантов видеоконтроля:

**

где – число элементов (число pixel) разрешения в поле изображения;

*Fk* – частота кадров;

*q* – отношение сигнал/помеха;

*Т* – время штатной работы (хорошая видимость и др.).

### Ранжирование каналов утечки сигнальной информации

## Таблица 16

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Код yrpoз** | **Наименование угрозы** | ***Т (час)*** | ***m***  ***(шт)*** | ***I1***  ***(Мб)*** | ***l x m*** | ***Fk***  ***(Гц)*** | ***q***  ***(дБ)*** | ***I***  ***(Мб)*** | ***b***  ***(дол.)*** | ***α***  ***Мб***  ***дол.*** |
| S1 | перехват побочных излучений от ЭВМ | 3000 | - | - | - | - | - | 103 | 40000 | 0,02 |
| S2 | Применение закладных устройств в ЭВМ | 3000 | - | - | - | - | - | 103 | 20000 | 0,05 |
| S4 | Копирование информации с магнитных носителей | 3000 | 50 | 1,44 | - | - | - | 72 | 1000 | 0.07 |
| S5 | Внешний (через окна) видео контроль с документированием | 200 | - | - | 250х250 | 25 | 10 | 4,7x105 | 10000 | 47 |
| S7 | Использование вносимых, кратковременного действия видеоконтрольных устройств или микро фотокамер | 100 | - |  | 250х250 | 25 | 40 | 2,6х102 | 1000 | 0,26 |

Возможности инженерно-технических средств защиты информации определяются их тактико-техническими характеристиками (уровнями ослабления сигналов, уровнями создаваемых помех, уровнями экранировки и т. п.). Требования должны учитывать специфику зон защиты, степень важности информации, допустимый риск (допустимые потери) и др.

Применяя средства активной или пассивной защиты, мы тем или иным способом уменьшаем пропускную способность каналов утечки информации. Происходит обесценивание информации, то есть в конечном итоге снижение стоимости ущерба. Активные средства обеспечивают это путем создания помех, а средства пассивной защиты – путем ослабления уровня информационного сигнала.

## Ранжирование видов противодействия утечки информации

## Таблица 17

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Код средства защиты** | **Вид противодействия** | **Виды**  **угроз** | **В(дол.)** | ***α***  **Мб**  **дол.** | ***β***  **Мб**  **дол.** | ***η*** | **Общий**  **ранг**  **(*η* 0)** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| П1 | Применение электромагнитной экранировки помещения (S=120м2) | Spl  Sp2 | 8000 | 4,35  126 | 0,54  7.87 | 2,34  991,6 | 994 |
| П2 | Радиомониторинг с использованием сканеров | Sp1  Sp2 | 4500 | 4,35  126 | 0,96  14,0 | 4,17  1764 | 1768 |
| П4 | Зашумление стен | Sp4 | 3000 | 15,7 | 5,23 | 82,1 | 82,1 |
| П5 | Зашумление труб системы отопления | Sp5 | 600 | 4,5 | 7,5 | 33,7 | 33,7 |
| П6 | Использование рентгенопросмотровых устройств (контроль вещей) | Sp6 | 8000 | 0,7 | 0,13 | 0,10 | 0,10 |
| П7 | Применение магнитомеров (обнаружение диктофонов) | Sp6 | 1500 | 0,7 | 0,7 | 0,49 | 0,49 |
| П8 | Повышение звукоизоляции окон и дверей | Sp7 | 1000 | 0,3 | 0,6 | 0,18 | 0,18 |
| П9 | Использование специальных жалюзей и штор | Sp9 | 500 | 3,94  0,11  0,47 | 47,2  22,0  47,0 | 186  2,42  22,1 | 210,5 |
| П10 | Специальный осмотр телефонных аппаратов | Sp11 | 200 | 157 | 157 | 2,46х104 | 2,46х104 |

* 1. **Экономическая оценка стоимости средств защиты информации**

## Стоимостная оценка защиты информации объекта

### Таблица 18

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Количество** | **Стоимость** |
| **1** | **2** | **3** | **4** |
| 1. | Видеокамера «LCL-217HS» | 2 | 26 100.00 |
| 2. | Видеокамера «MTV-63V 3HP» | 2 | 19 720.00 |
| 3. | Датчик движения «Контроль-Люкс 360°» | 2 | 2 438.00 |
| 4. | Датчик движения «M-901A» | 2 | 330.00 |
| 5. | Датчик разбития стекла «Breakglass 2000» | 3 | 570.00 |
| 6. | Громкоговоритель «**LBC3087/31**» | 1 | 1 176.00 |
| 7. | Приемно-контрольный прибор «Астра-781» | 1 | 2 608.00 |
| 8. | Световой оповещатель «Астра-10 (О12-3)» | 1 | 112.00 |
| 9. | Звуковой оповещатель «DBS12/24BW» | 1 | 803.00 |
| 10. | Пожарный датчик «ИП 212/101-4-A1R» | 1 | 640.00 |
| 11. | Пожарный датчик «ИП212/101-2» | 2 | 414.00 |
| 12. | Извещатель пожарный ручной «ИПР 513-3А» | 1 | 552.00 |
| 13. | Часы «Gastar» | 1 | 1 386.00 |
| 14. | Контрольный считыватель «Em Marin» | 1 | 3 893.00 |
| 15. | Электромагнитный замок «Малыш-5 ТМ» | 4 | 5 336.00 |
| 16. | Генератор шума «Гром ЗИ – 4» | 1 | 13 000**.**00 |
| 17. | Генератор шума«ГШ-К-1000М» | 1 | 4 200.00 |
| 18. | Генератор шума «Купол-W-ДУ» | 1 | 14 000.00 |
| 19. | Генератор шума«SEL SP-41/C» | 1 | 8 000.00 |
| 20. | Генератор шума «SI-8001» | 2 | 30 800.00 |
| 21. | Генератор зашумления «Волна 4 М» | 1 | 11 200.00 |
| 22. | Генератор зашумления «SEL SP-21B1» | 1 | 7 000.00 |
| 23. | Фильтр питания «ФСП-1Ф-7А» | 1 | 7 561.00 |
| 24. | Виброакустическая система «ВГШ-103» | 1 | 11 340.00 |
| 25. | Виброакустический генератор шума «ANG-2000» | 1 | 5 400.00 |
| **ИТОГО:** | | | **178 579.00** |

**ЗАКЛЮЧЕНИЕ**

В рамках данной курсовой работы было проведено моделирование объекта защиты и угроз безопасности информации. Построена структурная и пространственная модель объекта защиты, классифицированы и выявлены наиболее опасные и реальные пути организации несанкционированной утечки информации по техническим каналам и при проникновении злоумышленника на территорию предприятия, проведена стоимостная оценка защиты информации объекта.

Анализ объекта защиты выявил наиболее вероятные технические каналы утечки информации, это: радиоэлектронный, оптический, материально-вещественный и акустический.

В целом, работа над курсовой работой позволила систематизировать и структурировать ранее полученные знания в области защиты информации и полностью убедила и доказала необходимость комплексного подхода при реализации систем безопасности и систем защиты информации в частности.

Дата: Подпись:

**СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

1. *Торокин А. А.* Основы инженерно-технической защиты информации. – М: “Ось-89”, 1998. - 334 с.
2. *Машкина И.В.*, "Курс лекций по инженерно-технической защите информации", УГАТУ, 2004 г.
3. *Петраков А.В.* "Основы практической защиты информации", Учеб.пособие для ВУЗов, -2-е изд., М.: Радио и связь, 2000г.- 430 с.
4. http://tre.kai.ru/rates/method/kurs\_itzi.htm
5. http://www.aktivsb.ru/
6. domarev.kiev.ua/book-02-1/part3/chapter10.html
7. http://www.kft.ru/catalog/index.htm
8. http://www.alarmcom.ru/a032.htm