Оглавление

[ВВЕДЕНИЕ 5](#_Toc264816351)

[МОДЕЛИРОВАНИЕ ОБЪЕКТА ЗАЩИТЫ 7](#_Toc264816352)

[1.1 Описание объекта защиты 7](#_Toc264816353)

[1.2 Моделирование объектов защиты 11](#_Toc264816354)

[2 МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИИ В ЗАЛЕ ПЕРЕГОВОРОВ 13](#_Toc264816355)

[2.1 Моделирование угроз воздействия на источники информации 13](#_Toc264816356)

[2.2 Моделирование возможных каналов утечки информации 14](#_Toc264816357)

[2.3 Оценка степени угрозы защищаемой информации 16](#_Toc264816358)

[3 МОДЕЛИРОВАНИЕ МЕРОПРИЯТИЙ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ЗАЩИТЫ 17](#_Toc264816359)

[3.1 Расчет зон распространения акустических и электромагнитных волн с объекта защиты 17](#_Toc264816360)

[3.2 Разработка модели скрытия вида деятельности организации (объекта) 19](#_Toc264816361)

[3.3 Разработка мероприятий по технической защите информации на объекте защиты 19](#_Toc264816362)

[3.4 Разработка модели охранной и пожарной сигнализации объекта (помещения) 22](#_Toc264816363)

[4 ОЦЕНКА ЭФФЕКТИВНОСТИ И ВОЗМОЖНОСТЕЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ 23](#_Toc264816364)

[4.1 Оценка степени защиты информации на объекте 23](#_Toc264816365)

[4.2 Экономическая оценка стоимости средств защиты информации 26](#_Toc264816366)

[ЗАКЛЮЧЕНИЕ 27](#_Toc264816367)

[Библиографический список 28](#_Toc264816368)

# ВВЕДЕНИЕ

Информация ценилась во все времена. Чтобы владеть ею происходили убийства, войны. В наши дни она имеет не меньшую ценность. Эта ценность может определяться не только количеством труда потраченного на ее создание, но и количеством прибыли, полученной от ее возможной реализации. Поэтому актуальность рассматриваемой темы в том, что в наше время остро встает вопрос о необходимости различными методами защищать информацию своего предприятия, но многие предприниматели не знают, что следует делать, дабы сохранить те или иные сведения в тайне, с выгодой реализо­вать их, не понести убытки от их утечки или утраты.

**Целями системы защиты информации предприятия являются:**

* предотвращение утечки, хищения, утраты, искажения, под­делке информации;
* предотвращение угроз безопасности личности, предприятия, общества, государства;
* предотвращение несанкционированных действий по унич­тожению, модификации, искажению, копированию, блокированию информации;
* предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правово­го режима документированной информации как объекта собственности;
* защита конституционных прав граждан на сохранение лич­но тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
* сохранение, конфиденциальности документированной информации в соответствии с законо­дательство.

Целью данной курсовой работы является изучение возможных технических каналов утечки информации, а также по полученным знаниям спроектировать систему защиты информации от утечки в помещении ООО «Рога и копыта».

Для достижения цели, были поставлены следующие задачи:

1. Определить список защищаемой информации, её носители, возможные пути утечки

2. Составить модель объекта защиты

3. Изучить технические каналы утечки информации

4. Произвести моделирование угроз безопасности информации

5. Оценить степень защиты информации

Объектом исследования является зал для переговоров ООО «Рога и копыта», а предметом- защищаемая информация.

# МОДЕЛИРОВАНИЕ ОБЪЕКТА ЗАЩИТЫ

## 1.1 Описание объекта защиты

В данном курсовом проекте представлен объект защиты – зал для переговоров на предприятии ООО «Рога и копыта». Выбор данного помещения как объекта защиты обусловлен следующими факторами:

* в зале для переговоров циркулирует наиболее ценная информация;
* его посещают сотрудники организации всех должностных категорий, а также посетители организации;
* в помещении много элементов интерьера и мебели, в которой легко спрятать закладные устройства.

Главное здание ООО «Рога и копыта» представляет собой двухэтажное сооружение, несущие стены которого состоят из железобетонных блоков, толщиной 300 мм, а перегородки из шлакоблоков, толщиной 220 мм. Его площадь составляет 1430 м2. Само сооружение разделено на два функциональных блока: производственный ( размером 24 х 41,56 м) и административный ( размером 24 х 18 м), которые разделены несущей стеной с усиленной шумоизоляцией. Чердак и подвал отсутствуют. Планы этажей приведены на рисунках 1 и 2.

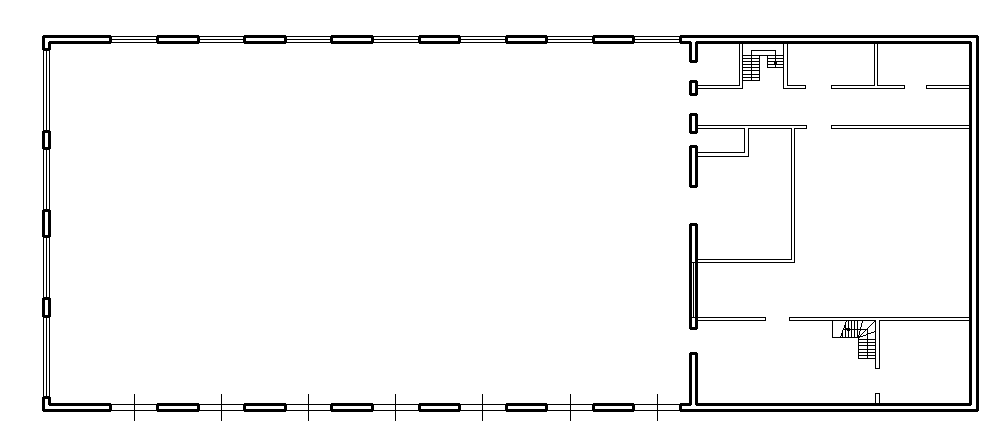


Рисунок 1- План 1-го этажа

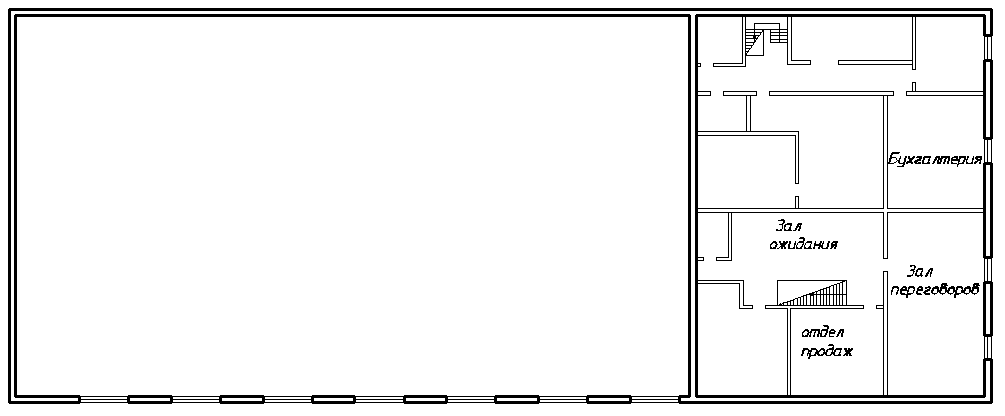


Рисунок 2- План 2-го этажа

Прилегающая территория представляет собой асфальтированную площадку, по периметру огороженную железобетонным забором. Размер территории составляет:

По ширине - 180 м;

По длине – 220 м.

Данная площадь предназначена для стоянки грузовых автомобилей. На ней также расположен пункт охраны, площадью 40 м2. Въезд на территорию оснащен распашными железными воротами и шлагбаумом.

Схематичное расположение зданий можно увидеть на рисунке 3.

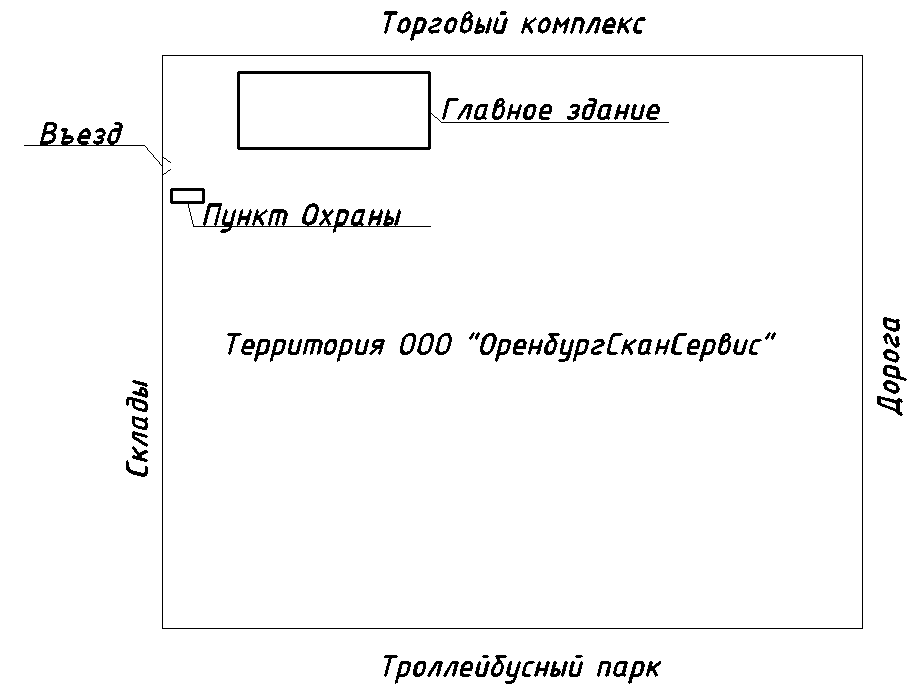


Рисунок 3- План прилегающей территории

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 1

|  |  |  |
| --- | --- | --- |
| №  п.п | **Факторы влияния** | **Параметры** |
| 1 | 2 | 3 |
| **1** | **Общая характеристика помещения** | |
| 1.1 | Этаж | 2 |
| 1.2 | Площадь, м2 | 72 |
| 1.3 | Смежные помещения | Бухгалтерия, зал ожидания, отдел продаж,  Внизу – служебное помещение |
| **2** | **Ограждения** | |
| 2.1 | Стены | *Наружная* – железобетонная толщиной 300 мм,  *Перегородки* – Отштукатуренная с двух сторон стена, толщина – 1,5 кирпича ; |
| 2.2 | Потолок | Железобетонная плита толщиной 300 мм, оштукатуренный |
| 2.3 | Пол | Железобетонная плита толщиной 300 мм, покрытый паркетом |
| 2.4 | Окно | Количество – 2, ПВХ, толщина стекла – 3 мм, двойное остекление, обращены во двор предприятия |
| 2.5 | Дверь | Дверь щитовая, облицованная фанерой с двух сторон с прокладкой из пористой резины находится со стороны зала ожиданий |
| **3** | **Предметы мебели и интерьера** | |
| 3.1 | Шкаф книжный | 2 шт. |
| 3.2 | Стол приставной | 4 шт. |
| 3.3 | Кресло кожаное вращающееся | 1 шт. |
| 3.4 | Стулья | 9 шт. |
| 3.5 | Диван | 1 шт. |
| 3.6 | Журнальный столик | 1 шт. |
| **4** | **Радиоэлектронные средства и электрические приборы** | |
|  | *ВТСС* | |
| 4.1 | Люстра | На потолке |
| **5** | **Средства коммуникации** | |
| 5.1 | Розетки электропитания | 2 шт. |
| 5.2 | Электропроводка | 1 распредкоробка, скрытая в стенах |

3D-модель офиса представлена на рисунках.

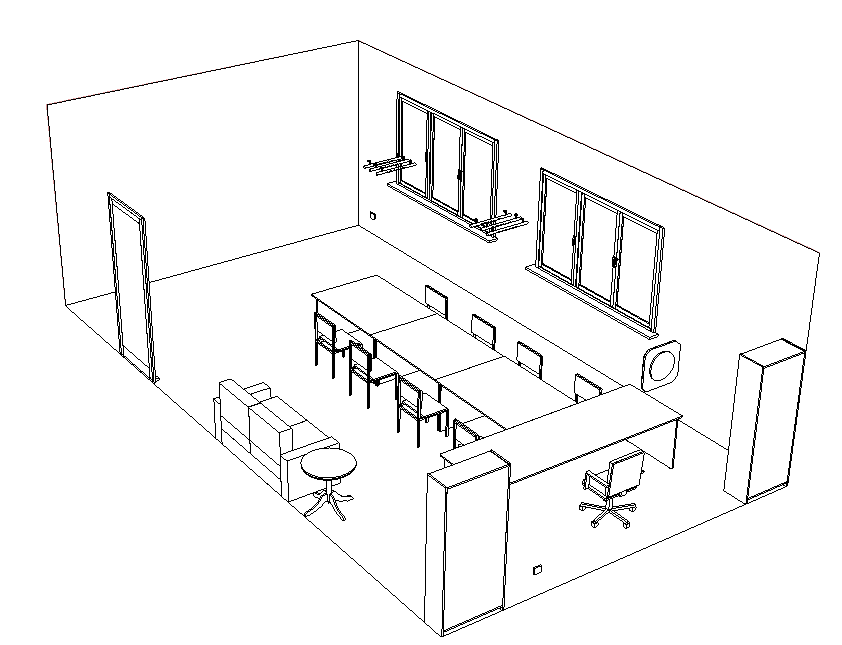
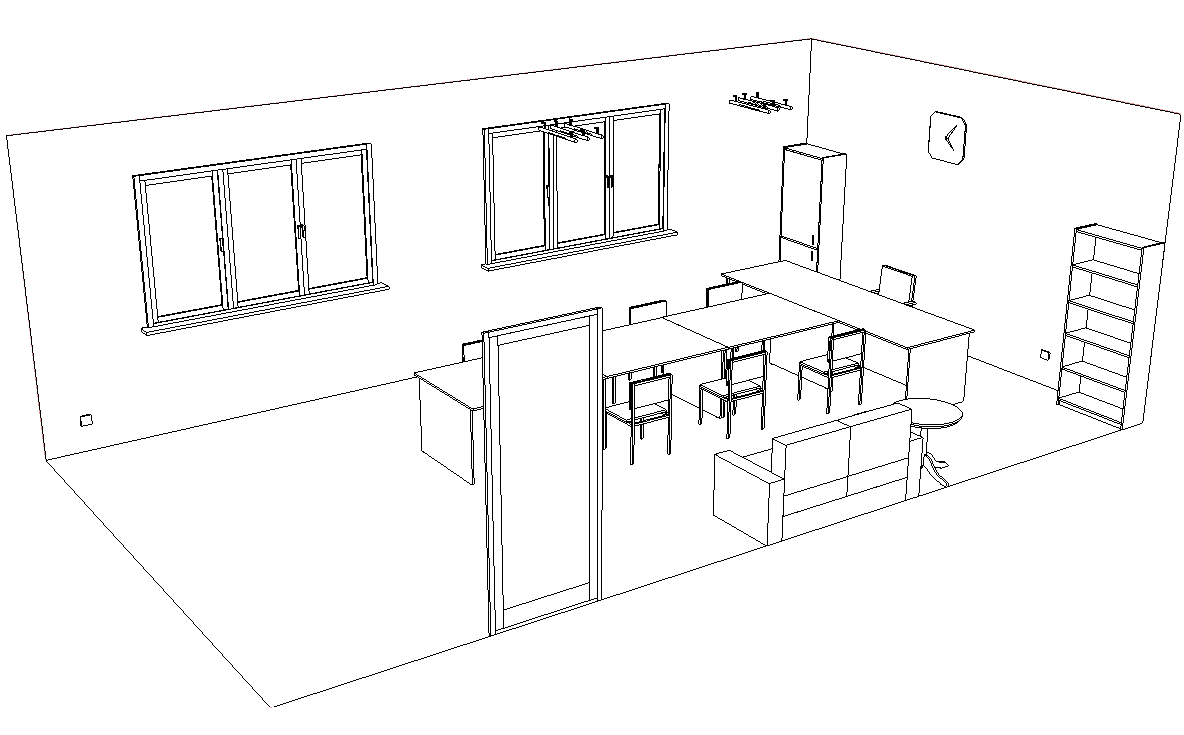


Рисунок 4- Офис

## 1.2 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 в рисунке 5.

#### Конфиденциальная информация

Об организации

О внутренней деятельности организации

О внешней деятельности организации

* характеристики разрабатываемых проектов

- планы и программы развития

- персональные данные сотрудников и студентов

* партнеры
* переговоры и соглашения
* заказы и поставки
* структура предприятия
* финансы

Рис. 1.

Стр

Рисунок 5 - Структурная модель защищаемой информации

В рассматриваемом помещении находится только речевая информация, содержащаяся в беседах сотрудников и телефонных разговорах, информация на бумажных и электронных носителях в данном помещении отсутствует.

# **2 МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИИ В ЗАЛЕ ПЕРЕГОВОРОВ**

Информация в зале переговоров подвергается угрозам воздействия и утечки. Эти потенциальные угрозы существуют всегда, но возмож­ность их резко возрастает, когда злоумышленник пытается проник­нуть в организацию или вербует сотрудника, возникает очаг пожа­ра или проявляются достаточно информативные признаки техни­ческих каналов утечки информации.

## **2.1 Моделирование угроз воздействия на источники информации**

При моделировании угроз воздействия прогнозируются марш­руты движения злоумышленника из нулевого состояния вне терри­тории организации к источникам информации в зале переговоров, оцениваются параметры (вероятность и время реализации) отдельных участков маршрутов (дуг семантической сети). По ним оценивается ущерб и ранг угроз.

Способы проникновения злоумышленника в зал переговоров зависят от квалификации злоумышленника, модели объек­тов защиты и времени проникновения.

В данном сценарии рассматривается вариант проникновения квалифицированного злоумышленника, который имеет в органи­зации сообщника без специальной подготовки.

Время проникновения целесообразно разделить на рабочее и нерабочее. Рабочее время характеризуется следующими услови­ями: пропуск людей и автотранспорта производится через конт­рольно-пропускной пункт (КПП) по пропускам, извещатели тех­нических средств охраны на территории и в здании выключают­ся, входная дверь в административное здание, в котором разме­щается зал переговоров, открывается для свободного про­хода.

В рабочее время несанкционированное проникновение в орга­низацию возможно через КПП по фальшивым документами и че­рез забор. Хотя второй способ проникновения в рабочее время ма­ловероятен, полностью исключить его нельзя. В рабочее время про­никнуть в зал переговоров может как «чужой» злоумышленник, так и со­трудник организации. Очевидно, что сотруднику сделать это проще. Проникновение возможно при открытой и закрытой двери зала переговоров, но наиболее легкий вариант для злоумыш­ленника — дверь открыта.

Во внерабочее время проникновение злоумышленника в орга­низацию возможно через забор, а также через окно или дверь зда­ния.

Если злоумышленник имеет предварительную информацию о расположении и типах средств охраны и видеоконтроля, он мо­жет попытаться проникнуть в зал переговоров во внерабочее время путем скрытного преодоления в ночное время рубежей и зон безопаснос­ти или спрятавшись в конце рабочего дня в одном из не закрываемых помещений организации.

## **2.2 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 2

|  |  |  |
| --- | --- | --- |
| **Каналы утечки информации с объекта защиты** | | |
| **1** | **2** |  |
| 1. | Оптический канал | Окна зала переговоров со стороны двора. |
| Приоткрытая дверь |
| 2. | Радиоэлектронный канал | Розетки |
| Система пожарной сигнализации |
| 3. | Акустический канал | Дверь |
| Стены помещения |
| Окна контролируемого помещения |
| 4. | Материально-вещественный канал | Документы на бумажных носителях |
| Персонал предприятия |
| Мусор |

Граф структура возможных каналов утечки конфиденциальной информации с объекта защиты

Таблица 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Наименование  эл. информации** | **Гриф информации** | **Наименование источника информации** | **Местонахождение**  **источника информации** |
| **1** | **2** | **3** | **5** | **6** |
| 1. Оптический канал | | | | |
| 1.1 | Окна | ДСП | Переговоры | Зал переговоров |
| 2. Радиоэлектронный канал | | | | |
| 2.1 | Сеть 220 V | ДСП | Сеть 220 V | Зал переговоров |
| 3. Акустический канал | | | | |
| 3.1 | Стены, дверь | ДСП | Переговоры | Зал переговоров |
| 4. Материально-вещественный канал | | | | |
| 4.1 | Компоненты  документов | ДСП | Мусор | Мусорка |

## **2.3 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 4

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **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 дороги | См. Приложение 1 | Лазерная система мониторинга помещения, бинокль | автомобиль | Оптический |
| 2. | Зал переговоров | См. приложение 4 | Видео- и аудиопередатчик | Персонал предприятия | Радиоэлектронный |
| 3. | Оконная рама | См. приложение 4 | Микрофон | При проведении уборочных работ | Радиоэлектронный |
| 4. | Розетка 220В | См. приложение 4 | Закладное устройство | При проведении уборочных работ | Радиоэлектронный |
| 5. | Стол директора | См. приложение 4 | Закладное устройство | Подарочный набор директору | Акустический |
| 6. | Стены | См. приложение 4 | Подслушивание | Соседние помещения | Акустический |

# 3 МОДЕЛИРОВАНИЕ МЕРОПРИЯТИЙ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ЗАЩИТЫ

## 3.1 Расчет зон распространения акустических и электромагнитных волн с объекта защиты

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 уровня акустического сигнала за ограждениями помещения ведется по формуле:

*Roг = Rрс + 6 + 10∙lg Soг – Koг дБ,*

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

*Sог* – площадь ограждения, м2;

*Koг* – звукоизолирующая способность ограждения, дБ.

Уровень речевого сигнала в помещении возьмем 70 дБ (для громкой речи), а звукоизолирующую способность для стен, двери и окон посмотрим в таблице звукопоглощающих свойств строительных конструкций при частоте звука 500 и 1000 Гц.

Произведя расчеты получаем:

Для 500 Гц

Rст1=70+6+10*∙*lg(6,12\*2,5)-58=29,8 дБ

Rст2=70+6+10*∙*lg(11,7\*2,5)-58=32,7 дБ

Rпер1=70+6+10*∙*lg(6,12\*2,5)-48=39,8 дБ

Rпер2=70+6+10*∙*lg(11,7\*2,5)-48=42 дБ

Rок=70+6+10*∙*lg2(1,2\*1,5)-38=44 дБ

Rдв=70+6+10*∙*lg(2\*0,8)-32=46 дБ

Для 1000 Гц

Rст1=70+6+10lg(6,12\*2,5)-65=23 дБ

Rст2=70+6+10lg(11,7\*2,5)-65 =26 дБ

Rпер1=70+6+10lg(6,12\*2,5)-54=34 дБ

Rпер2=70+6+10lg(11,7\*2,5)-54=37 дБ

Rок=70+6+10lg2(1,2\*1,5)-46=36 дБ

Rдв=70+6+10lg(2\*0,8)-35=43 дБ

Из расчетов видно, что коэффициент поглощения ограждающих конструкций не удовлетворяет рекомендуемым нормативам поглощения. Следовательно, необходимо принимать меры по защите информации от утечки по акустическому каналу для данного помещения. Так как переговоры в кабинете не всегда носят строгоконфиденциальный характер, целесообразно установить генераторы шума и вибрационные датчики на окна. Это позволит избежать высоких затрат, связанных с использованием звукопоглощающих средств и обеспечить надежную защиту информации.

## 3.2 Разработка модели скрытия вида деятельности организации (объекта)

План организационно технических мероприятий по активному скрытию объекта защиты

Таблица 5

|  |  |  |
| --- | --- | --- |
| **№**  **п\п** | **Демаскирующий признак** | **Мероприятия по уменьшению (ослаблению) демаскирующих признаков** |
| **1** | **2** | **3** |
| **I. Организационные мероприятия** | | |
| 1. | Проведение переговоров | 1. При проведении переговоров, закрывать двери |
| 2. | Прием посетителей | 1. Выключение сотового телефона и др. устройств имеющие функции записи, при посещении кабинета проректора |
| **II. Технические мероприятия** | | |
| 1. | 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 |
| 2. | Контрольно-пропускной режим | 1. Организация контрольно-пропускного режима 2. Разграничение зон доступа 3. Персонификация и учет перемещения сотрудников по помещения |

## 3.3 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.

Модель защиты информации от утечки по техническим каналам с объекта зашиты

Таблица 6

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п\п** | Место установки | **Тип (индекс) устройства съема информации** | **Способ применения** | **Технический канал закрытия утечки информации** |
| **1** | **2** | **3** | **4** | **5** |
| 1. | Окно | «Шорох-4» Вибропреобразователь пьезоэлектрический «КВП-2»(6 шт) | По решению руководства | Акустический |
| 2. | Дверь | «Шорох-4»  Акустический излучатель  «АСМик-1»(1 шт.) | По решению руководства | Акустический |
| 3. | Розетка 220 В. | Устройство защиты сети питания 220В  «МП-3» | Постоянно | Акустический |

Тактико-технические характеристики средств защиты

Таблица 7

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п\п** | Место установки | **Тип (индекс) устройства защиты информации** | **Технические характеристики** |
| **1** | **2** | **3** | **4** |
| 1. | Окно, батареи | Вибропреобразователь пьезоэлектрический «КВП-2» | Площадь оконного стекла толщиной 3 мм, защищаемая одним преобразователем - 1 м2 сопротивление одного преобразователя - 30 Ом  Габаритные размеры - 16х19 мм  Вес - не более 0,015 кг |
| 2. | Дверь | Акустический излучатель  «АСМик-1» | Сопротивление каждого излучателя - 8 Ом  Габаритные размеры-67х48х38 мм  Вес - не более 0,07 кг |
| 3. | Зал переговоров объекта защиты | «ШОРОХ-4» Системa постановки виброакустических и акустических помех | Расширенный диапазон частот (от 100 Гц до 12 кГц);  Многоуровневая система контроля работоспособности и состояния линий;  Визуальная индикация отклонения сигнала в каждой октавной полосе каждого канала;  Гарантированный энтропийный коэффициент качества шума (не хуже 0,93);  Число октавных полос в каналах-7;  Число модулей в блоке-1 – 4;  Число независимых каналов (в модуле)-1 или 2;  Максимальная выходная мощность одного канала:  в двухканальном модуле не менее 2 Вт  в одноканальном модуле не менее 4 Вт  Энтропийный коэффициент качества шума, при подключённой нагрузке не хуже 0,93  Время непрерывной работы системы без ухудшения характеристик не менее 24 часов. |
| 4. | Розетка 220 В. | Устройство защиты сети питания 220В  «МП-3» | максимальная потребляемая защищаемым средством мощность не более 170 Вт;  напряжение включения устройства не более 170 В;  напряжение отключения устройства не менее 30 В;  при пропадании напряжения переменного тока в сети, вносимое затухание на частоте 1 кГц не менее 80 дБ. |

## 3.4 Разработка модели охранной и пожарной сигнализации объекта (помещения)

Номенклатура средств системы охранной и пожарной сигнализации

Таблица 8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п.п** | **Наименование** | | **Количество** | **Стоимость, руб.** |
| I. Система охранной сигнализации | | | | |
| 1. | Датчик разбития стекла «Breakglass 2000» | | 3 | 570.00 |
| 2. | Звуковой оповещатель «DBS12/24BW» | | 1 | 803.00 |
| II. Система пожарной сигнализации | | | | |
| 1. | Пожарный датчик «ИП212/101-2» | | 2 | 414.00 |
| 2. | Извещатель пожарный ручной «ИПР 513-3А» | | 1 | 552.00 |
| III. Система допуска сотрудников | | | | |
| 1. | | Электромагнитный замок «Малыш-5 ТМ» | 1 | 1 334.00 |
| **Итого** | | | | 3 673.00 |

# 4 ОЦЕНКА ЭФФЕКТИВНОСТИ И ВОЗМОЖНОСТЕЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

## 4.1 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 9.

Ранжирование каналов утечки акустической информации

Таблица 9

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Код угрозы | Вид угрозы | Δ F  (кГц) | Т(час) | q(дБ) | I(Мб) | b(s)(у.е) | 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 |
| Sp2 | Долговременная радиозакладка с сетевым питанием, в том числе с ДУ | 3,5 | 3000 | 40 | 6,3х104 | 500 | 113.4 |
| Sp3 | Контроль стен (стетоскопы) | 3,5 | 3000 | 10 | 1,57х104 | 1000 | 14.1 |
| Sp4 | Использование вносимых диктофонов | 3,5 | 50 | 40 | 1,05х103 | 1500 | 1.89 |
| Sp5 | Направленные микрофоны | 2,0 | 200 | 10 | 6х102 | 2000 | 0,94 |
| Sp6 | Лазерный контроль оконных стекол | 2,5 | 1500 | 20 | 1,1х104 | 100000 | 19,6 |
| Sp7 | Проводные (телефонные) закладки | 3,5 | 3000 | 20 | 3,14х104 | 200 | 40,1 |

Аналогичным образом формируется (для данного помещения) спектр сигнальных угроз, представленный в таблице 16

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 10

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 | Внешний (через окна) видео контроль с документированием | 200 | - | - | 250х250 | 25 | 10 | 4,7x105 | 10000 | 47 |
| S2 | 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 уменьшается пропускная способность каналов утечки информации. Активные средства создают помехи, а средства пассивной защиты  ослабляют уровень информационного сигнала.

Ранжирование видов противодействия утечки информации

Таблица 11

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Код средства защиты** | **Вид противодействия** | **Виды**  **угроз** | **В(руб.)** | ***α***  **Мб**  **руб.** | ***β***  **Мб**  **руб.** | ***η*** | **Общий**  **ранг**  **(*η* 0)** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| П2 | Радиомониторинг с использованием сканеров | Sp1  Sp2 | 4500 | 4,35  126 | 0,96  14,0 | 4,17  1764 | 1768 |
| П3 | Зашумление стен | Sp3 | 3000 | 15,7 | 5,23 | 82,1 | 82,1 |
| П4 | Зашумление труб системы отопления | Sp4 | 600 | 4,5 | 7,5 | 33,7 | 33,7 |
| П5 | Применение магнитомеров (обнаружение диктофонов) | Sp5 | 1500 | 0,7 | 0,7 | 0,49 | 0,49 |
| П6 | Повышение звукоизоляции окон и дверей | Sp6 | 2000 | 0,3 | 0,6 | 0,18 | 0,18 |
| П7 | Использование специальных жалюзей и штор | Sp6 | 1000 | 3,94  0,11  0,47 | 47,2  22,0  47,0 | 186  2,42  22,1 | 210,5 |
| П8 | Специальный осмотр телефонных аппаратов | Sp7 | 200 | 157 | 157 | 2,46х104 | 2,46х104 |

## 4.2 Экономическая оценка стоимости средств защиты информации

Стоимостная оценка защиты информации объекта

Таблица 12

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Количество** | **Стоимость** |
| **1** | **2** | **3** | **4** |
| 1. | «ШОРОХ-4» Системa постановки виброакустических и акустических помех | 1 | 50 000.00 |
| 2. | Вибропреобразователь пьезоэлектрический «КВП-2» | 8 | 19 360.00 |
| 3. | Акустический излучатель  «АСМик-1» | 1 | 1 100.00 |
| 4. | Устройство защиты сети питания 220В  «МП-3» | 1 | 3 000.00 |
| 5. | Датчик разбития стекла «Breakglass 2000» | 2 | 380.00 |
| 6. | Устройство защиты цифровых ТА  «МП-1Ц» | 1 | 3 000.00 |
| 7. | Пожарный датчик «ИП 212/101-4-A1R» | 1 | 640.00 |
| 8. | Извещатель пожарный ручной «ИПР 513-3А» | 1 | 552.00 |
| 9. | Генератор шума «Салют 2000 С» | 1 | 7 670.00 |
| 10. | Электромагнитный замок «Малыш-5 ТМ» | 1 | 1 334.00 |
| **ИТОГО:** | **87 036.00** | | |

# ЗАКЛЮЧЕНИЕ

Утечка информации — это ее бесконтрольный выход за пределы организации (территории, здания, помещения) или круга лиц, которым она была доверена. И естественно, что при первом же обнаружении утечки принимаются определенные меры по ее ликвидации.

Поставленная цель в начале работы была достигнута, т.е. были изучены возможные технические каналы утечки информации, а также запроектирован комплекс защиты информации от утечки на примере отдельного помещения.

Для достижения цели были выполнены поставленные задачи:

1. Определен список защищаемой информации, её носители, возможные пути утечки

2. Составлена модель объекта защиты

3. Изучены технические каналы утечки информации

4. Произведено моделирование угроз безопасности информации

5. Оценена степень защиты информации.

В завершении исследования можно сделать следующий вывод, что в современном мире, мире высоких технологий и рыночных отношений, перед каждым предприятием встает необходимость защищать свои конфиденциальные данные, а для этого необходимо грамотно организовать технический комплекс защиты информации.

# Библиографический список

* Торокин А.А. Основы информационно-технической защиты информации./ Торокин А.А.- М.: Ось-89, 1998.- 765 с.
* Торокин А.А. Инженерно- техническая защита информации./ Торокин А.А.- М.: Гелиос АРВ, 2005.- 765 с.
* Хорев А.А. Способы и средства защиты информации./ Хорев А.А.- М.: МО РФ, 1998.- 320 с.
* Халяпин Д.В. Вас подслушивают? Защищайтесь. / Халяпин Д.В.- М.: НОУ ШО «Баярд», 2004.- 432 с.
* Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов.- М.: Академический Проект; Фонд "Мир",2003.-640с

Приложение 5

Установка средств защиты информации



Вибропреобразователь пьезоэлектрический «КВП-2»



«ШОРОХ-4» Системa постановки виброакустических и акустических помех



Акустический излучатель «АСМик-1»



Устройство защиты сети питания 220В «МП-3»



Устройство защиты цифровых ТА «МП-1Ц»



Генератор шума «Салют 2000 С»



Электромагнитный замок «Малыш-5 ТМ»

