Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования

**«Санкт-Петербургский национальный исследовательский**

**университет информационных технологий, механики и оптики»**

**Факультет:** Безопасности информационных технологий

**Направление (специальность)** 10.03.01 «Информационная безопасность»

**Профиль** «Комплексная защита объектов информатизации»

**КУРСОВАЯ РАБОТА**

По дисциплине: «Техническая защита информации»

**«Разработка системы защиты объекта»**

Автор курсовой работы:

студент гр. N3364, Смирнов М.Г.

Курсовой проект выполнен с оценкой \_\_\_\_\_\_\_\_\_\_\_

Руководитель: Беляев С.С.

Дата защиты \_\_\_\_\_\_\_\_\_ 2019г.

Санкт-Петербург

2019

СОДЕРЖАНИЕ

[Введение 3](#_Toc9420473)

[Глава 1 МОДЕЛИРОВАНИЕ ОБЪЕКТА ЗАЩИТЫ 4](#_Toc9420474)

[1.1. Описание объекта защиты 4](#_Toc9420475)

[1.2. Моделирование объектов защиты 4](#_Toc9420476)

[1.3. Моделирование возможных каналов утечки информации 8](#_Toc9420477)

[1.4. Оценка степени угрозы защищаемой информации 10](#_Toc9420478)

[Глава 2 МОДЕЛИРОВАНИЕ МЕРОПРИЯТИЙ ИНЖЕНЕРНО – ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ЗАЩИТЫ 13](#_Toc9420479)

[2.1 Разработка модели скрытия вида деятельности объекта 13](#_Toc9420480)

[2.2 Разработка мероприятий по технической защите информации на объекте защиты 14](#_Toc9420481)

[2.3 Разработка модели охранной и пожарной сигнализации объекта ( 15](#_Toc9420482)

[ГЛАВА 3 ОЦЕНКА ЭФФЕКТИВНОСТИ И ВОЗМОЖНОСТЕЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ 18](#_Toc9420483)

[3.1 Оценка степени защиты информации на объекте 18](#_Toc9420484)

[3.2 Экономическая оценка стоимости средств защиты информации 19](#_Toc9420485)

[Заключение 21](#_Toc9420486)

[Список используемых источников 22](#_Toc9420487)

Введение

Становление информационного общества связано с широким распространением персональных компьютеров, построением глобальной информационной Сети и подключения к ней большого числа пользователей. Эти достижения должны коренным образом изменить жизнь общества, выдвинув на передний план деятельность, связанную с производством, потреблением, трансляцией и хранением информации.

Одной из наиболее серьезных проблем, затрудняющих применение информационных технологий, является обеспечение информационной безопасности.

Информационная безопасность - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Угроза информационной безопасности организации – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия для организации.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Согласно ГОСТ 350922-96, защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Целью данной работы является описание и обеспечение информационной безопасности на выбранном объекте по техническим каналам. Приводится список защищаемой информации, её носители, возможные пути утечки, технические каналы утечки, проводится моделированием угроз безопасности информации.

Глава 1 МОДЕЛИРОВАНИЕ ОБЪЕКТА ЗАЩИТЫ

1. Описание объекта защиты

Объектом защиты данной курсовой работы является помещение частной фармацевтической компании ООО «Аглая».

Помещение расположено по адресу гор. Санкт-Петербург, 4-ая Советская, дом 23. С северной и северо-восточной стороны от него проходит подземный теплопровод. С западной стороны на расстоянии 40 метров расположены служебное здание, пункт водоснабжения (К – колодец, 140 суточный дебит воды, м3) и воздушная линия электропередачи.

Объект защиты представляет собой пятиэтажное 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, автоматизированная система управления и телефон.

1. Моделирование объектов защиты

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

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

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.

Для структурирования информации в качестве исходных данных используется перечень сведений, составляющих ведомственную или коммерческую тайну, а также перечень источников информации в организации. Структурирование информации производится путем классификации информации в соответствии с функциями, задачами и структурой организации с привязкой элементов информации к ее источникам.

Для выбранного объекта защиты структурная модель защищаемой информации приведена на рисунке 1.

#### 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

Рисунок 1 - Структура конфиденциальной информации

На основе схемы классификации информации разрабатывается перечень источников информации с их описанием. Данный перечень представлен в таблице 1.

Таблица - Структура защищаемой информации

| **№**  **п\п** | **Наименование источника информации** | **Гриф конфиденциальности** | **Источник информации** | **Место нахождения источника информации** |
| --- | --- | --- | --- | --- |
| 1.1.1 | Структура предприятия | ДСП | 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 |
| 1.3.2 | Партнеры | ДСП | Руководство предприятия, документы на бумажных носителях | Сейф с секретными документами, каб. №2, рабочий стол директора |
| 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 |

В приведенной структуре основные источники информации – это бумажные и электронные документы, а также речевая информация, содержащаяся в беседах сотрудников и телефонных разговорах.

Пространственная модель объекта – схемы, с указанными местами расположения источников защищаемой информации. 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.

Информация по описанию объекта защиты структурирована в таблицу 2.

Таблица - Пространственная модель контролируемых зон

| №  п.п | **Пространственная характеристика помещения** | **Функциональная, конструктивная и техническая характеристика помещения** |
| --- | --- | --- |
| 1 | Этаж | Второй |
| 2 | Количество окон, тип сигнализации, наличие штор на окнах | По три окна в каждом из кабинетов (окна выходят на восток), по одному окну в кабинете начальника и помещении техобслуживания оборудования, эти окна выходят на запад. На всех окнах имеются жалюзи, установлена сигнализация (срабатывает при открытии или ударе) и датчики разбития стекла «Breakglass 2000», F2, Y2, M1:2 |
| 3 | Двери, кол-во, одинарные, двойные | 4 двери звукоизолирующие тяжелые,  двери выходят в 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 | Вентиляционные отверстия, места размещения, размеры отверстий | Отсутствуют |
| 6 | Батареи отопления, типы, куда выходят трубы | Централизованное, восьми секционные, трубы выходят на 1 этаж |
| 7 | Цепи электропитания | Напряжение 220 В, 7 розеток электропитания,  2 входящих телефонных кабелей, 1 входящий АСУ |
| 8 | Телефон | 1. ТА-68, зав. № 0076, Т3, Тк12х0.5  2. ТА-68, зав. № 076, С1:5, Тк12х0.5 |
| 9 | Радиотрансляция | Громкоговоритель **«LBC3087/31», N24** |
| 10 | Электрические часы | Часы «Gastar SP 3340 Red», N1:17, выходит к электрическому щиту в коридоре |
| 11 | Бытовые радиосредства | Отсутствуют |
| 12 | Бытовые электроприборы | Отсутствуют |
| 13 | ПЭВМ | 1. Системный блок, зав. № 0076, V1:16;  2. Монитор Samsung, зав. № 0716, V1:15;  3. Клавиатура, зав. № 276, V1:15. |
| 14 | Технические средства охраны | 1. «Контроль-Люкс 360°», 12 м, H1:10; H14;  2. «M-901A»,12 м, V12; D1:19; |
| 15 | Телевизионные средства наблюдения | 1. «LCL-217 HS», 176 гр., B26; X1:12.  2.»MTV-63V 3HP», 176 гр., V17, X1:19 |
| 16 | Пожарная сигнализация | 1. «ИП 212/101-4-A1R», N1:10;  2.«ИП212/101-2», H7, Z7.  3. Извещатель пожарный ручной «ИПР 513-3А», X24 |
| 17 | Другие средства | Отсутствуют |

1. Моделирование возможных каналов утечки информации

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (TCP), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью TCP разведывательной информации об объекте. Причем под разведывательной информацией обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

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

* акустические;
* оптические;
* электромагнитные;
* материально-вещественные.

Классификация возможных каналов утечки информации для данного объекта защиты приведена в таблице 3.

Таблица - Классификация возможных каналов утечки информации

| **Каналы утечки информации с объекта защиты** | | |
| --- | --- | --- |
| 1 | Оптический канал | Окно каб. №1 со стороны 4-ой Советской |
| Окно каб. №2 со стороны 4-ой Советской |
| Окно каб. №3 со стороны 4-ой Советской |
| 2 | Радиоэлектронный канал | Стоянка автотранспорта на Енотовой улице |
| 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 |

Классификация возможных каналов утечки информации конфиденциальной информации с объекта защиты приведена в таблице 4.

Таблица - Классификация возможных каналов утечки информации конфиденциальной информации

|  | **Наименование  эл. информации** | **Гриф информации** | **Цена**  **информации** | **Наименование источника информации** | **Местонахождение**  **источника информации** |
| --- | --- | --- | --- | --- | --- |
| 1. Оптический канал | | | | | |
| 1.1 | Обрабатываемая информация | ДСП | Не определена | Секретарь ООО «Аглая» Павлюк И.И. | Кабинет №3 |
| 1.2 | Руководитель предприятия | ДСП | Не определена | Директор OOO «Аглая» Смирнов Д.Т. | В соответствии со служебной необходимостью |
| 1.3 | Уставные документы | ДСП | Не определена | Директор OOO «Аглая» Смирнов Д.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 | Телефон | ДСП | Не определена | Секретарь «Аглая» Павлюк И.И.  Директор OOO «Аглая» Смирнов Д.Т. | В соответствии со служебной необходимостью |
| 3. Акустический канал | | | | | |
| 3.1 | Телефоны | ДСП | Не определена | Секретарь «Аглая» Павлюк И.И.  Директор OOO «Аглая» Смирнов Д.Т. | В соответствии со служебной необходимостью |
| 4. Материально-вещественный канал | | | | | |
| 4.1 | Уставные и руководящие документы | ДСП | Не определена | Директор OOO «Аглая» Смирнов Д.Т. | В соответствии со служебной необходимостью |
| 4.2 | Компоненты производства | ДСП | Не определена | Отходы производства | Канализация |

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.

Данная модель представлена в таблицах 5-7.

Таблица - Модель получения информации по техническим каналам

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п\п** | **Место** **установки** | **Позиционное место установки устройств съема информации** | **Тип (индекс)**  **устройства съема информации** | **Вероятная возможность**  **(способ) установки** | **Технический канал утечки информации** |
| 1 | Просмотр окна со стороны ул. 4-ая Советская | J1:1 | Лазерная система мониторинга помещения «HKG GD-7800» | Конкуренты | Оптический |
| 2 | Окно со стороны ул. 4-ая Советская | L1 | Оптический прибор (Бинокль) | Автостоянка по ул. 4-ая Советская | 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 | Оконная рама | J1:1 | Микрофон «РК-905» | При проведении уборочных работ | Радиоэлектронный |
| 7 | Розетка 220В | I1:2 | «TN-1 Тройник» | При проведении плановых закупок отделом снабжения | Радиоэлектронный |
| 8 | Стол руководителя предприятия | D1:5 | «ТС-3 маркер» | Подарочный набор руководителю | Акустический |
| 9 | Внешняя стена кабинета №3 | Y1:10 | стетоскоп-микрофон «HKG GD 0016» | Посетителями организации | Акустический |
| 10 | Окно со стороны просп. Сталинграда | Н1 | «Радиостетоскоп Т-5» | Конкуренты организации | Акустический |
| 11 | Стол руководителя предприятия | Е1:12 | «Кард» | Подарочный набор руководителю | Акустический |

Таблица - Модель получения информации по техническим каналам

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п\п** | **Место** **установки** | **Тип (индекс)**  **устройства съема информации** | **Технические характеристики** |
| 1 | Просмотр окна со стороны 4-ой Советской | Лазерная система мониторинга помещения «HKG GD-7800» | Напряжение питания -8 х 1,5 В  Мощность–5Вт  Длина волны - 750-840м |
| 2 | Окно со стороны 4-ой Советской | 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 |
| 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 4-ой Советской | «Радиостетоскоп Т-5» | Мощность–5 мВт  Радиус действия–150 м |

Таблица - Возможные пути проникновения злоумышленников

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ элемента информации** | **Цена информации** | **Путь проникновения злоумышленника** | **Оценки реальности канала** | **Величина угрозы** | **Ранг угрозы** |
| 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 |
| 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 |

В данной главе представлено описание объекта защиты информации и его моделирование. Также были смоделированы возможные каналы утечки информации и дана оценка степени угроз защищаемой информации.

Глава 2 МОДЕЛИРОВАНИЕ МЕРОПРИЯТИЙ ИНЖЕНЕРНО – ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ЗАЩИТЫ

* 1. Разработка модели скрытия вида деятельности объекта

Таблица - План организационно технических мероприятий по активному скрытию объекта защиты

| **№**  **п\п** | **Демаскирующий признак** | **Мероприятия по уменьшению (ослаблению) демаскирующих признаков** |
| --- | --- | --- |
| **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 |
| **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 8. Организация работы системы зашумления 9. Установка в ПЭВМ генераторов зашумления 10. Персонификация доступа в систему 11. Программная защита системы ПЭВМ 12. Плановые (внеплановые) проверки ПЭВМ 13. Спецпроверки помещений 14. 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:

* 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. В таблице 9 представлена модель защиты информации от утечки по техническим каналам с объекта зашиты.

Таблица - Модель защиты информации от утечки по техническим каналам с объекта зашиты

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п\п** | **Место установки** | **Позиционное место установки устройств съема информации** | **Тип (индекс) устройства защиты от съема информации** | **Способ применения** | **Технический канал закрытия утечки информации** |
| 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 |
| 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 |

* 1. Разработка модели охранной и пожарной сигнализации объекта

Номенклатура средств системы охранной и пожарной сигнализации представлена в таблице 10.

Таблица - Номенклатура средств системы охранной и пожарной сигнализации

| **№**  **п.п** | **Наименование** | **Схемное**  **обозначение** | **Позиция** | **Кол-во** | **Стоимость, руб.** |
| --- | --- | --- | --- | --- | --- |
| I. Система охранной сигнализации | | | | | |
| 1 | Видеокамера «LCL-217HS» | LCL | B26  X1:12 | 4 | 15 800.00 |
| 2 | Датчик движения «Контроль-Люкс 360°» | К-Л | Н1:10  Н14 | 4 | 2 955.00 |
| 3 | Датчик разбития стекла «Breakglass 2000» | BG | F2  Y2  M1:2 | 3 | 1870.00 |
| 4 | Громкоговоритель «**LBC3087/31**» | LBC | N24 | 1 | 1 971.00 |
| II. Система пожарной сигнализации | | | | | |
| 1 | Пожарный датчик «ИП 212/101-4-A1R» | ИП-R | N1:10 | 3 | 640.00 |
| 2 | Извещатель пожарный ручной «ИПР 513-3А» | ИПР | X24 | 1 | 552.00 |
| III. Система допуска сотрудников | | | | | |
| 1 | Контрольный считыватель «Em Marin» | EM | B1:27 | 1 | 5 893.00 |
| 2 | Электромагнитный замок «Малыш-5 ТМ» | М-5 | A1:26  U19  B1:15  G1:18 | 4 | 5 736.00 |
| **Итого** | | | | | **93 702.00** |

* 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.

Таблица - Звукопоглощающие свойства строительных конструкций

|  |  |  |
| --- | --- | --- |
| **Материал** | **Толщина** | **Звукоизоляция, дБ** |
| Стена из железобетонных блоков | 300 мм | 73 |
| Отштукатуренная с двух сторон стена | 1,5 кирпича | 69 |
| Одинарное остекление | 3 мм | 35 |
| 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.

Результаты проведенных вычислений представлены в таблице 12.

Таблица - Уровни акустического сигнала на строительных конструкциях

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п\п** | **Строительная конструкция** | | **Позиционное обозначение** | **Уровень (дБ)** |
| **Точка №1** | | | | |
| 1.1 | Окно | | I1-P1 | 68.1 |
| 1.2 | Дверь | | U19-U23 | 44.2 |
| 1.3 | Стена внешняя | | A2-F2  P2-U2 | 25.1 |
| 1.4 | Стена внутренняя | | A2-A26  A26-U26  U23-U26  U2-U18 | 37.1 |
| **Точка №2** | | | | |
| 2.1 | При S=6 м2 | Стена внутренняя | A2-A26  A26-L26 | 32.7 |
| 2.2 | Стена внешняя | A2-F2 | 29.8 |
| 2.3 | Окно | I1-L1 | 65.7 |
| 3.1 | При S=5.4 м2 | Стена внутренняя | U2-U18  U23-U26  M26-U26 | 27.4 |
| 3.2 | Стена внешняя | P2-U2 | 35.4 |
| 3.3 | Окно | M1-P1 | 67.4 |
| 3.4 | Дверь | U19-U23 | 39.4 |
| 4.1 | При S=6.3 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 | 51 |
| 5.4 | Дверь | U19-U23 | 42 |

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.

ГЛАВА 3 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* – средне спектральное отношение мощности сигнала к мощности помехи.

Результаты расчетов отображены в таблице 13.

Таблица - Ранжирование каналов утечки акустической информации

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Код угрозы** | **Вид угрозы** | **Δ F**  **(кГц)** | **Т(час)** | **q(дБ)** | **I(Мб)** | **b(s)(руб.)** | **α**  **Мб**  **руб.** |
| 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 |
| 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 |
| 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 |

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 представлено в таблице 14.

Таблица - Ранжирование видов противодействия утечки информации

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Код средства защиты** | **Вид противодействия** | **Виды**  **угроз** | **В(руб.)** | ***α***  **Мб**  **руб.** | ***β***  **Мб**  **руб.** | ***η*** | **Общий**  **ранг**  **(*η* 0)** |
| 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

Экономическая оценка стоимости средств защиты информации представлена в таблице 15.

Таблица - Стоимостная оценка защиты информации объекта

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Количество** | **Стоимость, руб.** |
| 1 | Видеокамера «LCL-217HS» | 4 | 16 800.00 |
| 3 | Датчик движения «Контроль-Люкс 360°» | 4 | 2 955.00 |
| 5 | Датчик разбития стекла «Breakglass 2000» | 3 | 870.00 |
| 6 | Громкоговоритель «**LBC3087/31**» | 1 | 1 871.00 |
| 7 | Приемно-контрольный прибор «Астра-781» | 1 | 2 608.00 |
| 10 | Пожарный датчик «ИП 212/101-4-A1R» | 3 | 640.00 |
| 12 | Извещатель пожарный ручной «ИПР 513-3А» | 1 | 552.00 |
| 14 | Контрольный считыватель «Em Marin» | 1 | 4 893.00 |
| 15 | Электромагнитный замок «Малыш-5 ТМ» | 4 | 5 736.00 |
| 16 | Генератор шума «Гром ЗИ – 4» | 2 | 15 500**.**00 |
| 19 | Генератор шума «SEL SP-41/C» | 2 | 10 707.00 |
| 20 | Генератор шума «SI-8001» | 2 | 33 150.00 |
| 21 | Генератор зашумления «Волна 4 М» | 2 | 13 750.00 |
| 23 | Фильтр питания «ФСП-1Ф-7А» | 1 | 7 861.00 |
| 24 | Виброакустическая система «ВГШ-103» | 1 | 11 740.00 |
| 25 | Виброакустический генератор шума «ANG-2000» | 1 | 6 400.00 |
| **ИТОГО:** | | | **271 425.00** |

В данной главе была произведена оценка эффективности, возможностей средств защиты информации и рассчитана экономическая оценка стоимости средств защиты информации.

Заключение

В результате выполнения курсовой работы было дано описание помещения частной фармацевтической компании ООО «Аглая» как объекта защиты информации, проведено моделирование объекта защиты и угроз безопасности информации, смоделированы возможные каналы утечки информации и дана оценка степени угроз защищаемой информации.

Были разработаны модели мероприятий инженерно-технической защиты информации объекта защиты: модель скрытия вида деятельности, мероприятий по технической защите информации от утечки и воздействия на объекте защиты и модель охранной и пожарной сигнализаций помещения.

Также была произведена оценка эффективности, возможностей средств защиты информации и рассчитана экономическая оценка средств защиты информации. Стоимостная оценка средств защиты информации объекта равна 271 425.00 руб.

Список используемых источников

1. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
2. Торокин А. А. Основы инженерно-технической защиты информации. – М: “Ось-89”, 1998. - 334 с.
3. Машкина И.В., "Курс лекций по инженерно-технической защите информации", УГАТУ, 2004 г.
4. Петраков А.В. "Основы практической защиты информации", Учебное пособие для ВУЗов, -2-е изд., М.: Радио и связь, 2000г.- 430 с.