**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**КУРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**Кафедра Комплексной защиты информационных систем**

**Пояснительная записка к курсовому проекту**

**по дисциплине**

**«Инженерно-техническая защита информации»**

**специальности 090104 – Комплексная защита объектов информатизации**

**Тема: Моделирование объектов защиты и угроз безопасности**

**Вариант 1.6**

**Курск – 2010 г.**

**Вариант 1.6**

**СОДЕРЖАНИЕ**

* Титульный лист.
* Содержание, включающее следующие разделы.

1. Описание объекта защиты Стр.3

1.1. Исходные данные варианта; Стр.4

2. Моделирование объекта защиты: Стр.6

2.1. Структурная модель;

2.2. Пространственная модель; Стр.9

3. Моделирование угроз безопасности Стр.10

3.1. Моделирование способов физического проникновения; Стр.11

3.2. Моделирование технических каналов утечки информации; Стр.15

4.Выводы по работе Стр.21

5. Список использованных источников Стр.23

*Приложение:* Эскиз объекта информационной защиты. Стр.24

1. **Описание объекта защиты**

В качестве объекта информационной защиты рассмотрим некоторую небольшую организацию, оказывающую услуги населению в области ЖКХ, управляющую компанию по обслуживанию многоквартирных жилых домов. Структурная организация фирмы представлена следующими основными подразделениями, размещенными в отдельных комнатах в собственном двухэтажном здании на втором этаже:

R1. Генеральный директор

R2. Приемная

R3. Главный инженер

R4. Отдел кадров, юридический отдел

R5. Бухгалтерия

R6. Отдел проектирования и строительства

R7. Производственный отдел

* 1. **Исходные данные варианта;**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **О фирме** | | | | | | | | | | | |
| **1.1** | | **1.2** | | **1.3** | | **1.4** | | **1.5** | | **1.6** | |
| **Структура** | | **Методы управления** | | **Финансы** | | **Планы и программы** | | **Проблемы и пути их решения** | | **Безопасность** | |
| к | 350 | дсп |  | к | 380 | ск | 25 | дсп | 580 | к | 650 |
|  |  | 550 |  |  |  |  | 600 |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **О внутренней деятельности фирмы** | | | | | | | | | | | |
| **2.1** | | **2.2** | | **2.3** | | **2.4** | | **2.5** | | **2.6** | |
| **Качество продукции** | | **Себестоимость продукции** | | **Характеристики разрабатываемой продукции** | | **Возможности производства** | | **Исследовательский работы** | | **Технологии** | |
| ск | 250 | ск | 250 | ск | 500 | к |  | ск |  | кт |  |
|  | 700 |  |  |  |  | 50 | 150 | 400 |  | 200 | 800 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **О внешней деятельности фирмы** | | | | | | | | | | | |
| **3.1** | | **3.2** | | **3.3** | | **3.4** | | **3.5** | | **3.6** | |
| **Принципы,**  **концепция и стратегия маркетинга** | | **Каналы приобретения и сбыта** | | **Партнеры** | | **Конкуренты** | | **Переговоры и соглашения** | | **Участие в международном сотрудничестве** | |
| к | 650 | дсп |  | ск | 250 | дсп |  | ск | 25 | к | 650 |
|  |  | 550 |  |  |  | 550 |  |  | 600 |  |  |

Формат элемента конфиденциальной информации имеет следующую графическую структуру:

|  |  |
| --- | --- |
| Гриф конфиденциальности | Количество страниц бумажного носителя |
| Объем в Кб (для электр. носителя) | Цена информации (для эксп. оценки) |

Цена элемента информации имеет относительный характер

|  |  |
| --- | --- |
| Гриф конфиденциальности информации | Условная цена единицы информации |
| ДСП (для служебного пользования) | 0.2 |
| К (конфиденциально) | 0.4 |
| СК (строго конфиденциально) | 0.6 |
| КТ (коммерческая тайна) | 1 |

1. **Моделирование объекта защиты**

**2.1. Структурная модель**

Считается, что цена элемента информации может быть определена двумя способами – методом экспертных оценок и по формулам.

* Определение цены элемента информации методом экспертных оценок может осуществляться, если известен ущерб, который будет причинен фирме в случае утечки этой информации. При этом вид и объем информации не влияют на эту цену.
* Цена элемента информации может вычисляться по формуле, учитывающей объем информации и цену единицы ее объема.

В расчете цены элемента информации, размещенного на электронном носителе будем использовать формулу:

C = V · S, где C – цена элемента информации;

V – объем информации в Кб;

S – условная цена единицы информации

В расчете цены элемента информации, размещенного на бумажном носителе воспользуемся формулой:

C = 2.5· V · S , где C – цена элемента информации;

V – объем информации в страницах;

S – условная цена единицы информации

Результат расчета цены для всех элементов информации

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№**  **элемента информации** | **Наименование элемента информации** | **Гриф конфиденциальности информации.** | **Объем**  **в Кб** | **Объем**  **В стр.** | **Вид расчета**  **(Ф -формула;**  **Э-экспертная оценка)** | **Цена элемента информации** |
| 1.1 | Структура | К | 0 | 350 | Ф | 350 |
| 1.2 | Методы управления | ДСП | 550 | 0 | Ф | 110 |
| 1.3 | Финансы | К | 0 | 380 | Ф | 380 |
| 1.4 | Планы и программы | СК | 0 | 25 | Э | 600 |
| 1.5 | Проблемы и пути их решения | ДСП | 0 | 580 | Ф | 290 |
| 1.6 | Безопасность | К | 0 | 650 | Ф | 650 |
| 2.1 | Качество продукции | СК | 0 | 250 | Э | 700 |
| 2.2 | Себестоимость продукции | СК | 0 | 250 | Ф | 375 |
| 2.3 | Характеристики разрабатываемой продукции | СК | 0 | 500 | Ф | 750 |
| 2.4 | Возможности производства | К | 50 | 0 | Э | 150 |
| 2.5 | Исследовательский работы | СК | 400 | 0 | Ф | 240 |
| 2.6 | Технологии | КТ | 200 | 0 | Э | 800 |
| 3.1 | Принципы,  концепция и стратегия маркетинга | К | 0 | 650 | Ф | 650 |
| 3.2 | Каналы приобретения и сбыта | ДСП | 550 | 0 | Ф | 110 |
| 3.3 | Партнеры | СК | 0 | 250 | Ф | 375 |
| 3.4 | Конкуренты | ДСП | 550 | 0 | Ф | 125 |
| 3.5 | Переговоры и соглашения | СК | 0 | 25 | Э | 600 |
| 3.6 | Участие в международном сотрудничестве | К | 0 | 650 | Ф | 650 |

Результаты, расчета цены и эскиз объекта информационной защиты позволяют получить структурную модель объекта защиты.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  элемента информации | Наименование элемента информации | Гриф конфиденциаль-ности информации | Цена элемента информации | Наименование источника информации | Местонахождение источника информации |
| 1.1 | Структура | К | 350 | См п.1 | R4, R3 |
| 1.2 | Методы управления | ДСП | 110 | См п.1 | R1, R3 |
| 1.3 | Финансы | К | 380 | См п.1 | R4, R5 |
| 1.4 | Планы и программы | СК | 600 | См п.1 | R1, R4, R6 |
| 1.5 | Проблемы и пути их решения | ДСП | 290 | См п.1 | R3, R4,R7 |
| 1.6 | Безопасность | К | 650 | См п.1 | R1, R3 |
| 2.1 | Качество продукции | СК | 700 | См п.1 | R6 |
| 2.2 | Себестоимость продукции | СК | 375 | См п.1 | R2, R5 |
| 2.3 | Характеристики разрабатываемой продукции | СК | 750 | См п.1 | R6 |
| 2.4 | Возможности производства | К | 150 | См п.1 | R3, R7 |
| 2.5 | Исследовательский работы | СК | 240 | См п.1 | R1, R6 |
| 2.6 | Технологии | КТ | 800 | См п.1 | R6 |
| 3.1 | Принципы,  концепция и стратегия маркетинга | К | 650 | См п.1 | R1, R2, R4 |
| 3.2 | Каналы приобретения и сбыта | ДСП | 110 | См п.1 | R3, R5 |
| 3.3 | Партнеры | СК | 375 | См п.1 | R1, R3, R4 |
| 3.4 | Конкуренты | ДСП | 125 | См п.1 | R1, R3, R4 |
| 3.5 | Переговоры и соглашения | СК | 600 | См п.1 | R1, R3, R4 |
| 3.6 | Участие в международном сотрудничестве | К | 650 | См п.1 | R1, R3, R4, R5 |

**2.2. Пространственная модель объекта информационной защиты.**

|  |  |  |
| --- | --- | --- |
| **№**  **элемента** | **Наименование элемента**  **пространственной зоны** | **Характеристики пространственной зоны** |
| 1 | Этаж | 2. Здание двухэтажное |
| 2 | Количество окон, наличие штор, решеток | 11, на всех окнах жалюзи, на 1 окне решетка. |
| 3 | Двери: количество и какие | 12, 3-стальные, обшитые деревом, выходящие на улицу, 7-деревянные в помещениях, 2 – металлические усиленные с кодовым замком в R4 и R5 |
| 4 | Соседние помещения: название, толщина стен | Нет; кирпичная кладка 65 см, облицовка. |
| 5 | Помещение над потолком: название, толщина перекрытий | Нет, железобетонные плиты, 30 см. |
| 6 | Помещение под потолком:  название, толщина перекрытий | Офисные помещения, железобетонные плиты, 30 см. |
| 7 | Вентиляционные отверстия: места размещения, размеры | Туалет, 15х20 |
| 8 | Батарея отопления | 15 батарей расположенных вдоль окон и 2 стояка уходящих на 1-й этаж. Все трубы выведены через подвал в теплоцентрали. |
| 9 | Цепи электропитания | Цепь электропитания фирмы подключена к городской сети напряжением 220 В частотой 50 Гц. У центрального входа в помещении находится электрический щиток. К цепи электропитания подключены все кабинеты и помещения. В помещениях находится 29 розеток. Источник бесперебойного питания. |
| 10 | Телефон | Мини АТС Samsung подключено 10 телефонов кабелем UTP, один из них системный –Т2 |
| 11 | Радиотрансляция | Отсутствует |
| 12 | Электрические часы | Отсутствуют |
| 13 | Бытовые радиосредства, телевизоры, аудио- и видео магнитофоны, их типы | Отсутствуют |
| 14 | Бытовые электроприборы | Кондиционеры(Samsung S418 ZAOD), 4 шт. |
| 15 | ПЭВМ | 11 шт.Офисные ПК 2,4ГГц ,1Гб ОЗУ, 200Гб HDD Все компьютеры имеют доступ к сети Internet , 2шт. Коммутатора LAN D-Link 8 портов, 1шт ADSL модем Zyxel HT 660. Все входит в состав локальной сети, все компьютеры имеют выход в интернет. |
| 16 | Технические средства охраны | Датчики движения – 4 шт., датчики вскрытия – на входных дверях + 11 на окнах, вывод на телефонную линию и звуковые извещатели. |
| 17 | Телевизионные средства наблюдения | Отсутствуют |
| 18 | Пожарная сигнализация | Помещение оборудовано пожарным дымовым линейным извещателем ИП 212-7 (ИДПЛ). Температурные и дымовые детекторы, расположенные во всех помещениях, кроме санузла и коридора. Они подключены к телефонной линии. |

1. **Моделирование угроз безопасности**

Моделирование угроз безопасности информации позволяет оценить ущерб, который может быть нанесен фирме в результате хищения элементов конфиденциальной информации, представленной с помощью разработанной ранее структурной модели.

Моделирование угроз включает:

1. моделирование способов физического проникновения злоумышленника к источникам информации;
2. моделирование технических каналов утечки информации;

Действие злоумышленника по добыванию информации и материальных ценностей определяется поставленными целями и задачами, мотивацией, квалификацией и технической оснащенностью. Прогноз способов физического проникновения следует начать с выяснения, кому нужна защищаемая информация. Для создания модели злоумышленника необходимо мысленно проиграть с позиции злоумышленника варианты проникновения к источникам информации. Чем больше при этом будет учтено факторов, влияющих на эффективность проникновения, тем выше будет вероятность соответствия модели реальной практике. В условиях отсутствия информации о злоумышленнике лучше переоценить угрозу, хотя это может привести в увеличению затрат.

* 1. **Моделирование способов физического проникновения**

Важным фактором при выборе пути злоумышленником является оценка реальности этого пути. Реальность пути связана с вероятностью выбора злоумышленником этого пути. Она определялась методом экспертных оценок. Вероятность зависит от простоты реализации именного этого пути проникновения. Очевидно, что через некоторые окна и двери легче проникнуть, поэтому следующие соображения:

1. Проникнуть легче через дверь, чем через окно;
2. Легче проникнуть в окно, не содержащее дополнительных средств защиты, чем в окно с решетками;
3. Проникнуть легче через обычную дверь, чем через железную;
4. Чем больше нужно миновать препятствий, тем путь менее вероятен;

Определим следующие оценки Or реальности пути:

1. Or=0,1 - для маловероятных путей;

2. Or=0,5 - для вероятных путей ;

3. Or=0,9 - для наиболее вероятных путей.

Величина угрозы находится по формуле:

D=Or ∙ Si ,

где: D – величина угрозы, выраженная в условных единицах;

Or – оценка реальности пути;

Si – цена элемента информации i .

Для формализации оценки угрозы введем ранжирование величины угрозы по ее интервалам, сопоставляемым с рангами.

* Определим диапазон значений величин угроз от 1 до Dmax=800;
* вводится в рассмотрение, например, 6 ранга;
* устанавливается наивысший по значимости ранг R1=1 для угроз, имеющих значительные величины;
* определяется линейный интервал ранга d=Dmax/6, d=133
* соответствие рангов угроз и интервалов величин угроз определяется следующими формулами:

R6=6 : [1÷ R6max], R6max = d-1;

Ri=i : [(R(i+1)max +1)÷ Rimax] , Rimax = R (i-1)max + d; i = (2,3,4,5);

R1=1 : [ >R2max +1].

Пусть максимальная величина угрозы Dmax = 800, тогда d=200.

Определяем ранги и интервалы значений угроз:

R6=6 для интервала [ 1÷ 132];

R5=5 для интервала [133 ÷ 265];

R4=4 для интервала [266 ÷ 398];

R3=3 для интервала [399 ÷ 531];

R2=2 для интервала [532 ÷ 664];

R1=1 для интервала [ > 665];

Полученная система рангов представлена в таблице

|  |  |
| --- | --- |
| Интервал величины угрозы | Ранг угрозы Ri |
| 665 - | 1 |
| 532 – 664 | 2 |
| 399 – 531 | 3 |
| 266 – 398 | 4 |
| 133 – 265 | 5 |
| 1 – 132 | 6 |

Из таблицы рангов видно, что наиболее уязвимой является информация от R3 и выше, то есть величиной от 399 и выше.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Наименование элемента информации | Цена информации | Цель (комната) | Путь проникновения злоумышленника | Оценка реальности пути | Величина угрозы в условных единицах | Ранг угрозы |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| 1 | Технологии | 800 | R6 | w10  d2-d10 | 0.5  0.5 | 400 | 3 |
| 2 | Характеристики разрабатываемой продукции | 750 | R6 | w10  d2-d10 | 0.5  0.5 | 375 | 4 |
| 3 | Безопасность | 650 | R1, R3 | d1-d3  w1-d3  d2-d5-d4  d2-d6 | 0.5  0.5  0.5  0,5 | 325 | 4 |
| 4 | Принципы,  концепция и стратегия маркетинга | 650 | R1, R2, R4 | d1-d3  w1-d3  d2-d5-d4  d2-d5  d2-d7 | 0.5  0.5  0.5  0.5  0.1 | 325 | 4 |
| 5 | Участие в международном сотрудничестве | 650 | R1, R3, R4, R5 | d1-d3  w1-d3  d2-d5-d4  d2-d6  d2-d7  w11  d12  d2-d11 | 0.5  0.5  0.5  0.5  0.1  0.5  0.5  0.1 | 325 | 4 |
| 6 | Планы и программы | 600 | R1, R4, R6 | w10  d2-d10  d1-d3  w1-d3  d2-d7 | 0.5  0.5  0.5  0.5  0.1 | 300 | 4 |
| 7 | Переговоры и соглашения | 600 | R1, R3, R4 | d1-d3  w1-d3  d2-d5-d4  d2-d6  d2-d7 | 0.5  0.5  0.5  0.5  0.1 | 300 | 4 |

Следуя из результатов таблицы предлагаются следующие меры для улучшения защиты информации. Самым уязвимым является элемент Технологии с рангом 3 и комната R6.

1. Поставить решетки на окна w9, W10
2. Дверь d10 заменить на металлическую.

Все остальные элементы получили ранг ниже третьего, их рассматривать мы не будем.

**3.2. Моделирование технических каналов утечки информации**

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное оборудование технических средств обработки информации, оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т.п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы, такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, электробытовые приборы и др. В качестве каналов утечки интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При моделировании технических каналов утечки, помимо выявления самих каналов, т.е. источника сигнала, пути утечки, определяется оценка реальности канала, величина и ранг угрозы.

Оценка реальности канала определяется как отношение стоимости информации к стоимости реализации канала утечки, а величина угрозы - как произведение стоимости информации на оценку реальности канала.

|  |  |
| --- | --- |
| Интервал величины угрозы | Ранг угрозы Ri |
| 665 - | 1 |
| 532 – 664 | 2 |
| 399 – 531 | 3 |
| 266 – 398 | 4 |
| 133 – 265 | 5 |
| 1 – 132 | 6 |

*Пропускная способность канала утечки информации:*

* для акустической радиозакладки:

C0 = ΔF\*log2(1+q) [Бод], где ΔF - ширина полосы частот сигнала [Гц];

q - средне спектральное соотношение сигнал/помеха по мощности [дБ];

* для визуального (фото) контроля:

C0 = k\*F0\*(m×n)\*log2(1+q) [Бод], где F0 – частота кадров изображения;

m×n – число элементов разрешения в кадре; k – коэффициент конфиденциальной информации.

*Стоимость элемента информации:*

Cи = C0\*t\*Cэ , где С0 – пропускная способность канала утечки информации; t – время работы канала; Cэ – стоимость 1 Кбайта элемента информации.

*Оценка реальности канала утечки информации:*

α = Cи/Cку, где Cи – стоимость элемента информации;

Cку – стоимость канала утечки информации.

*Величина угрозы:*

Cу = Cи\*α, где Cи – стоимость элемента информации;

α - оценка реальности канала утечки информации.

Характеристики технических каналов утечки информации.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование средства съема информации | ΔF, Гц | q, дБ | C0, Кбод | t, с (в день) | Cку, |
| Телефонная закладка | 400 | 20 | 0,34 | 600 | 10000 |
| Направленный микрофон | 5700 | 10 | 2,4 | 600 | 24000 |
| Лазерный микрофон | 5700 | 20 | 3,1 | 600 | 450000 |
| Акустическая радио закладка | 1440 | 40 | 0,94 | 600 | 18000 |
| Селективный вольтметр | 40000 | 10 | 16,8 | 600 | 65000 |
| Минивидеокамера (800×600) | F0=75 | 50 | 12463 | 600 | 150000 |

Модель технических каналов утечки информации

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ эл. инф.** | **Наименование элемента информации** | **Цена инф-ии** | **Источник сигнала, передающее устройство** | **Путь утечки** | **Вид канала** | **Оценка реаль-ности канала** | **Величина угрозы** | **Ранг угрозы** |
| 1 | Технологии | 800 | 1) Мини видеокамера | 1) Скрытый визуальный контроль при помощи мини видеокамеры | 1) Опторадио- электронный | 0,598 | 478 | 3 |
| 2 | Характеристики разрабатываемой продукции | 750  750  750 | 1) Мини видеокамера   2) ПЭМИН кабеля  3) ПЭМИН монитора | 1) Скрытый визуальный контроль при помощи мини видеокамеры 2) Сканиро-вание при помощи селективного вольтметра  3) Сканиро-вание при помощи селективного вольтметра | 1) Опторадио- электронный 2) Радио-электронный  3) Радио-электронный | 0,598 0,866  1,861 | 448 650  1395 | 3 2  1 |
| 3 | Принципы, концепция и стратегия маркетинга | 650 | 1) Мини видеокамера | 1) Скрытый визуальный контроль при помощи мини видеокамеры | 1) Опторадио- электронный | 0,598 | 388 | 4 |
| 4 | Переговоры и соглашения | 600  600  600  600  600 | 1) Мини видеокамера2) ПЭМИН кабеля 3) ПЭМИН монитора  4) Человек, направленный микрофон  5) Человек, лазерный микрофон | 1) Скрытый визуальный контроль при помощи мини видеокамеры2) Сканиро-вание при помощи селективного вольтметра 3) Сканиро-вание при помощи селективного вольтметра  4)Подслушивание с помощью направленного микрофона  5)Подслушивание с помощью лазерного микрофона | 1) Опторадио- электронный2) Радио-электронный 3) Радио-электронный  4)Акустический  5)Оптоэлектронный | 0,359 0,26  1,117  0,432  0,03 | 215 156  670  260  18 | 5 5  1  5  6 |
| 5 | Планы и программы | 600 | 1) Мини видеокамера | 1) Скрытый визуальный контроль при помощи мини видеокамеры | 1) Опторадио- электронный | 0,359 | 215 | 5 |
| 6 | Исследовательский работы | 240  240  240 | 1) Мини видеокамера   2) ПЭМИН кабеля  3) ПЭМИН монитора | 1) Скрытый визуальный контроль при помощи мини видеокамеры 2) Сканиро-вание при помощи селективного вольтметра  3) Сканиро-вание при помощи селективного вольтметра | 1) Опторадио- электронный 2) Радио-электронный  3) Радио-электронный | 0,359 0,345  1,117 | 86 82  268 | 6 3  4 |
| 7 | Партнеры | 375  375  375  375  375  375 | 1) ПЭМИН кабеля 2) ПЭМИН монитора  3) Человек, направленный микрофон  4) Человек, лазерный микрофон  5) Человек, телефонная закладка  6) Человек, акустическая радиозакладка | 1) Сканиро-вание при помощи селективного вольтметра 2) Сканиро-вание при помощи селективного вольтметра  3)Подслушивание с помощью направленного микрофона  4)Подслушивание с помощью лазерного микрофона  5)Подслушивание с помощью телефонной закладки  6)Подслушивание с помощью акустической радиозакладки | 1) Радио-электронный 2) Радио-электронный  3)Акустический  4)Оптоэлектронный  5)Акустоэлектрический  6)Акусторадиоэлектронный | 0,057 1,117  0,432  0,03  0,147  0,226 | 21 440  162  11  56  85 | 6 3  5  6  6  6 |
| 8 | Проблемы и пути их решения | 290  290  290  290  290  290  4060,8 | 1) Мини видеокамера2) ПЭМИН кабеля 3) ПЭМИН монитора  4) Человек, направленный микрофон  5) Человек, лазерный микрофон  6) Человек, телефонная закладка  7) Человек, акустическая радиозакладка | 1) Скрытый визуальный контроль при помощи мини видеокамеры2) Сканиро-вание при помощи селективного вольтметра 3) Сканиро-вание при помощи селективного вольтметра  4)Подслушивание с помощью направленного микрофона  5)Подслушивание с помощью лазерного микрофона  6)Подслушивание с помощью телефонной закладки  7)Подслушивание с помощью акустической радиозакладки | 1) Опторадио- электронный2) Радио-электронный 3) Радио-электронный  4)Акустический  5)Оптоэлектронный  6)Акустоэлектрический  7)Акусторадиоэлектронный | 0,359 0,26  1,117  0,432  0,03  0,147  0,226 | 7 75  323  125  8  216  918 | 6 6  4  4  6  5  5 |

**4.Выводы по работе**

Для несанкционированного добывания информации в настоящее время используется широкий арсенал технических средств, из которых малогабаритные технические средства отражают одно из направлений в развитии современных разведывательных технологий. Выполняемые в портативном, миниатюрном и сверхминиатюрном виде, эти средства аккумулируют в себе новейшие научные, технические и технологические достижения электроники, акустики, оптики, радиотехники и других наук. Такие средства находят широкое применение, как в деятельности правоохранительных органов, так и иностранных технических разведок, в подпольном информационном обеспечении незаконных экономических, финансовых и криминальных организаций. В условиях рыночной экономики появление значительного числа конкурирующих между собой различных структур естественным образом создало определенное пространство, на котором применение подобных устройств технической разведки для добывания информации различной значимости является наиболее вероятным.

Информационная сфера играет все возрастающую роль в обеспечении безопасности всех сфер жизнедеятельности общества. Через эту сферу реализуется значительная часть угроз не только национальной безопасности государства, но и экономическому благополучию учреждений и предприятий.

Одними из основных источников угроз информационной безопасности для последних – преступные сообщества, конкурентные организации, группы и формирования и противозаконная деятельность отдельных лиц, направленная на сбор или хищение ценной информации, закрытой для доступа посторонних лиц. Причем в последние годы приоритет в данной сфере деятельности смещается в экономическую область.

Главной причиной возникновения промышленного (экономического) шпионажа является стремление к реализации конкурентного преимущества – важнейшего условия достижения успеха в рыночной экономике. Охота за чужими секретами позволяет компаниям экономить собственные средства на ведение НИОКР и фундаментальные исследования, быть в курсе дел конкурентов, использовать их научно-технические достижения.

Западный опыт промышленного шпионажа сегодня активно переносится на территорию России. В нашей стране промышленный шпионаж осуществляется в целях: овладения рынками сбыта, подделки товаров, дискредитации или устранения (физического или экономического подавления) конкурентов, срыва переговоров по контрактам, перепродажи фирменных секретов, шантажа определенных лиц, создания условий для подготовки и проведения террористических и диверсионных акций).

На рынке России представлен арсенал самых современных технических средств промышленного шпионажа, которые находят все более широкое применение на практике. К ним относятся: визуально-оптические, фотографические, телевизионные, тепловизионные (инфракрасные), акустические, радио-, радиотехнические и некоторые другие средства разведки.

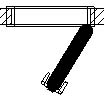
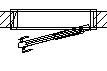
Для организации защиты конфиденциальной информации необходимо знать возможности технических средств промышленного шпионажа и способы их применения.

Итак, можно сделать вывод, что защита информации от несанкционированного физического доступа и от утечки по техническим каналам является сложной и важной задачей. В то же время, расчет моделей физического доступа и утечки по техническим каналам позволяет избежать лишних расходов на защиту информации, сделать этот процесс рациональным и управляемым.

1. **Список использованных источников**
2. Способы и средства защиты информации. Хорев А.А М.: МО РФ, 1996.
3. Защита информации в офисе. И. К. Корнеев, Е. А. Степанов. 336 стр. ТК Велби, Проспект, 2008 г.
4. Комплексная защита информации в корпоративных системах. В. Ф. Шаньгин. 592 стр.Форум, Инфра-М, 2010 г.
5. Утечка и защита информации в телефонных каналах. А. В. Петраков, В. С. Лагутин. 324 стр. РадиоСофт, 2009 г.
6. Комплексная защита информации на предприятии. В. А. Северин, 368 стр. Городец, 2008 г.
7. Информационная безопасность и защита информации. В. П. Мельников, С. А. Клейменов, А. М. Петраков. 336 стр. Академия, 2009 г.
8. Оценка необходимости защиты информации предприятия. Галкин А. П. // Вестник ассоциации Русская оценка. 1999. № 1. С. 55-58.

**Условные обозначения на эскизе**

Дверь Металлическая дверь



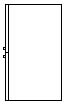
Окно Окно с решеткой



Компьютер Телефон



Сейф Шкаф



Стол

