**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ**

**КУРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

Кафедра Комплексной защиты информационных систем

Пояснительная записка к курсовой работе

по дисциплине

«Технические средства охраны объектов» специальности 090104 – Комплексная защита объектов информатизации

**Выполнил** студент группы ЗИ – 51 Львов Р.Л.

**Проверил** к.т.н. с.н.с. Карасовский В.В.

2009 г.

**Содержание**

|  |  |
| --- | --- |
| 1. Исходные данные варианта………………………………………………… | 3 стр. |
| 1.1. Структурная модель …………………………………………………..….. | 4 стр. |
| 1.2 Пространственная модель ………………………………………………… | 7 стр. |
| 1.3 Эскиз………………………………………………………………..………. | 9 стр. |
| 2. Моделирование угроз безопасности.……………………………………….. | 10 стр. |
| 2.1. Моделирование способов физического проникновения………….… | 10 стр. |
| 3. Предложения по техническому оснащению средствами охраны  охраняемого объекта…………………………………………………….…….. | 14 стр. |
| 4. Вывод…………………………………………………………………………. | 17 стр. |
| 5. Список используемой литературы………………………………………….. | 18 стр. |
| Приложение №1………………………………………………………………… | 19 стр. |

1. Исходные данные варианта.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ вар.** | **Элементы информации** | | | | | | | | | | | | | | | | | |
| **1.1** | | **1.2** | | **1.3** | | **1.4** | | **1.5** | | **1.6** | | **2.1** | | **2.2** | | **2.3** | |
| **1.10** | к | 400 | кт | 300 | к | 300 | к |  | к | 250 | дсп | 900 | кт |  | к |  | к |  |
|  |  |  | 300 |  |  | 270 | 450 |  | 300 |  |  | 450 |  | 500 | 650 | 450 |  |
| **№ вар.** | **Элементы информации** | | | | | | | | | | | | | | | | | |
| **2.4** | | **2.5** | | **2.6** | | **3.1** | | **3.2** | | **3.3** | | **3.4** | | **3.5** | | **3.6** | |
| **1.10** | ск | 100 | ск |  | дсп | 550 | дсп | 900 | кт | 300 | к |  | кт | 300 | к |  | дсп | 900 |
|  | 600 | 200 | 750 |  |  |  |  |  | 300 | 500 | 650 |  | 300 | 270 | 450 |  |  |

1.1 Структурная модель.

Разработка структурной модели связано со структурированием информации и предусматривает классификацию информации, учитывающую структуру, функции и задачи объекта защиты с обязательной привязкой элементов информации к ее источникам. Детализация информации проводится до уровня, на котором элементу информации соответствует один источник.

Гриф конфиденциальности информации и ее цена определяются в соответствии с выбранным вариантом задания, т.е. определяются конкретными форматами элементов информации.

Предполагается, что вышеуказанная информация может быть представлена в виде:

1. Бумажного документа (с указанием количества страниц)
2. Электронного документа (с указанием объема в Кбайтах)
3. Бумажного или электронного документа (без указания объема)

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 расчетах цены элементов информации используется условная цена единицы информации (1е.и.=1Кбайт), зависящая от грифа конфиденциальности представленная в таблице 4. Условная цена является относительной величиной и характеризует соотношение абсолютных цен различных видов защищаемой конфиденциальной информации. Очевидно, что в этом случае цена элемента информации также будет иметь относительный характер.

**Таблица 1. Условная цена единицы информации.**

|  |  |
| --- | --- |
| **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 |

В расчете цены элемента информации, размещенного на электронном носителе используется формула:

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 используется формула:

C = 2.5· V · S ,

где C – цена элемента информации;

V – объем информации в страницах;

S – условная цена единицы информации

Коэффициент 2.5 в формуле (2) объясняется следующими соображениями. Средний объем информации на странице размером А4 для шрифта кеглем 14 составляет примерно 4 тысячи знаков или 4 Кб. Учитывая, что листы обычно не бывают заполненными полностью, принимается средний объем информации – 2.5 Кб на страницу.

**Пример расчета цены для элемента информации №1.1, 1.2, 1.3,1.4:**

1. **элемент №1.1**

С=2,5\*400\*0,4=400;

1. **элемент №1.2**

С=300 (экспертная оценка);

1. **элемент №1.3**

С=2,5\*300\*0,4=300;

1. **элемент №1.4**

С=450 (экспертная оценка).

**Таблица 2. Расчет цены для всех элементов информации.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№**  **элемента инфор-мации** | **Наименование элемента информации** | **Гриф конфиден-циальности информации.** | **Объем**  **в Кб** | **Объем**  **В стр.** | **Вид расчета**  **(Ф –формула;**  **Э-экспертная оценка)** | **Цена элемента информации** |
| 1.1 | Структура | К |  | 400 | Ф | 400 |
| 1.2 | Методы управления | КТ |  | 300 | Э | 300 |
| 1.3 | Финансы | К |  | 300 | Ф | 300 |
| 1.4 | Планы и программы | К | 270 |  | Э | 450 |
| 1.5 | Проблемы и пути их решения | К |  | 250 | Э | 300 |
| 1.6 | безопасность | ДСП |  | 900 | Ф | 450 |
| 2.1 | Качество продукции | КТ | 450 |  | Ф | 450 |
| 2.2 | Себестоимость продукции | К | 500 |  | Э | 650 |
| 2.3 | Характеристики разрабатываемой продукции | К | 450 |  | Ф | 180 |
| 2.4 | Возможности производства | СК |  | 100 | Э | 600 |
| 2.5 | Исследовательский работы | СК | 200 |  | Э | 750 |
| 2.6 | Технологии | ДСП |  | 550 | Ф | 275 |
| 3.1 | Принципы, концепция и стратегия маркетинга | ДСП |  | 900 | Ф | 450 |
| 3.2 | Каналы приобретения и сбыта | КТ |  | 300 | Э | 300 |
| 3.3 | Партнеры | К | 500 |  | Э | 650 |
| 3.4 | Конкуренты | КТ |  | 300 | Э | 300 |
| 3.5 | Переговоры и соглашения | К | 270 |  | Э | 450 |
| 3.6 | Участие в международном сотрудничестве | ДСП |  | 900 | Ф | 450 |

Результаты, представленные в таблице 2 и эскиз объекта информационной защиты позволяют получить структурную модель объекта защиты в формате таблицы 5.

**Таблица 3. Структурную модель объекта защиты.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **элемента информации** | **Наименование элемента информации** | **Гриф конфиденциальности информации.** | **Цена элемента информации** | **Наименование источника информации** | **Местонахождение источника информации** |
| 1.1 | Структура | К | 400 | Бумажный  носитель | Бухгалтерия |
| 1.2 | Методы управления | КТ | 300 | Бумажный  носитель | Директор |
| 1.3 | Финансы | К | 300 | Электронный  носитель | Финансовый отдел |
| 1.4 | Планы и программы | К | 450 | Бумажный  носитель | Отдел разработок |
| 1.5 | Проблемы и пути их решения | К | 300 | Электронный  носитель | Отдел разработок |
| 1.6 | безопасность | ДСП | 450 | Электронный  носитель | Технический отдел №1 |
| 2.1 | Качество продукции | КТ | 450 | Электронный  носитель | Технический отдел №2 |
| 2.2 | Себестоимость продукции | К | 650 | Электронный  носитель | Отдел маркетинга |
| 2.3 | Характеристики разрабатываемой продукции | К | 180 | Бумажный  носитель | Технический отдел №2 |
| 2.4 | Возможности производства | СК | 600 | Электронный  носитель | Отдел разработок |
| 2.5 | Исследовательский работы | СК | 750 | Бумажный  носитель | Отдел разработок |
| 2.6 | Технологии | ДСП | 275 | Бумажный  носитель | Технический отдел №1 |
| 3.1 | Принципы, концепция и стратегия маркетинга | ДСП | 450 | Электронный  носитель | Отдел маркетинга |
| 3.2 | Каналы приобретения и сбыта | КТ | 300 | Бумажный  носитель | Отдел маркетинга |
| 3.3 | Партнеры | К | 650 | Электронный  носитель | Отдел маркетинга |
| 3.4 | Конкуренты | КТ | 300 | Бумажный  носитель | Отдел маркетинга |
| 3.5 | Переговоры и соглашения | К | 450 | Бумажный  носитель | Отдел маркетинга |
| 3.6 | Участие в международном сотрудничестве | ДСП | 450 | Электронный  носитель | Отдел маркетинга |

1.2 Пространственная модель.

Пространственная модель объекта информационной защиты – табличное описание пространственных зон с указанием месторасположения источников защищаемой информации. Источником для получения пространственной модели является разработанный ранее эскиз объекта информационной защиты. Пространственная модель представляется в формате таблицы 6:

**Таблица 4. Пространственная модель.**

|  |  |  |
| --- | --- | --- |
| **№**  **эл-та** | **Наименование элемента**  **пространственной зоны** | **Характеристики пространственной зоны** |
| 1 | Этаж | 1. Здание одноэтажное. |
| 2 | Количество окон, наличие штор, решеток | 16, на всех окнах жалюзи, 10 окон с решеткой. |
| 3 | Двери: количество и какие | 13 железных дверей с деревянным покрытием, 1 – входная двойная, 4 – стальные с кодовым замком. |
| 4 | Соседние помещения: название, толщина стен | Нет; кирпичная кладка 40 см. |
| 5 | Помещение над потолком: название, толщина перекрытий | Нет, железобетонные плиты, 35 см. |
| 6 | Помещение под потолком:  название, толщина перекрытий | Офисные помещения, железобетонные плиты, 25 см. |
| 7 | Вентиляционные отверстия: места размещения, размеры | Во всех помещениях (10 шт.), 20х20 см. |
| 8 | Батарея отопления | 17 батарей расположенных вдоль стен. 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 21 розетка. |
| 10 | Телефон | Во всех помещениях, за исключением К6. |
| 11 | Радиотрансляция | Отсутствует |
| 12 | Электрические часы | В приемной, над главным входом. |
| 13 | Бытовые радиосредства, телевизоры, аудио- и видео магнитофоны, их типы | ЖК телевизоры, 2 штуки (директор, приемная). Спутниковй ресивер OpenBox x300, 2 штуки (директор, приемная). |
| 14 | Бытовые электроприборы | Кондиционеры(Samsung С300 Cold), 10 шт. |
| 15 | ПЭВМ | 18 шт.  1 ПЭВМ – ноутбук, директор (Asus, Intel Centrino Duo 2250 Ггц, 512 МВ Мв Geforce Go 7300, 1024 МВ memory, 200 Gb, WinXP Professional, Wi-Fi). 16 ПЭВМ – настольные компьютеры (Formoza, Intel Pentium 4 2750 Ггц, 512 МВ Geforce 2300, 1024 МВ memory, 100 Gb, WinXp Professional).  1 ПЭВМ - сервер модели Hewlett Packard Server STC-450, процессор INTEL Pentium 3000 МГц, система Windows 2000, модем, сетевая карта, хаб (Сервер). Все компьютеры имеют доступ к сети Internet , а также входят в состав локальной сети. |
| 16 | Технические средства охраны | Датчики движения – 13 шт., датчики вскрытия – на входных дверях + 18 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. |

1.3 Эскиз.



*Рис.1. Эскиз объекта информационной защиты.*

2. 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 к увеличению затрат.

1. Моделирование способов физического проникновения.

Этот вид моделирования рассматривает все возможные способы физического проникновения злоумышленника и доступа его к защищаемой информации. Способ физического проникновения предполагает выбор конкретного пути преодоления злоумышленником преград для доступа к защищаемым элементам информации. Этот путь может проходить через пространственные зоны, рассмотренный пространственной моделью. Для построения такого пути необходимо проанализировать эскиз объекта и пространственную модель. В качестве препятствий могут быть окна (*О*) и двери (*Д*), которые нужно преодолеть злоумышленнику для достижения цели.

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;

В зависимости от этих соображений предлагаются 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 .

**Расчет величины угроз:**

|  |  |  |
| --- | --- | --- |
| D1.1=0,5\*400=200  D1.2=0,5\*300=150  D1.3=0,9\*300=270  D1.4=0,5\*450=225  D1.5=0,5\*300=150  D1.6=0,5\*450=225 | D2.1=0,9\*450=405  D2.2=0,9\*650=585  D2.3=0,9\*180=162  D2.4=0,5\*600=300  D2.5=0,5\*750=375  D2.6=0,5\*275=137,5 | D3.1=0,9\*450=405  D3.2=0,9\*300=270  D3.3=0,9\*650=585  D3.4=0,9\*300=270  D3.5=0,9\*450=405  D3.6=0,9\*450=405 |

Для формализации оценки угрозы целесообразно ввести ранжирование величины угрозы по ее интервалам, сопоставляемым с рангами. Ранги угроз с линейной шкалой можно устанавливать из следующих соображений:

* Определяется диапазон значений величин угроз как (1 ÷ Dmax);
* вводится в рассмотрение 6 рангов;
* устанавливается наивысший по значимости ранг R1=1 для угроз, имеющих значительные величины;
* определяется линейный интервал ранга d=Dmax/6;
* 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].

Максимальная величина угрозы **Dmax = 585**.

Линейный интервал ранга **d=585/6=97,5**.

Определяем ранги и интервалы значений угроз:

R6=6 для интервала [ 1÷ 97,4];

R5=5 для интервала [97,5 ÷ 194];

R4=4 для интервала [195 ÷ 292,4];

R3=3 для интервала [292,5 ÷ 389];

R2=2 для интервала [390 ÷ 487,4];

R1=1 для интервала [ > 487,5];

**Таблица 7. Система рангов.**

|  |  |
| --- | --- |
| **Интервал величины угрозы** | **Ранг угрозы Ri** |
| 487,5- | 1 |
| 390 – 487,4 | 2 |
| 292,5 – 389 | 3 |
| 195 – 292,4 | 4 |
| 97,5 – 194 | 5 |
| 1 – 97,4 | 6 |

**Таблица 8. Модель способов физического проникновения.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | **Наименование элемента информации** | **Цена элемента информации** | **Цель (комната)** | **Путь проникновения злоумышленника** | **Оценка реальности пути** | **Величина угрозы в условных единицах** | **Ранг угрозы** |
| 1.1 | Структура | 400 | К3 | 1. О6  2.Д1-Д2-Д5  3. О16-Д2-Д5 | 0,5  0,5  0,1 | 200 | 4 |
| 1.2 | Методы управления | 300 | К4 | 1. О8  2. О11-Д8  3. О16-Д2-Д9-Д8 | 0,5  0,5  0,1 | 150 | 5 |
| 1.3 | Финансы | 300 | К8 | 1.Д1-Д11  2.О16-Д11  3.О13-Д13-Д11 | 0,9  0,5  0,1 | 270 | 4 |
| 1.4 | Планы и программы | 450 | К2 | 1.О2  2.Д1-Д2-Д4  3.О16-Д2-Д4 | 0,5  0,5  0,1 | 225 | 4 |
| 1.5 | Проблемы и пути их решения | 300 | К2 | 1.О2  2.Д1-Д2-Д4  3.О16-Д2-Д4 | 0,5  0,5  0,1 | 150 | 5 |
| 1.6 | безопасность | 450 | К1 | 1.О1  2.О16-Д2-Д3  3.Д1-Д2-Д3 | 0,5  0,1  0,5 | 225 | 4 |
| 2.1 | Качество продукции | 450 | К9 | 1.О14  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 405 | 2 |
| 2.2 | Себестоимость продукции | 650 | К7 | 1.О13  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 585 | 1 |
| 2.3 | Характеристики разрабатываемой продукции | 180 | К9 | 1.О14  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 162 | 5 |
| 2.4 | Возможности производства | 600 | К2 | 1.О2  2.Д1-Д2-Д4  3.О16-Д2-Д4 | 0,5  0,5  0,1 | 300 | 3 |
| 2.5 | Исследовательский работы | 750 | К2 | 1.О2  2.Д1-Д2-Д4  3.О16-Д2-Д4 | 0,5  0,5  0,1 | 375 | 3 |
| 2.6 | Технологии | 275 | К1 | 1.О1  2.О16-Д2-Д3  3.Д1-Д2-Д3 | 0,5  0,1  0,5 | 137,5 | 5 |
| 3.1 | Принципы, концепция и стратегия маркетинга | 450 | К7 | 1.О13  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 405 | 2 |
| 3.2 | Каналы приобретения и сбыта | 300 | К7 | 1.О13  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 270 | 4 |
| 3.3 | Партнеры | 650 | К7 | 1.О13  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 585 | 1 |
| 3.4 | Конкуренты | 300 | К7 | 1.О13  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 270 | 4 |
| 3.5 | Переговоры и соглашения | 450 | К7 | 1.О13  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 405 | 2 |
| 3.6 | Участие в международном сотрудничестве | 450 | К7 | 1.О13  2.Д1-Д13  3.016-Д13 | 0,9  0,1  0,5 | 405 | 2 |

По результатам анализа модели физического проникновения можно предложить конкретные меры улучшения защиты элементов информации, представленные в первую очередь для элементов информации с рангами 1,2,3.

**Таблица 9. Меры по улучшению защиты.**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование элемента информации** | **Ранг угрозы** | **Меры по улучшению защиты** |
| 2.2 | Себестоимость продукции | 1 | Установка в помещение К8 датчика движения. |
| 3.3 | Партнеры | Установка видеокамер для наблюдения окна О1. |
| 2.1 | Качество продукции | 2 | Установка решеток на окна О12-О16.  Установка видеокамер для наблюдения окон О12-О14 и О-15-О16.  Установка датчиков движения в помещения К7,К9,К10. |
| 3.1 | Принципы, концепция и стратегия маркетинга |
| 3.5 | Переговоры и соглашения |
| 3.6 | Участие в международном сотрудничестве |
| 2.4 | Возможности производства | 3 |
| 2.5 | Исследовательские работы |

#### Предложения по техническому оснащению средствами охраны охраняемого объекта.

- Установка в помещение К8 датчика движения;

- Установка видеокамер для наблюдения окна О1;

- Установка решеток на окна О12-О16;

- Установка видеокамер для наблюдения окон О12-О14 и О-15-О16;

- Установка датчиков движения в помещения К7,К9,К10.

Таблица7

|  |  |  |  |
| --- | --- | --- | --- |
| **Шифр помеще-ния** | **Шифр элемента в помещении** | **Шифр системы обеспечения безопасности** | **Режим работы системы обеспечения безопасности** |
| К7 | Контроллер охраны (датчик движения) | О12 | Защита от проникновения |
| К8 | Контроллер охраны (датчик движения) | Д11 | Защита от проникновения |
| К9 | Контроллер охраны (датчик движения) | О14 | Защита от проникновения |
| К10 | Контроллер охраны (датчик движения) | О16 | Защита от проникновения |
| К1 | Видеокамера;  Решетка на окно | О1 | Защита от проникновения;  Отслеживание нарушителей |
| К7 | Решетка на окно | О12 | Защита от проникновения |
| К7 | Решетка на окно | О13 | Защита от проникновения |
| К9 | Видеокамера;  Решетка на окно | О14 | Защита от проникновения;  Отслеживание нарушителей |
| К9 | Видеокамера;  Решетка на окно | О15 | Защита от проникновения;  Отслеживание нарушителей |
| К10 | Решетка на окно | О16 | Защита от проникновения |

Контроллер охраны TSS-740 предназначен для построения различных систем охраны и контроля удаленных объектов, в том числе – охранно-пожарных систем.

В памяти контроллера может сохраняться до 10000 событий, на которые пользователем запрограммирована выдача сообщений. При необходимости эти события могут быть в любой момент считаны в компьютер по каналу передачи данных.

Контроллер может передавать оповещения о событиях:

* В виде SMS-сообщений
* В виде заданных речевых сообщений по голосовому каналу сотовой связи
* По стандартному каналу передачи данных сотовой связи (каналу CSD)

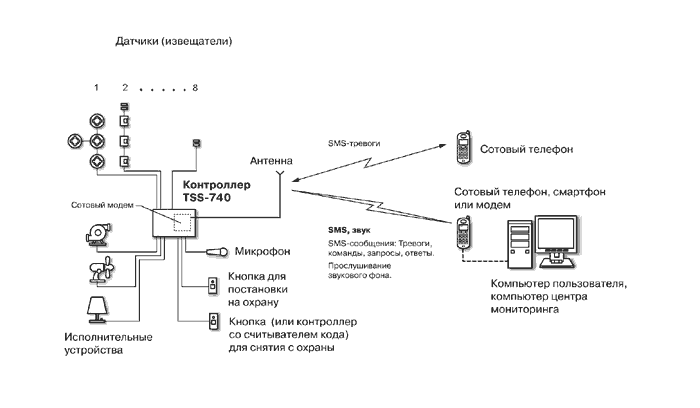
Кроме этого, для связи с контроллером можно использовать также канал передачи данных по проводной телефонной сети общего пользования через подключаемый к контроллеру внешний модем.

В память контроллера может быть записано до 8 номеров телефонов, по которым осуществляется рассылка SMS-сообщений и (или) голосовых сообщений, хранящихся в памяти контроллера.

Дистанционное задание настроек и управление контроллером может осуществляться с помощью SMS-сообщений и по каналу передачи данных. Настройка контроллера может быть осуществлена также при непосредственном подключении контроллера к компьютеру.

Контроллер не имеет жесткого алгоритма работы. Все настройки контроллера, в том числе сообщений, пороги генерации событий на аналоговых входах, реакции реле на события и прочее, задаются пользователем в зависимости от решаемой задачи с помощью специального программного обеспечения.

Звуковые файлы в WAV-формате, используемые в качестве речевых (звуковых) сообщений, создаются и загружаются в контроллер пользователем.



*Рис.2. Принцип работы контроллера TSS-740.*

Контроллер TSS-740 имеет:

1. Восемь аналоговых входов для подключения датчиков (извещателей), на которых может измеряться сопротивление в пределах от 0 до 20 кОм или напряжение в пределах от 0 до 12 В.

2. Четыре двоичных входа, к которым могут быть подключены управляющие элементы типа "сухой контакт" (например, кнопки для постановки и снятия с охраны).

3. Четыре электромагнитных реле, управляемых событиями контроллера а также внешними командами.

4. Два выхода для подключения внешних светодиодов индикации.

5. Один вход для подключения считывателя кода идентификаторов i-Button (Touch Memory) (для снятия или постановки на охрану).

6. Один порт RS-422 (RS-485) для подключения устройств расширения и дополнительных модулей.

7. Один порт RS-232 для подключения контроллера к компьютеру или подключения проводного модема.

8. Встроенный сотовый модем на базе модуля фирмы Siemens для передачи и приема информации по каналам сотовой связи стандарта GSM.

9. Вход для подключения внешней GSM-антенны.

10. Выход и вход для подключения микрофона и динамика (для автоматической выдачи речевых сообщений контроллера и осуществления голосовой связи с объектом в режиме переговорного устройства).

Номинальное напряжение питания контроллера - 12 В. Диапазон рабочих температур контроллера - от -18° до + 45° С.

4. Вывод.

Необходимо обеспечить защиту информации, располагаемой в помещениях этой фирмы, как от всевозможных способов физического проникновения злоумышленника и доступа его к защищаемой информации, так и технические каналы утечки информации.

Способ физического проникновения предполагает выбор конкретного пути преодоления злоумышленником преград для доступа к защищаемым элементам информации. Этот путь может проходить через пространственные зоны, рассмотренный пространственной моделью. В рассматриваемой мной корпорации наиболее уязвимыми элементами информации являются:

**1 ранг угрозы:**

- Себестоимость продукции;

- Партнеры.

**2 ранг угрозы:**

- Принципы, концепция и стратегия маркетинга;

- Переговоры и соглашения;

- Участие в международном сотрудничестве

**3 ранг угрозы:**

- Возможности производства;

- Исследовательские работы.

**Для улучшения защиты необходимо:**

- Установка в помещение К8 датчика движения;

- Установка видеокамер для наблюдения окна О1;

- Установка решеток на окна О12-О16;

- Установка видеокамер для наблюдения окон О12-О14 и О-15-О16;

- Установка датчиков движения в помещения К7,К9,К10.

Для улучшения защиты необходимо: осуществлять специальные проверки выделенных помещений с использованием нелинейных локаторов, установить доменное программное обеспечение для разграничения доступа пользователей к информации, установить специализированные программно-аппаратные средства авторизации и аутентификации пользователей действующей системы, в целях недопущения внутриструктурной коллизии персонала, установить специальные диэлектрических вставки в трубы систем отопления, водоснабжения, канализации, имеющих выход за пределы контролируемой зоны, использовать генераторы пространственного эл./магн. шума (пространственное эл./магн. зашумление), осуществить экранирование ТС и заземление.

5. Список используемой литературы.

1. Системный анализ в защите информации / Шумский А.А. – М, 2003.
2. Криптография и защита сетей / Принципы и практика. Вильям Столингс –М, 2005.
3. Информационная безопасность / К. Ю. Гуфан, М. П. Иванков – СПБ, 2004.

Приложение №1

